Oregon Blockchain

Week 3: Blockchains and Nodes

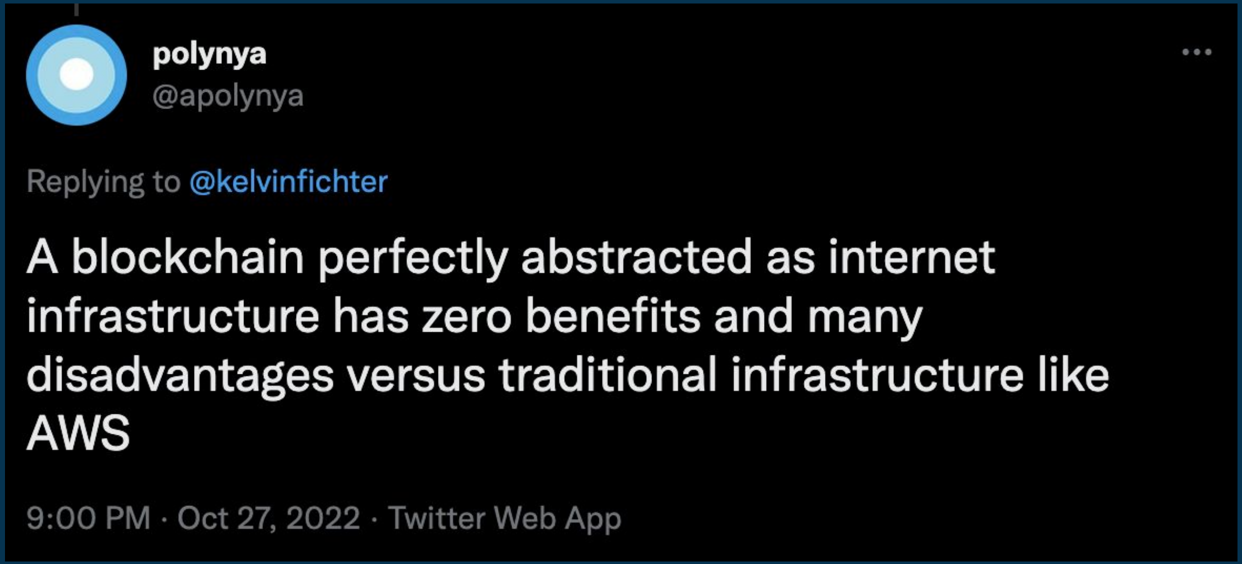
OBG Onboarding Fall 22

Homework!

- Name the purpose of blockchains and two things that use cryptography (try to not duplicate)!

- Any questions about last class/homework?

Why do we care how this shit works



polynya
@apolynya

Replying to @kelvinfichter

A blockchain perfectly abstracted as internet infrastructure has zero benefits and many disadvantages versus traditional infrastructure like AWS

9:00 PM · Oct 27, 2022 · Twitter Web App

The benefits are invisible to consumers!

No knowledge -> erodes node participation -> erodes benefits

What is a blockchain

Decentralized network that agrees on the inclusion and ordering of transactions

Mechanisms:

