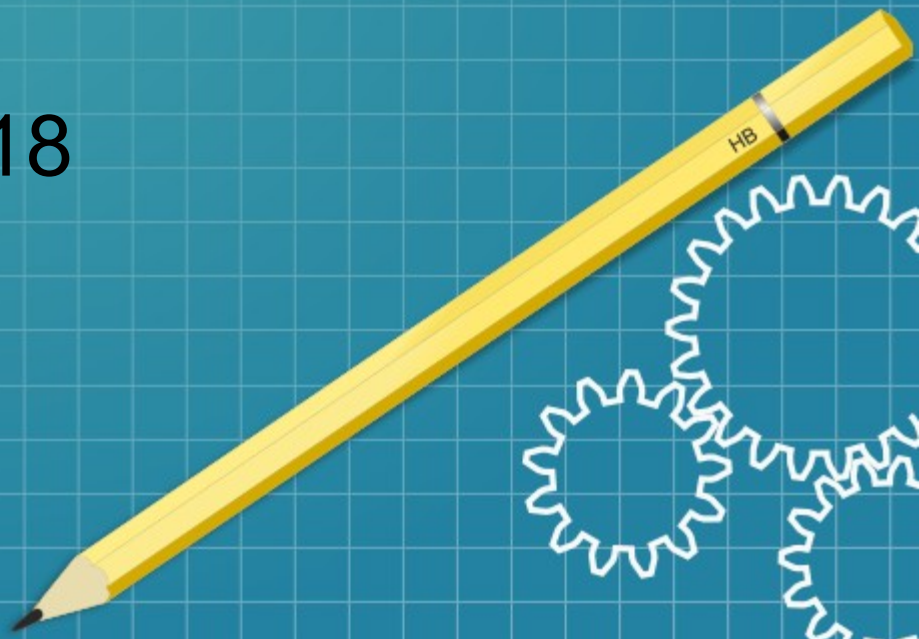
Application of Blockchain Technology

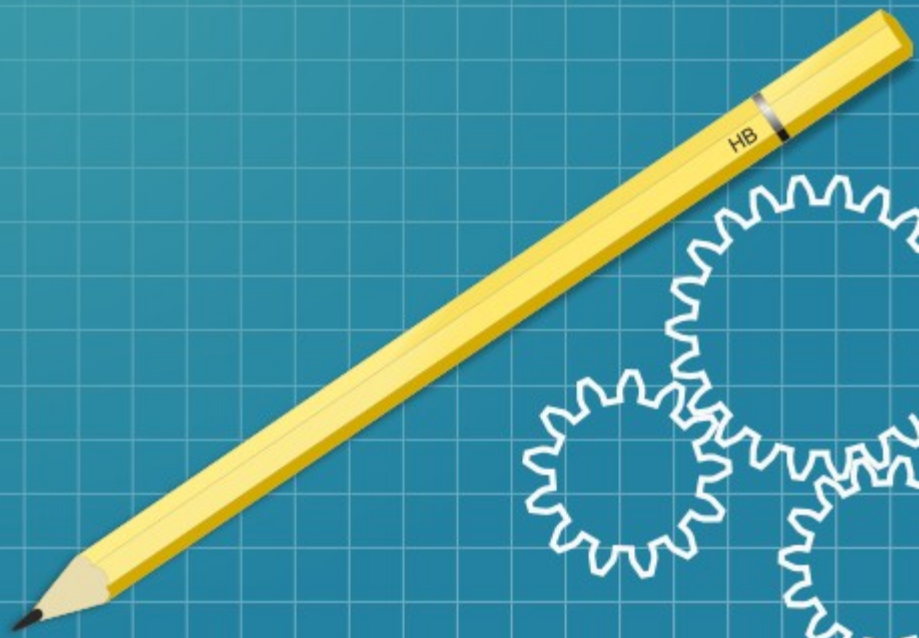
Xiyang Wang (Tony)

04/21/2018



Introduction

- Recently, savvy individuals have recognized the technical potential behind the Bitcoin
- IPFS
- Bitshares
- Steemit
- CDT



