PREVENTING DATA TAMPERING USING IPFS AND ETHEREUM

BY

PANDU RANGA REDDY

ABHINAV REDDY

KRISHNA CHAITANYA VARMA

VAMSI KRISHNA REDDY

WHAT IS DATA TAMPERING?

- **Data tampering** is that act of deliberately modifying (destroying, manipulating or editing) data through unauthorized channels. Data exists in two states; in transit or at rest. In both instances, data could be intercepted and tampered with. Digital communications are all about data transmission.

For example, in the instances where data packets are transmitted unprotected, a hacker can intercept the data packet, modify its contents and change its destination address. With data at rest, a system application can suffer a security breach and an unauthorized intruder could deploy malicious code that corrupts the data or underlying programming code. In both instances the intrusion is malicious and the effects on the data always dire. It is one of the biggest security threats that can face any application program or organization.

HOW TO PREVENT DATA TAMPERING

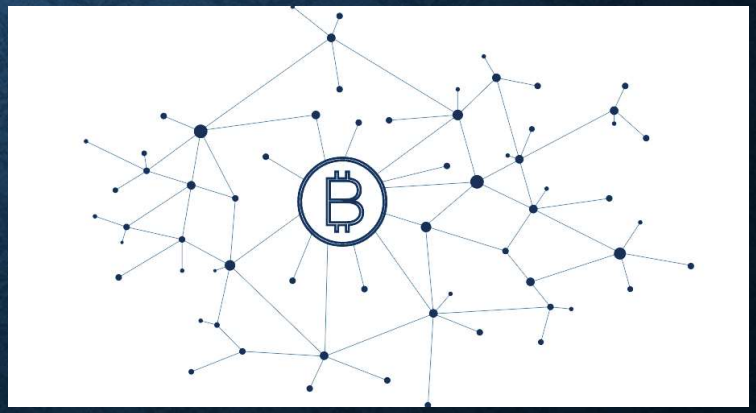
The solution is Blockchain. Blockchain technology began as a validating technology for bitcoin digital currency. It created a record of digital events distributed across different participants or entities involved in a transaction. Now blockchain is being pursued to provide global authenticity and security for any type of data and transactions.The idea behind blockchain is to create a public "ledger" of transactions that are linked chronologically and cannot be deleted or edited. Each record, or blockchain, is time-stamped and verifiable. It ensures data integrity by attributing data to an irrefutable identity, validating all copies of the ledger, ensuring full availability, and providing tamper-proof security.

WHAT IS BLOCKCHAIN?

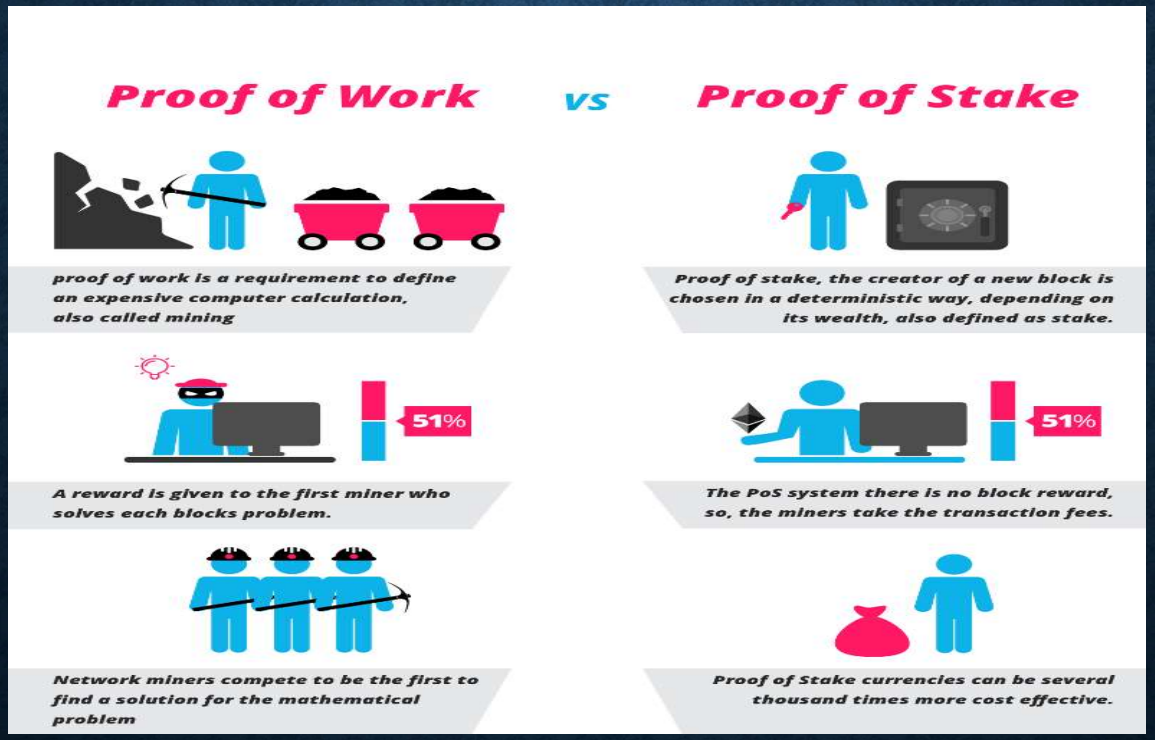
- A **blockchain** is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network.
- Mainly works on two concepts they are