1. Users (What gives the blockchain its magic)
2. Consensus protocol
3. State machine

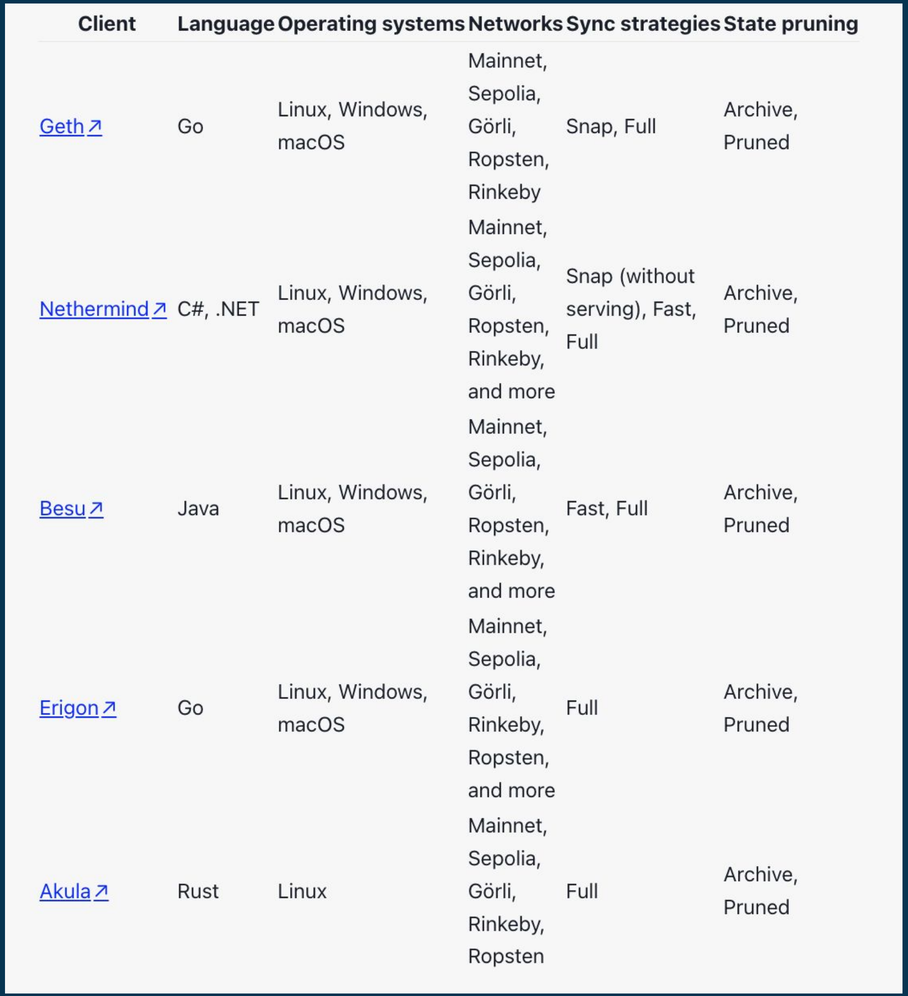
Oregon Blockchain

Mechanism 1: Users

Clients (FOSS Software!)

Protocol spec in yellow paper

Protocol implemented in different languages



Client	Language	Operating systems	Networks	Sync strategies	State pruning
Geth↗	Go	Linux, Windows, macOS	Mainnet, Sepolia, Görli, Ropsten, Rinkeby	Snap, Full	Archive, Pruned
Nethermind↗	C#, .NET	Linux, Windows, macOS	Mainnet, Sepolia, Görli, Ropsten, Rinkeby, and more	Snap (without serving), Fast, Full	Archive, Pruned
Besu↗	Java	Linux, Windows, macOS	Mainnet, Sepolia, Görli, Ropsten, Rinkeby, and more	Fast, Full	Archive, Pruned
Erigon↗	Go	Linux, Windows, macOS	Mainnet, Sepolia, Görli, Rinkeby, Ropsten, and more	Full	Archive, Pruned
Akula↗	Rust	Linux	Mainnet, Sepolia, Görli, Rinkeby, Ropsten	Full	Archive, Pruned