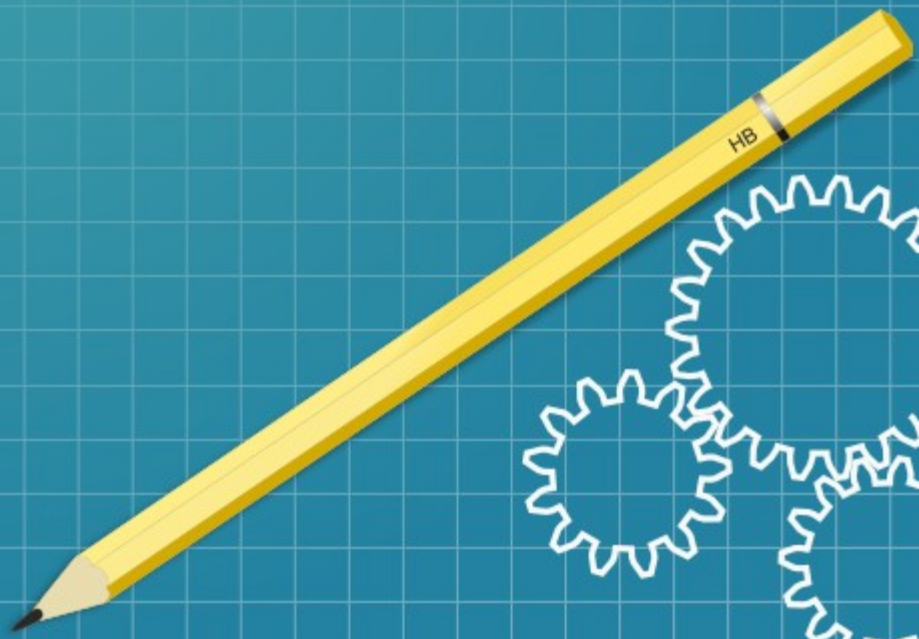
Smart Contract

- Facilitate the transfer and exchange of money or property in a transparent way without middleman
- Define all of the obligations and potential penalties involved in an agreement
- Smart contract platform also automatically enforces all of these obligations and penalties
- Smart contract platforms allow the development of decentralized applications to run on the network

Ethereum VS EOS

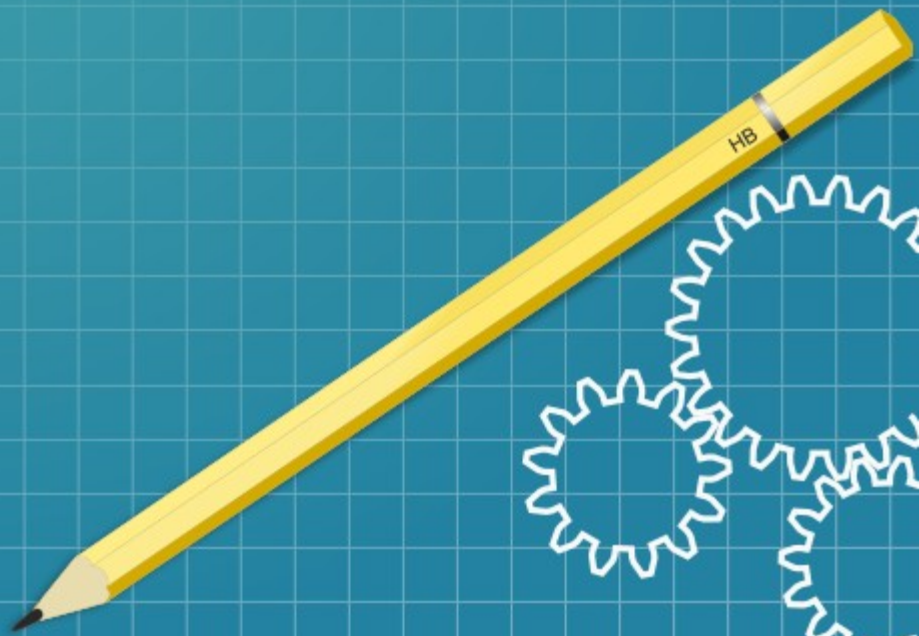
Ethereum

- Described as application-agnostic
- “No features”
-



EOS

- No transaction fees
- More flexibility
- Improved scalability



Design Philosophy

EOS

VS.

ethereum

- Provide all of the cryptography and app/blockchain communication functions to allow developers to focus on their business-specific logic functions
- Generalized role-based permissions
- Web toolkit for interface development
- Self-describing interfaces
- Self-describing database schemes
- Declarative permission scheme

"We have no features: as a corollary to generalization, we often refuse to build in even very common high-level use cases as intrinsic parts of the protocol, with the understanding that if people really want to do it they can always create a sub-protocol (e.g. ether-backed subcurrency, bitcoin/litecoin/dogecoin sidechain, etc…) inside of a contract."