  i.)Proof of Work

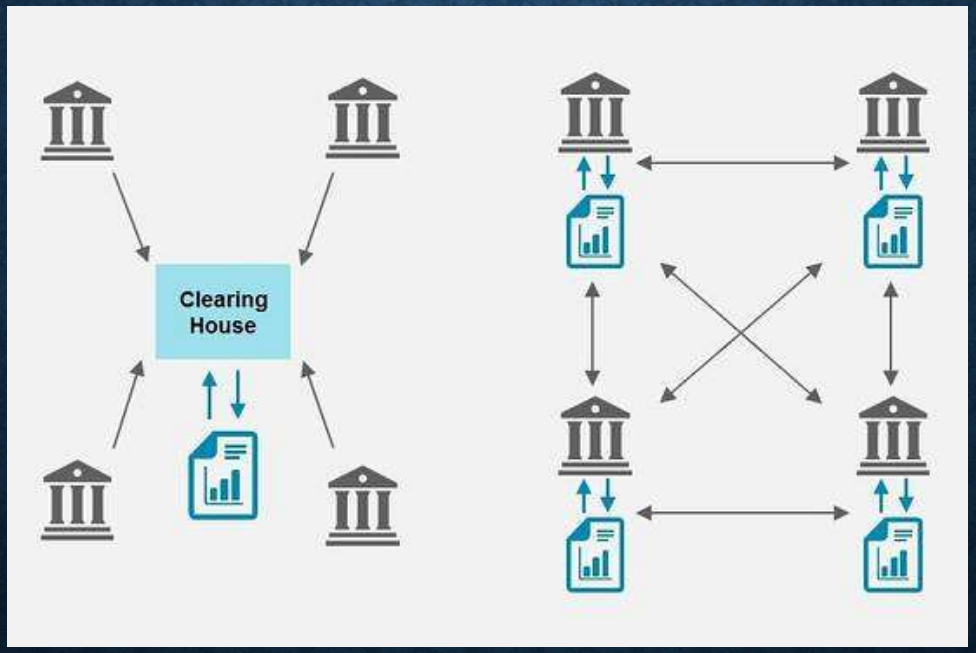
  ii.)Proof of Stake



PROOF OF WORK VS PROOF OF WORK



FROM CENTRALIZATION TO DECENTRALIZATION



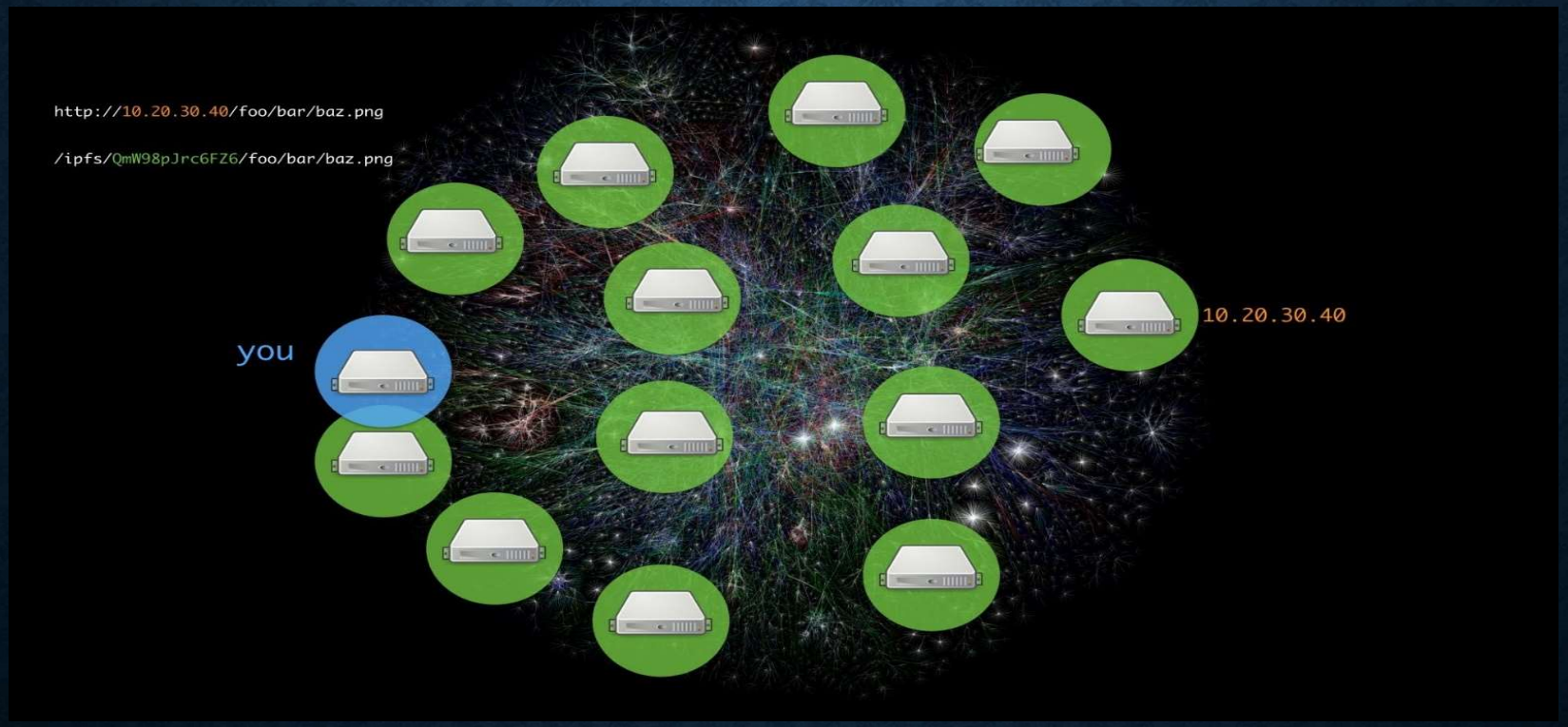
INTER PLANETARY FILE SYSTEM

- **InterPlanetary File System** (**IPFS**) is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. IPFS was initially designed by Juan Benet