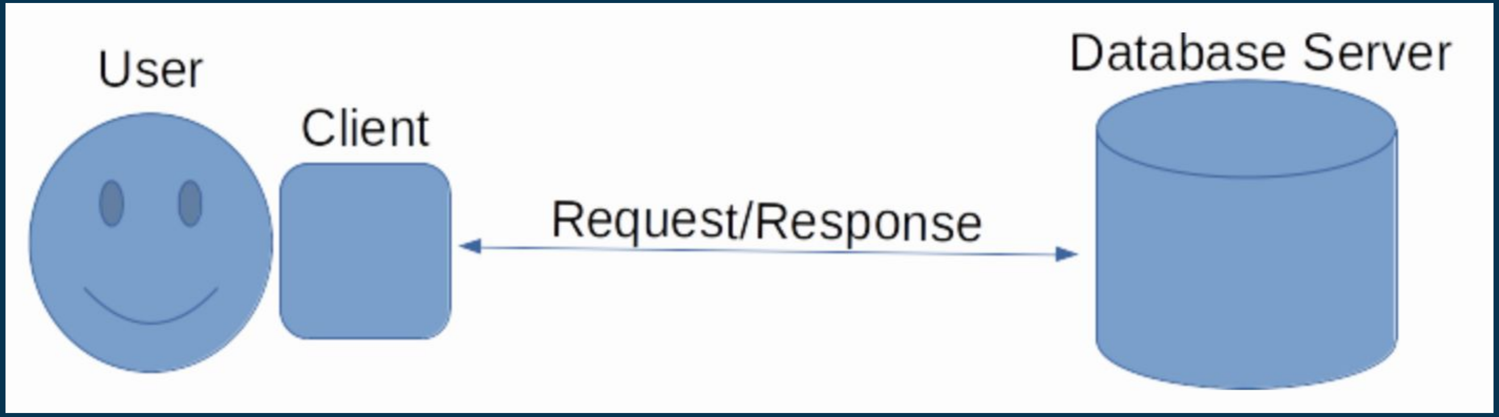
Network Users

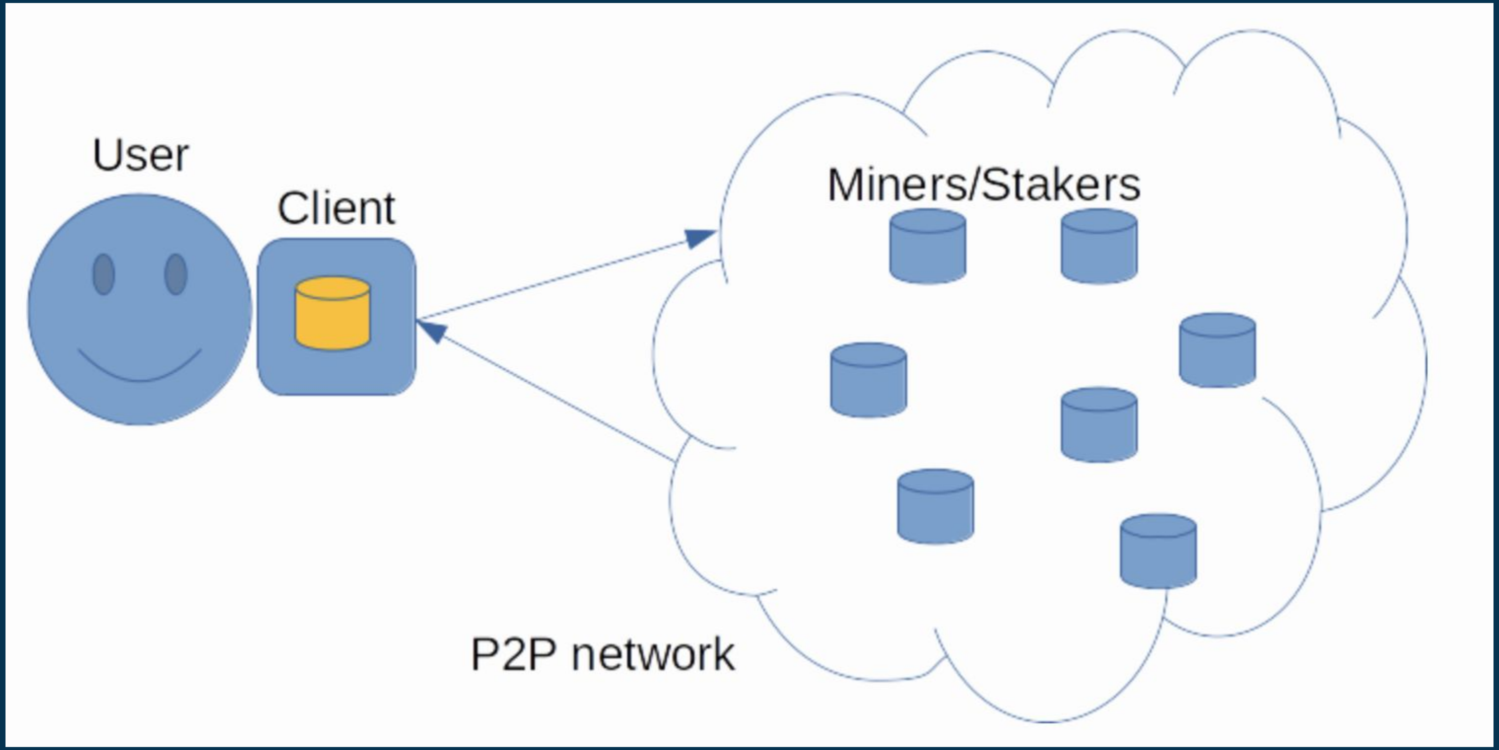
Block producers

- Miners & Validators
- Form consensus on what updates to publish
- Requires some hardware

Full nodes

- Choose to accept or reject inbound updates
- Form consensus on what updates are committed


User
Client
Request/Response
Database Server


User
Client
Miners/Stakers
P2P network

BTC independence day

Takeaways

Running a node gives you a vote in social consensus!