- Ethereum Design Rationale

https://github.com/ethereum/wiki/wiki/Design-Rationale

Scalability

EOS

VS.

ethereum

- Single-threaded performance of 10,000-100,000 transactions per second
- Parallelization will scale the network to millions of transactions per second
- Supports thousands of commercial scale decentralized applications
- Asynchronous communications
- Separates authentication from execution
- Does not require counting operations

- Currently limited by the single threaded performance of a CPU
- Early test networks achieved 25 transactions per second which can likely be optimized further to 50 or 100 tx/s
- The network has been overwhelmed in the past, e.g. during the Status ICO
- Vitalik Buterin has laid out a roadmap to "unlimited scalability" using the concept of sharding, which is technologically challenging and currently in progress

Economics of the Network

EOS

VS.

ethereum

- Ownership model
- Owning EOS tokens gives a proportional share in network bandwidth, storage, and processing power
- Reliable, predictable network bandwidth and computing power for small businesses
- Relatively small investment for minimum bandwidth and computing power
- Zero transaction fees, no cost for developers except the initial EOS tokens

- Rental model
- Gas fees are required in exchange for every calculation, storage operation, and bandwidth utilization
- Required fees fluctuate and can spike prohibitively high as miners preferentially select transactions with largest fees
- Rich actors can freeze the network by flooding it with high fee transactions
- Developers continually burn gas fees throughout development and deployment

Consensus Mechanism & Governance

EOS

VS.

ethereum

- Delegated Proof of Stake
- Mechanism to freeze and fix broken or frozen applications (e.g. if the DAO had been implemented on EOS, it could have been frozen, fixed, and updated without disrupting the other EOS applications)
- A legally binding constitution establishes a common jurisdiction for disputes
- EOS will also include self-funded community benefit apps selected by vote
- No risk of fork spawning multiple chains

- Proof-of-Work with plans to transition to Proof-of-Stake/Proof-of-Work hybrid
- Failed and broken applications either result in investor losses or disruptive hard forks (e.g. the failure of the DAO that resulted in ETH and ETC)
- Hard forks are at risk of spawning multiple competing networks
- Fixing one failed application requires disrupting the entire network (e.g. the DAO hard fork)

Denial-of-Service Attacks

EOS

VS.

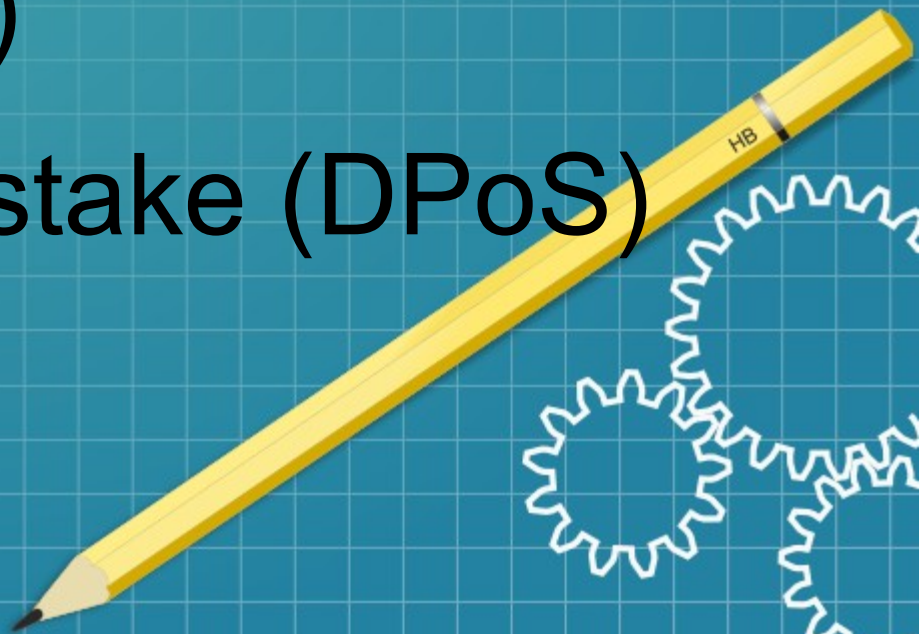
ethereum

- The ownership of EOS tokens gives users a proportional stake in the network bandwidth, storage, and computing power
- Spammers can only consume the proportion of the network that their EOS tokens entitle them to
- Denial-of-service attacks on a given app cannot disrupt the entire network
- Startups with a very small stake in the network will have guaranteed, reliable bandwidth and computational power