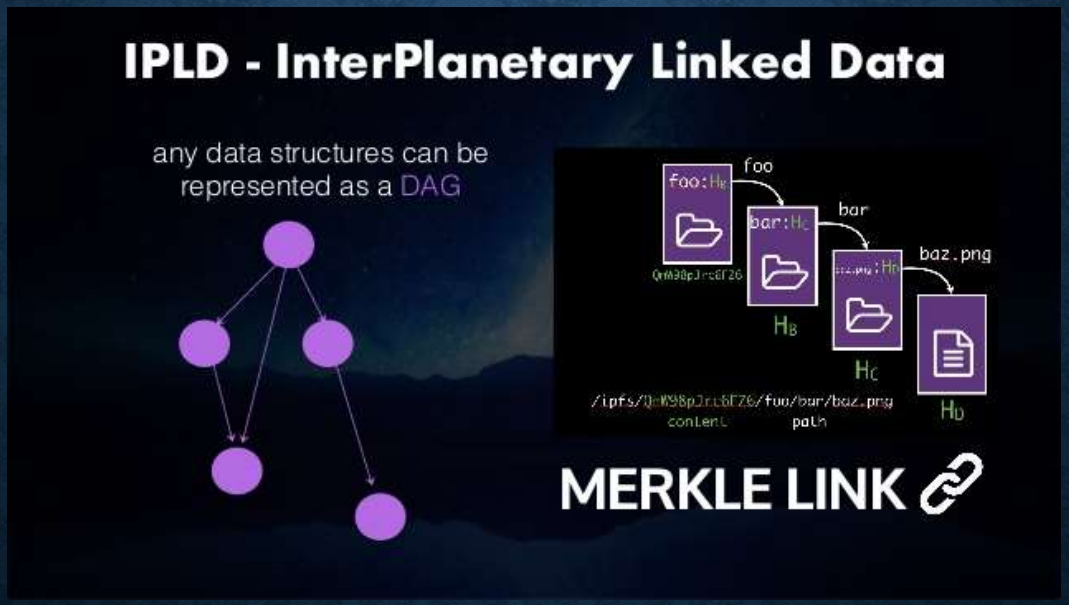
MORE ABOUT IPFS

- IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. In some ways, IPFS is similar to the World Wide Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks. This forms a generalized Merkle directed acyclic graph (DAG). IPFS combines a distributed hash table, an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and nodes do not need to trust each other, except for every node they are connected to. Distributed Content Delivery saves bandwidth and prevents DDoS attacks, Data Tampering, which HTTP struggles with.

