5 min break

Blockchain at Michigan

W1: Intro to Blockchain

2022

Questions For The Semester

1. What is a blockchain?
2. How does it work?
3. Why does it matter?
4. What’s in store for the future?
5. How can we use it?

The Road Ahead

W1: Introduction

W2: Consensus

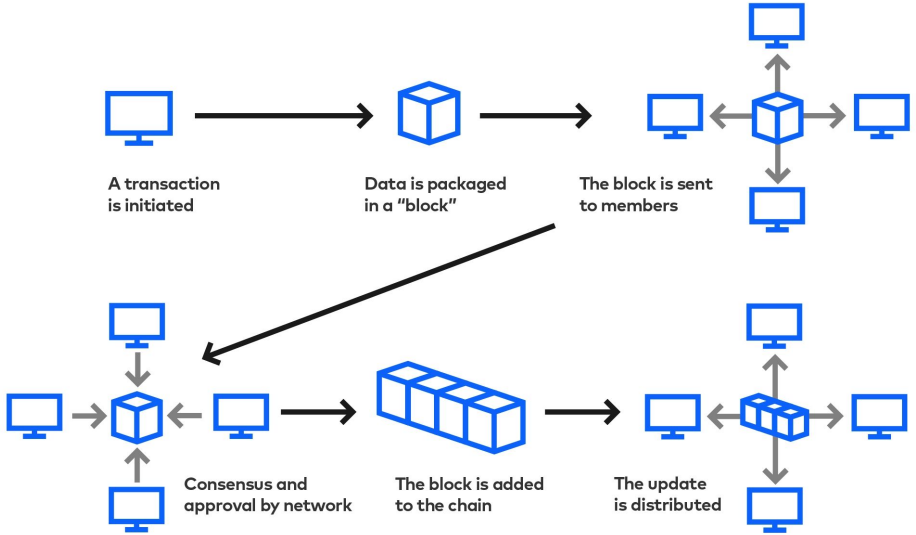
W3: PoW & Bitcoin

W4: PoS & Ethereum

W5: Solidity

W6: Web3, NFTs, Metaverse

The Road Ahead



https://www.slalom.com/sites/default/files/inline-images/blockchain-diagram-2-100.jpg

Trust

Who do you trust?

Do you trust me?

Trust

Who do you trust?

Do you trust me?

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

Trust

Who do you trust?

Do you trust me?

Blockchain = Automated Trust

What actually is it?

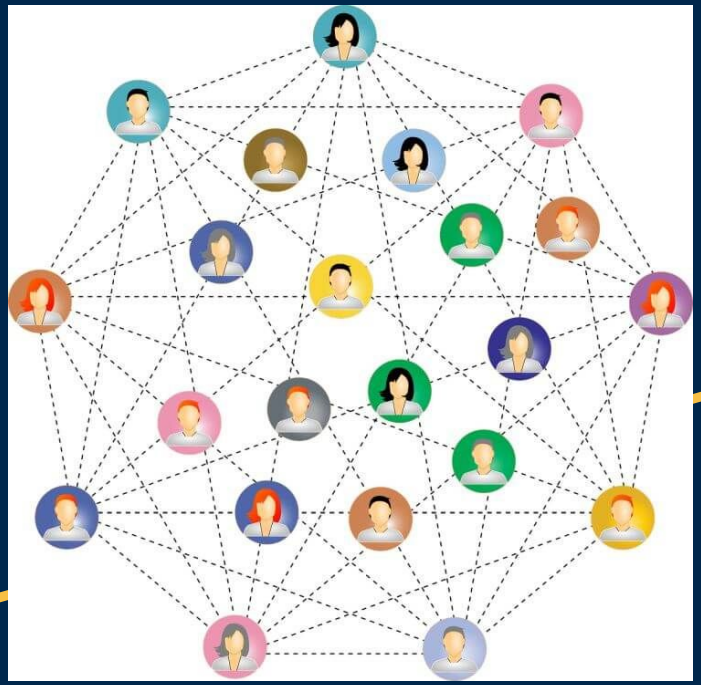
"A *blockchain* is a type of decentralized database system based on linking together previous records in secure blocks of information."

- Dictionary.com

What actually is it?