- Miners preferentially select high-fee transactions to add to the blockchain
- A single smart contract (like the Status ICO) can freeze out the entire network
- A flood of high-fee transactions can always freeze the network, regardless of how powerful the network is
- For example, the Status ICO was a "race-condition" ICO, meaning the first accepted transactions "win". People flooded the network with high-fee transactions, effectively freezing the entire network.

Consensus mechanism

- Proof of work (PoW)
- Proof of stake (PoS)
- Delegated Proof of stake (DPoS)



Proof of Work

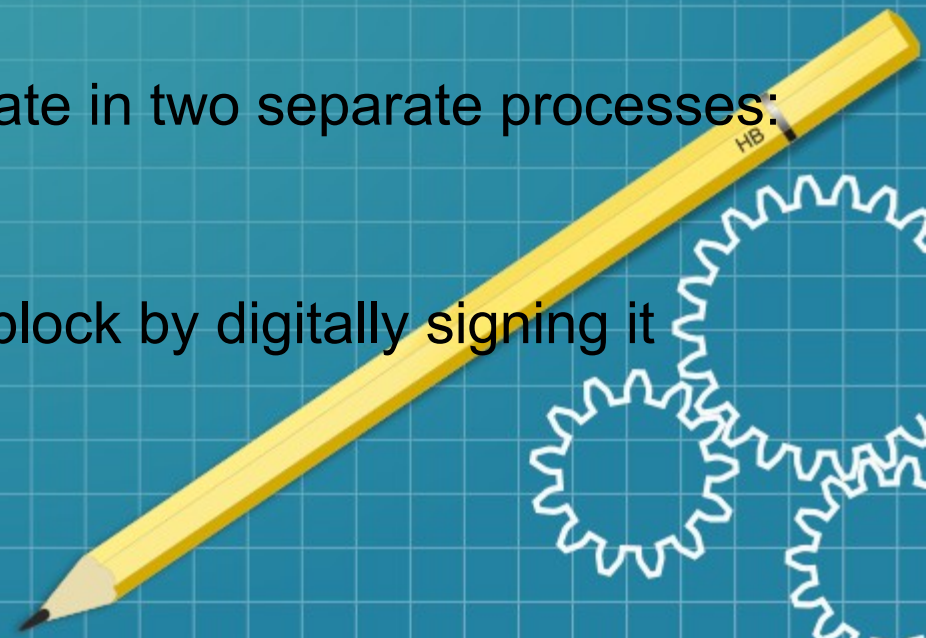
- Bitcoin as an example of a cryptocurrency system secured with a proof of work algorithm
- Mining
- Mining requires a great deal of computing power to run different cryptographic calculations to unlock the computational challenges. The computing power translates into a high amount of electricity and power needed for the proof of work.

Proof of Stake

- The proof of stake (PoS) seeks to address above issue by attributing mining power to the proportion of coins held by a miner. This way, instead of utilizing energy to answer PoW puzzles, a PoS miner is limited to mining a percentage of transactions that is reflective of his or her ownership stake.
- For instance, a miner who owns 3% of the Bitcoin available can theoretically mine only 3% of the blocks.
-

Delegated Proof of Stake

- Delegated proof of stake (DPoS) is a generic term describing an evolution of the basic PoS consensus protocols
- In the protocol, blocks are minted by a predetermined set of users of the system (delegates), who are rewarded for their duty and are punished for malicious behavior
- In DPoS algorithms, delegates participate in two separate processes:
- • building a block of transactions
- • verifying the validity of the generated block by digitally signing it
-