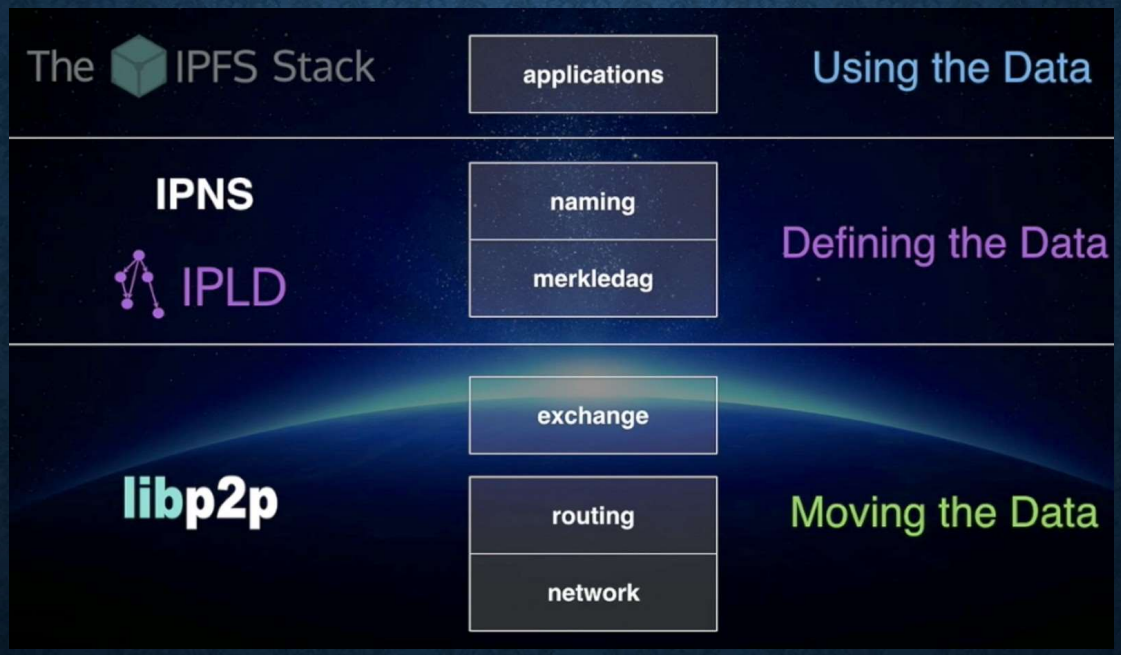
MORE ABOUT IPFS



INTERPLANETARY LINKED DATA



DIFFERENT LAYERS IN THE IPFS SYSTEM

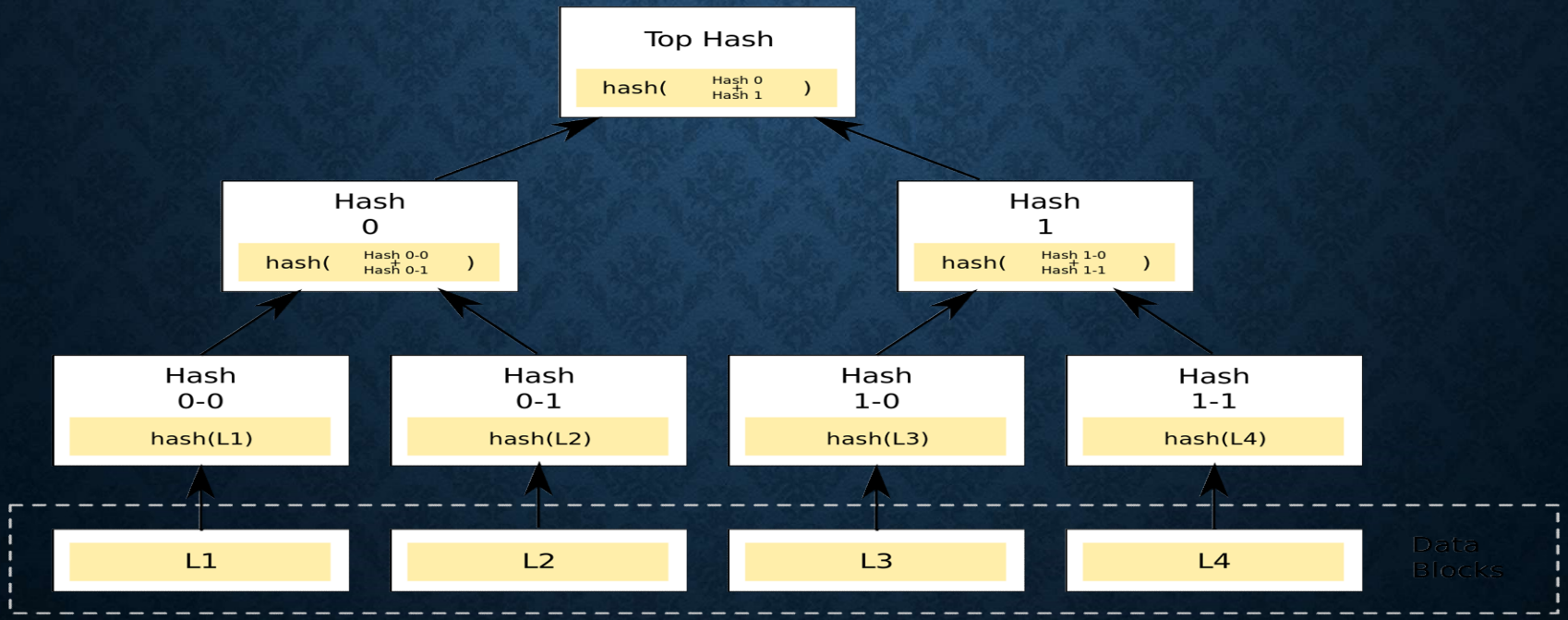


WHAT IS A MERKLE DAG?

Before we know about Merkle DAG we need to know about Merkle Tree

Merkle tree - In cryptography and computer science, a **hash tree** or **Merkle tree** is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