or

Using someone else’s node delegates your vote

Oregon Blockchain

Mechanism 2: Consensus Protocol

What is consensus

How a distributed system comes to agreement

State machine replication:

1. Happens in rounds
2. Everyone runs input on their own machines (Mechanism 3!)
3. Compare outputs
4. Form consensus on the truth
5. Go to next round

Consensus Thresholds

Consensus threshold depends on assumptions about network latency

In synchrony, requires 51% honest (2f + 1)

In partial synchrony, requires 66% honest (3f + 1)

* ⅓ faulty can trick ⅔ honest into disagreement due to network timeout

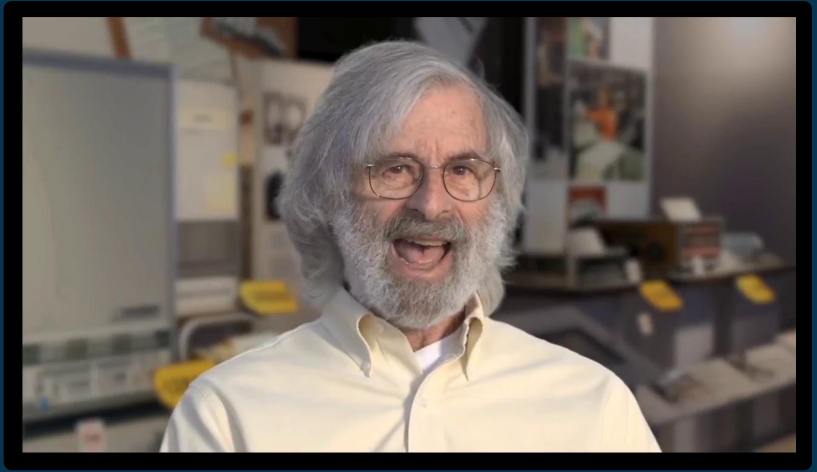
Classical BFT consensus ~1980s

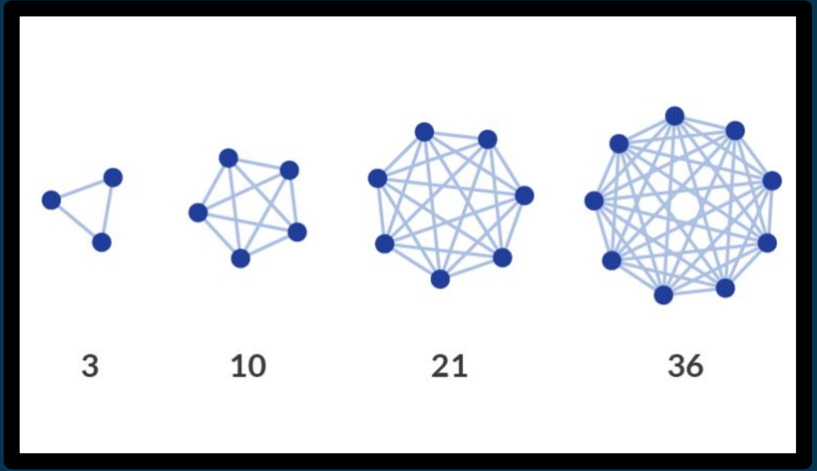
The Byzantine Generals Problem
Lamport et al. formalized consensus

Permissioned setting

No scale because of high communication complexity 😔

*Solana, Polygon, Cosmos, Sui/Aptos, Ethereum FFG





Nakamoto Consensus ~2010

Invented by a pseudonymous nerd on the internet

- Relaxed assumptions
- Changed voting structure for sybil resistance and scaling