Vulnerability

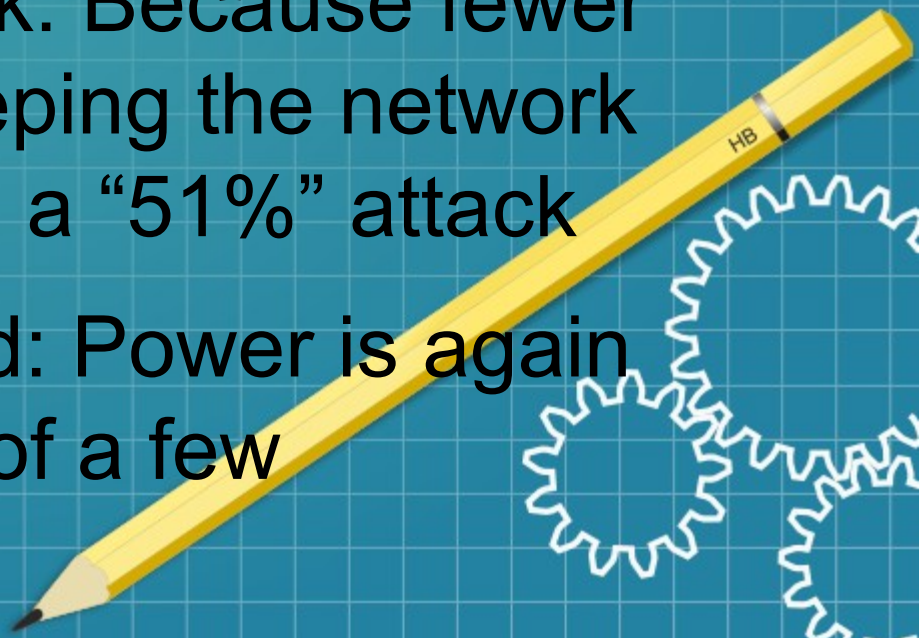
- Proof of Work
- PoW is vulnerable to a “51% attack,” meaning — in theory — nefarious miners could capture 51 percent of a network’s computing power, gain what’s termed “dominance“ and manipulate the blockchain to their advantage.

Vulnerability

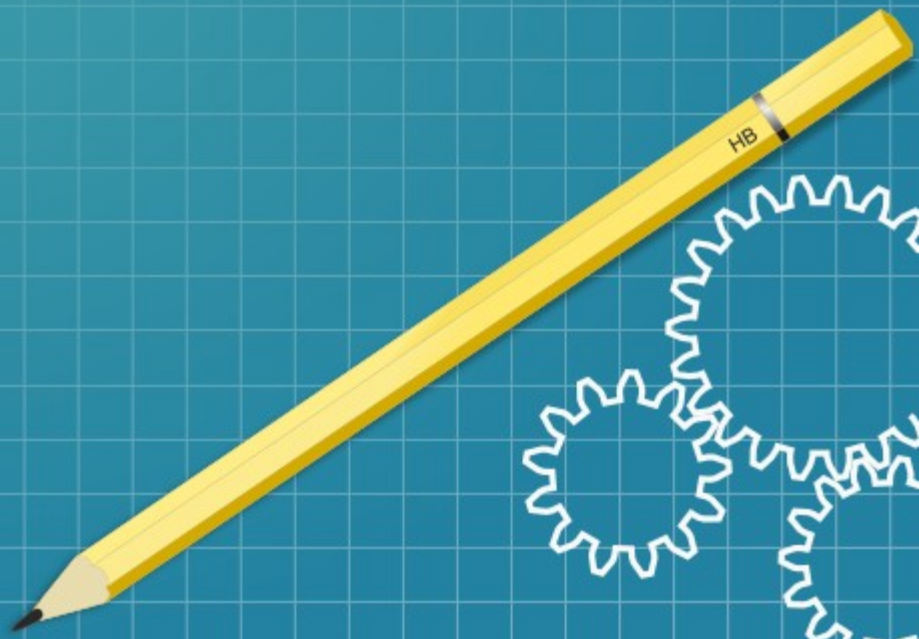
- Proof of Stake
- Someone with enough money to invest exclusively into the destruction of this system can do so by investing only money, as opposed to PoW where they need to invest money, time, expertise, hardware, electricity, etc.
- Only the richest stakeholders are permitted to have control of consensus in the blockchain

Vulnerability

- Delegated Proof of Stake
- Cartels: Witnesses could organize into cartels.
- Easier to organize an attack: Because fewer people are in charge of keeping the network alive, it’s easier to organize a “51%” attack
- Potentially more centralized: Power is again concentrated in the hands of a few



Which one is better?