MERKLE TREE


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

COMING BACK TO MERKLE DAG

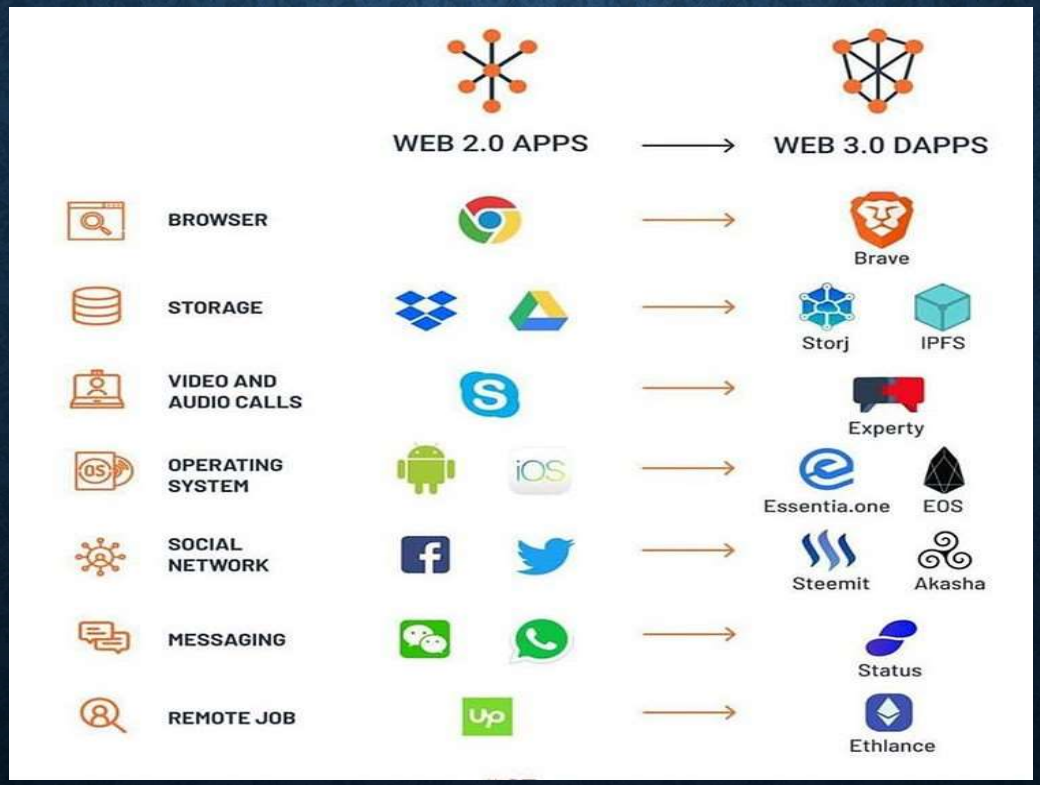
Merkle DAG. A directed acyclic graph whose objects are linked to each other (usually just by their hash), where the hash(object) includes all hash(linked_object)