1. Network
2. Data structure
3. Consensus protocols

1. Network

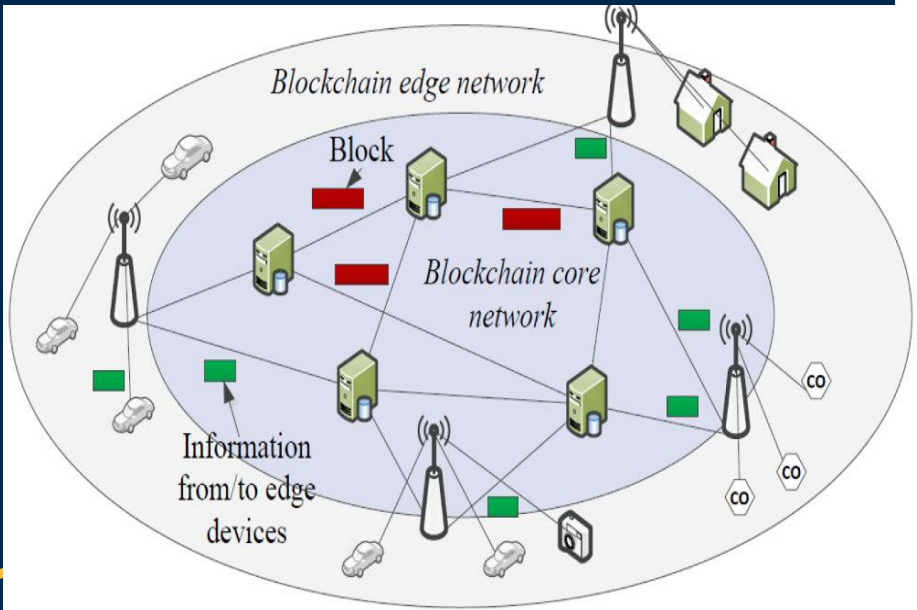


A network is a bunch of edges and nodes, where the edges connect some nodes together.

Many types of networks:

- Social Networks
- Biological Networks
- Computer Networks

1. Network



Peer-to-Peer (P2P) Connections between different servers on the network.

Distributed Systems

- Information dispersal
- Data storage
- Decentralization

Laptops, phones, servers, etc.

So... where is it?

Nodes!

Eg. Bitcoin:

- Full nodes
- Super nodes
- Light nodes
- Mining nodes

As of Jan 2022, size of Bitcoin blockchain is **324 GB**.

(reference)

More info:

https://medium.com/sazmining/what-is-a-bitcoin-node-b1106b050ace#:~:text=In%20the%20case%20of%20the,perform%20a%20different%20function%20entirely.

Questions?

2. Data Structure

Blockchain = Blocks in a chain

2. Data Structure

Blockchain = Blocks in a chain

Duh

2. Data Structure

Demo:

https://andersbrownworth.com/blockchain/blockchain

2. Data Structure

Longer = better?

2. Data Structure

Longer = better?

Yes

As of Oct 2021, Bitcoin transactions take around **10 mins ~ 1 hour**. (reference)

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

Questions?

3. Consensus

Coming soon...

(aka next week)

Is it safe?

51% attack

Is it safe?