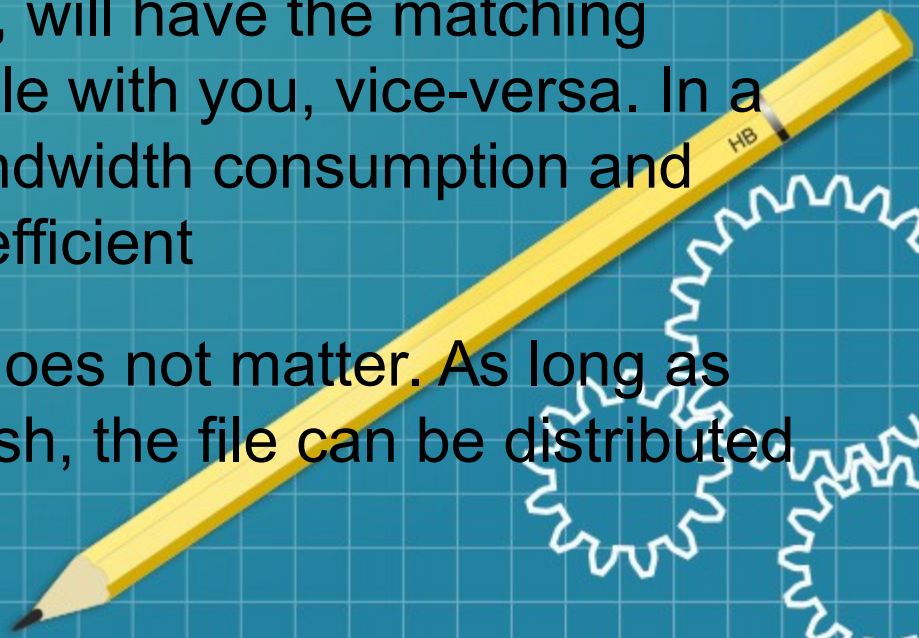


IPFS

- IPFS stands for Inter Planetary File System

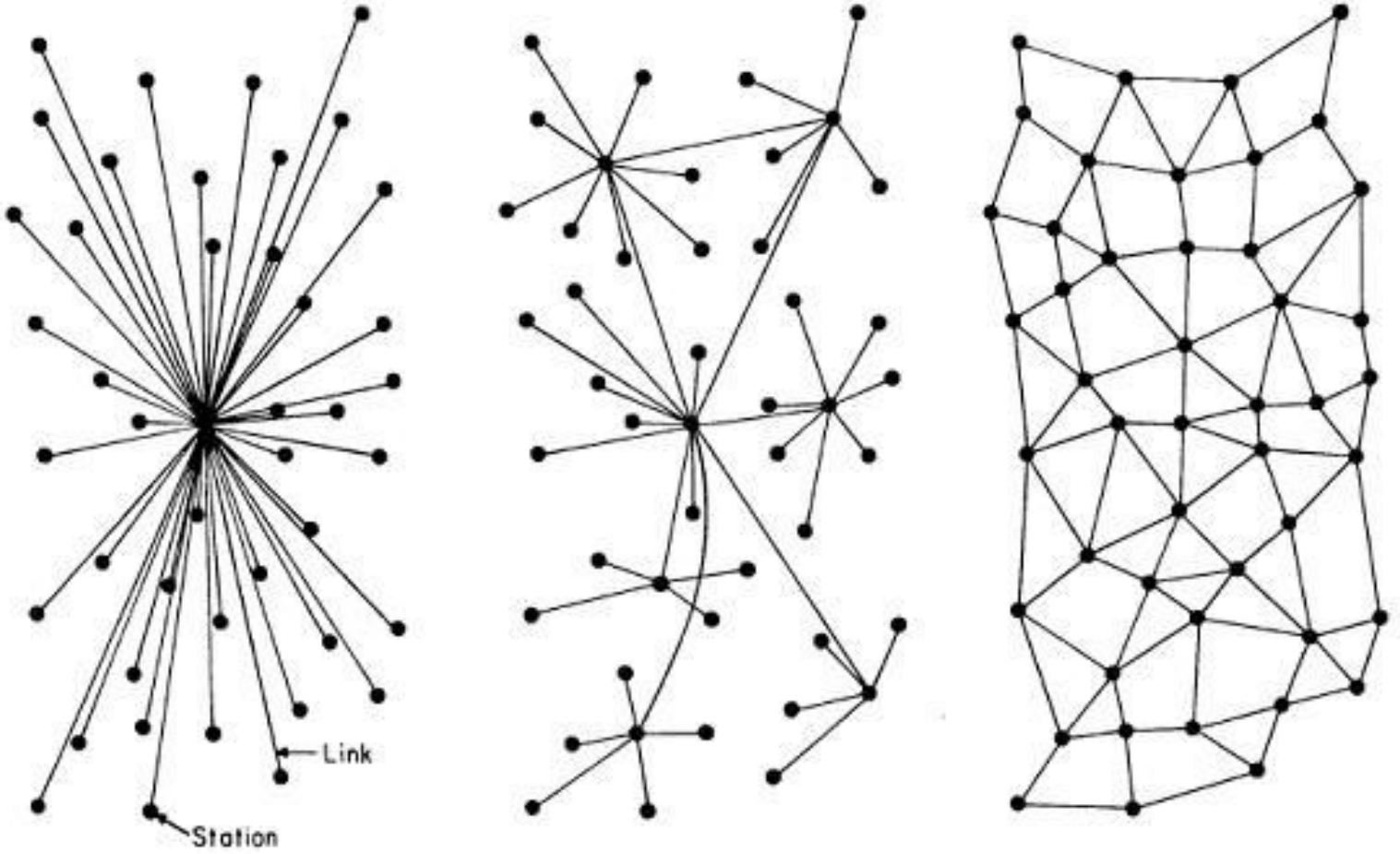
The basic idea of IPFS

- IPFS is a peer-to-peer file sharing system, which is by nature, distributed. In particular, it uses cryptographic hashes of the content as the pointer to the file, not the address of the file
- Anybody who has the same content, will have the matching hash, and that peer can share that file with you, vice-versa. In a distributed network such as this, bandwidth consumption and speed of file transfer is much more efficient
- Not only that, if the file is moved, it does not matter. As long as there is a peer with the matching hash, the file can be distributed