Finally the below figure tells us how and why ipfs is selected for our project.

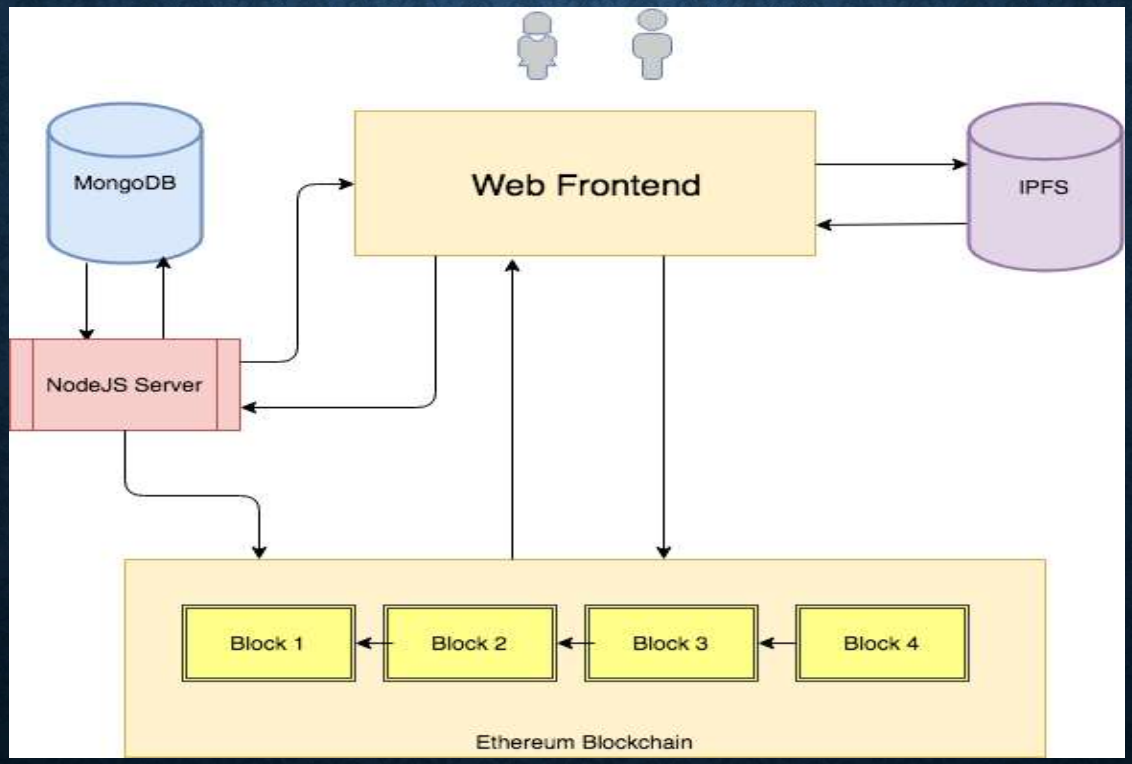
ETHEREUM FRAMEWORK

- **Ethereum** is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality. It supports a modified version of Nakamoto consensus via transaction-based state transitions.
- So we can build applications on it and integrate it with IPFS for better security and performance.

PRESENT VS FUTURE



IPFS AND ETHEREUM INTEGRATION



CONCLUSION

The main idea of this project is to prevent data tampering in a web environment by using blockchain concepts , IPFS and ethereum framework. i.e. securing data from all layers and achieving the global 51% trust in the system.