*Bitcoin, Ethereum, Cardano, etc

Nakamoto’s Breakthrough - Voting Structure

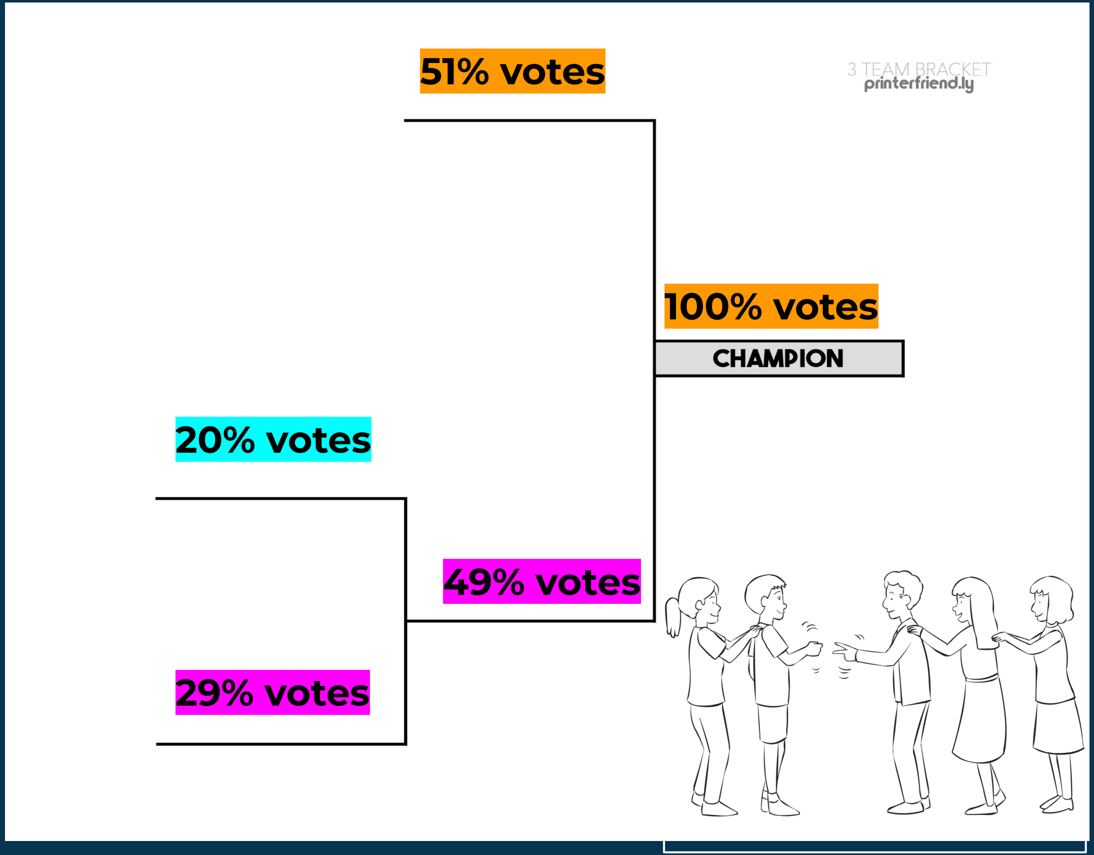
Can’t authenticate humans!
Vote w/ resources