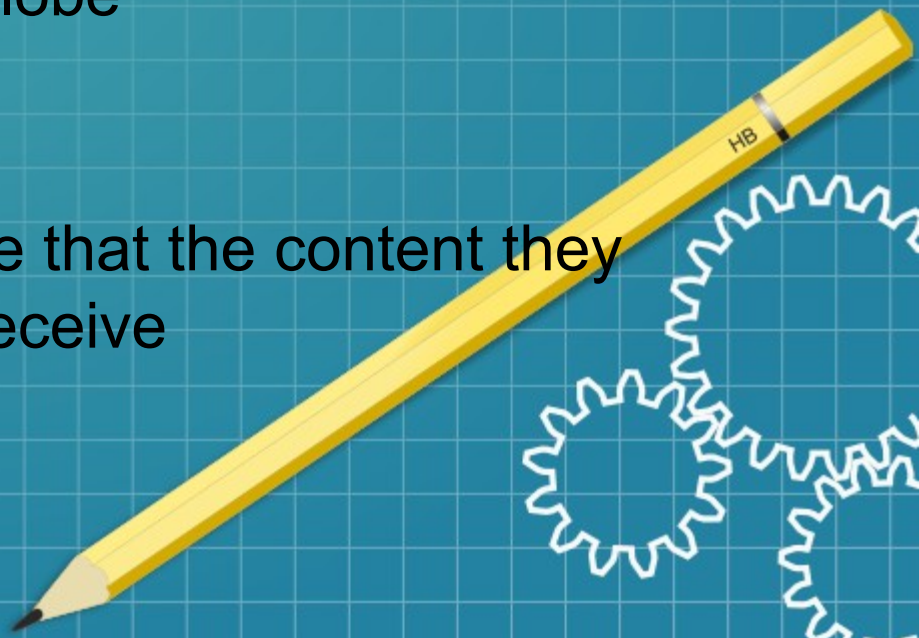
Difference between IPFS and HTTP

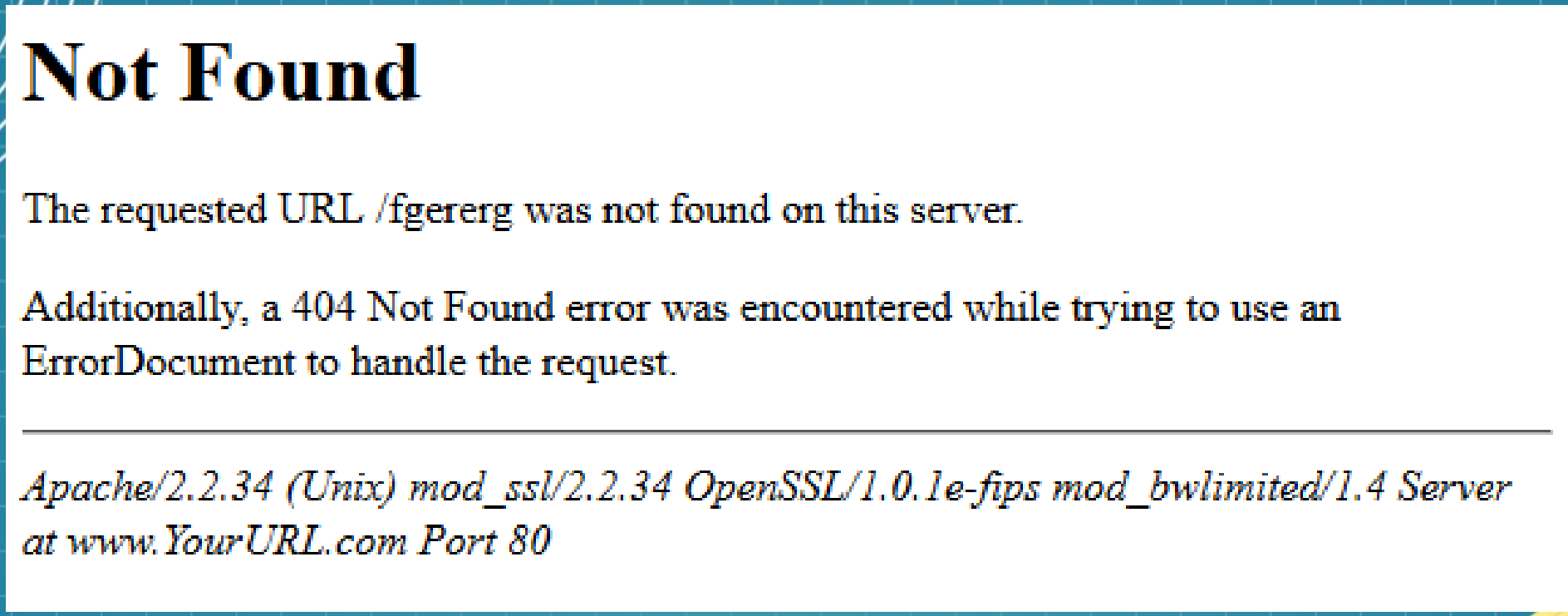
- HTTP is based on the centralized server model. This means that there is a single server somewhere that manages the links to other systems for exchange of information
- IPFS is not just a protocol. It is a distributed, hypermedia protocol that aims to make the web safer, faster and more open
- HTTP tries to download the whole file from one system. However, IPFS allows multiple parts of a file to be downloaded simultaneously from many different systems. This results in faster downloads and almost no loss of bandwidth


Link
Station
CENTRALIZED
(A)
DECENTRALIZED
(B)
DISTRIBUTED
(C)

Problems with centralized file sharing

- Bandwidth
- a small piece of file has to transfer through dozens of centralized servers, all across the globe
- Provenance
- people need some sort of guarantee that the content they requested, is the content they will receive





- It means that the website location has been changed and the server previously hosting it has gone down and no one knows the current location. This usually occurs if the web pages are too old and the server hosting them too outdated.

Blockchain with IPFS

- Like Bitcoin, the IPFS is a peer-to-peer network run by multiple nodes that store files that are submitted to the network. These nodes store only content that are interesting, including common indexing information that helps users find the nodes that keep the files they are looking for within the network.
- Each file submitted to the network is given a unique cryptographic hash that allows the IPFS network to automatically delete duplicates and track version history for every file. Historic versioning prevents information from being easily erased. Since the files are provided by distributed nodes, download speeds are higher.
- These characteristics make the IPFS a perfect place to store data, which can be referenced and time stamped with blockchain technology.

- Since blockchain technology is not fit to store large amounts of data, the IPFS can be used by blockchain applications that need a publicly accessible database. While the immutability provided by miners and the transparency of the blockchain, make it the perfect place to timestamp content and make it publically verifiable.




Set up IPFS

- Set up GPG
- Set up IPFS
- Encrypt a file with someone else's public key
- Upload the encrypted file to IPFS
- Download the file from another computer (or Virtual Machine) and make sure only the privileged party can decrypt and view it

Tutorial

Blockchain Tutorial