51% attack

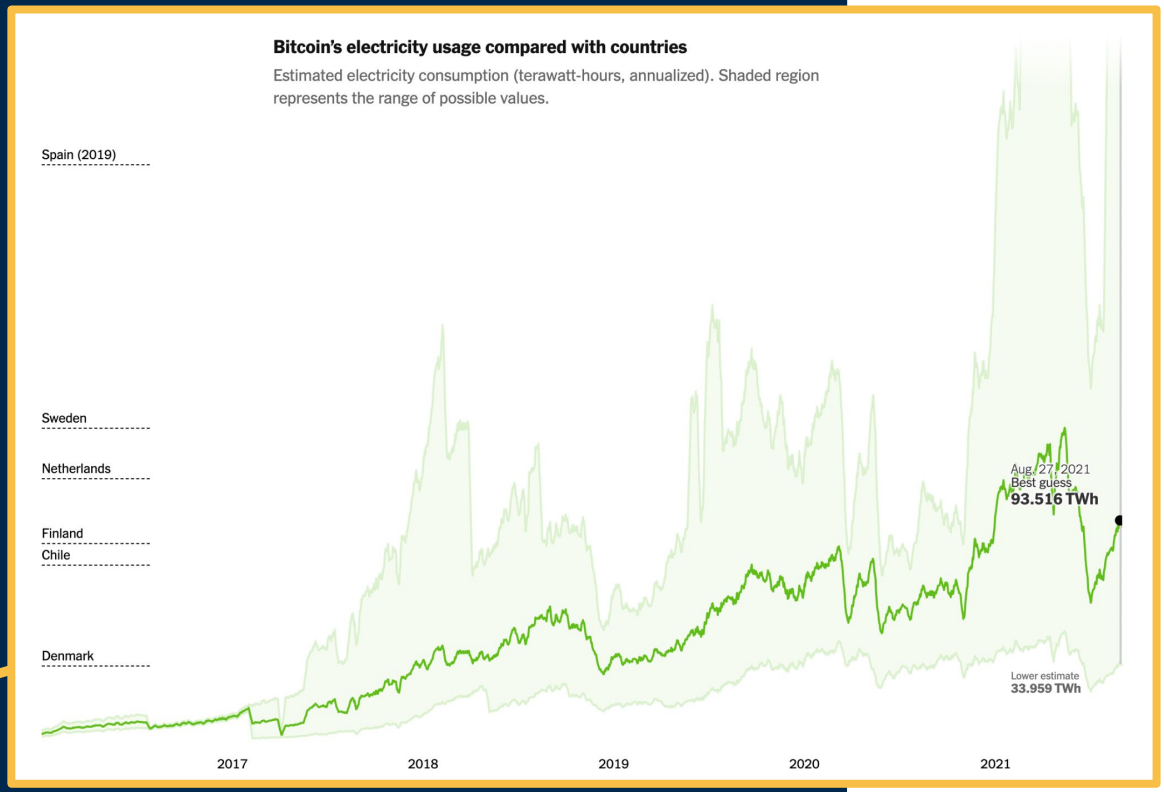
1. Impractical
2. Little incentive

As of July 2019, Bitcoin's hash rate is roughly **67,500,000 Th/s**. (reference)

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

Some perspective

51% attack



As of August 2021, Bitcoin used **~93 TWh** per year.

This is more than the entirety of Finland!

(reference)

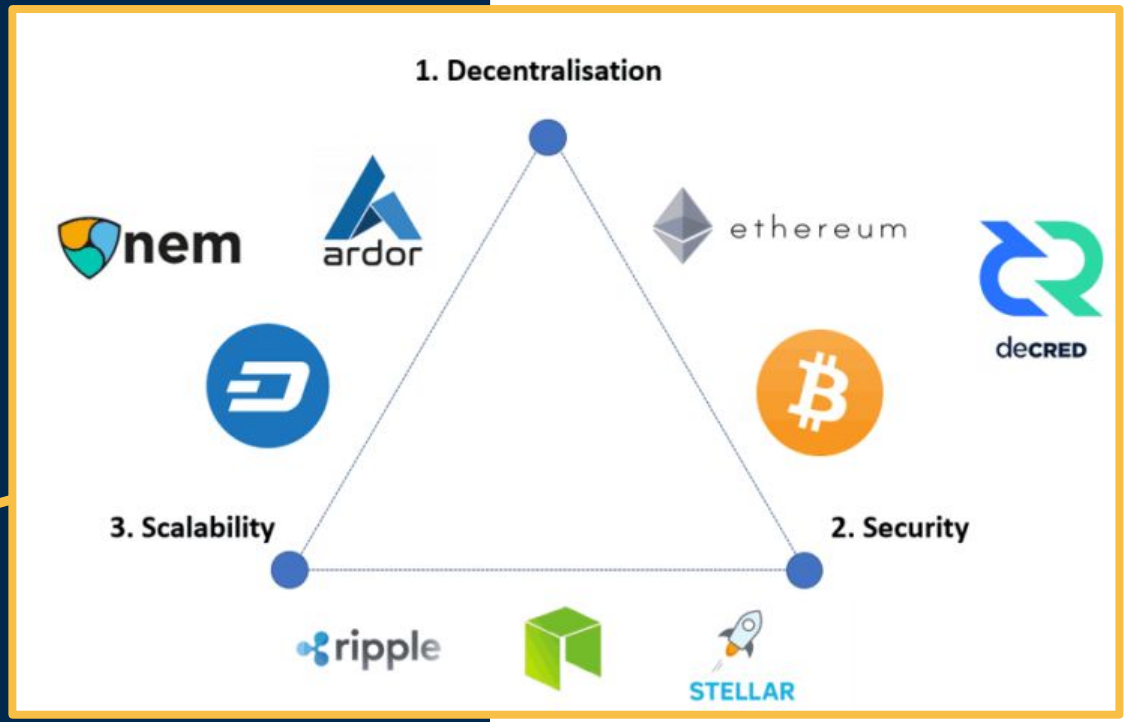
Just for fun!

In 2005, UMich used **~2.2 TWh**.

(reference)

Questions?

Blockchain Trilemma



Reference/More info:

https://toshitimes.com/what-is-the-blockchain-trilemma-security-vs-scalability-vs-decentralization/

Readings:

1. Crypto Anarchist Manifesto, by Tim May
2. bmoney, by Wei Dai

*There will be a discussion next session