*PoW = compute (hashing!)
*PoS = Staked collateral

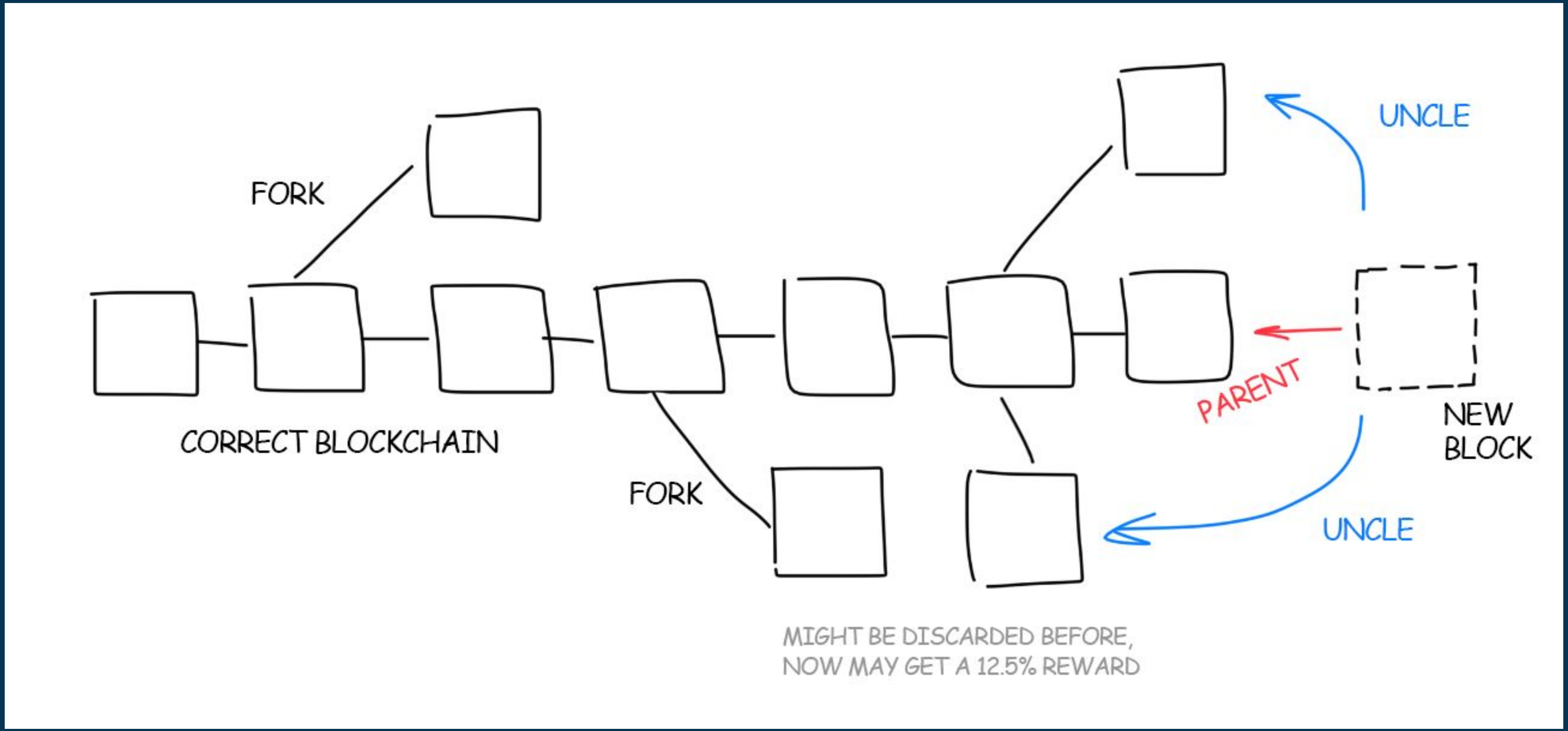
Fork choice = Longest Chain

Breakthroughs:

1. Permissionless participation
2. Node participation doesn’t affect performance 😄



Large block times for Synchrony!



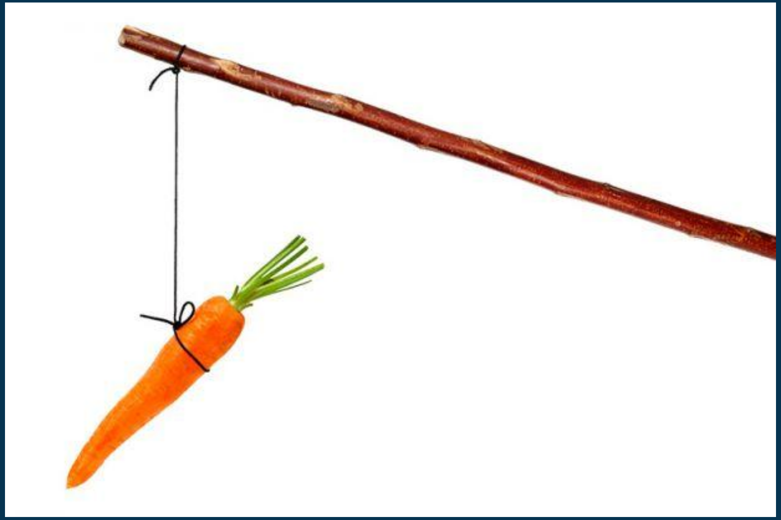
Carrots and Sticks (Incentives)

	Carrot	Stick	Full node punishment
PoW	tx fees + inflation	Mining on wrong chain incurs electricity costs & no carrots	Miners misbehaving, can remove voting power by changing hash function (makes mining equipment obsolete) !!Removes voting power of all miners!!
PoS	tx fees + inflation	Voting on wrong chain causes collateral to be slashed & no carrots	Validators misbehaving, can remove voting power of individual validators by slashing

*Game theory (cryptoeconomics) is very important for blockchains since haters can join!
**Must convince people that the inflation is valuable for 🥕 to work!

Takeaways

1. Voting structure of NC was a breakthrough -> humongous & permissionless networks
2. Incentive alignment important!
3. Consensus is a rich and complex field! (click here)



Oregon Blockchain

Mechanism 3: State Machine

State? Machine?

- State = snapshot (accounts, balances, etc)

  *Maintained in giant data structure known as Merkle tree

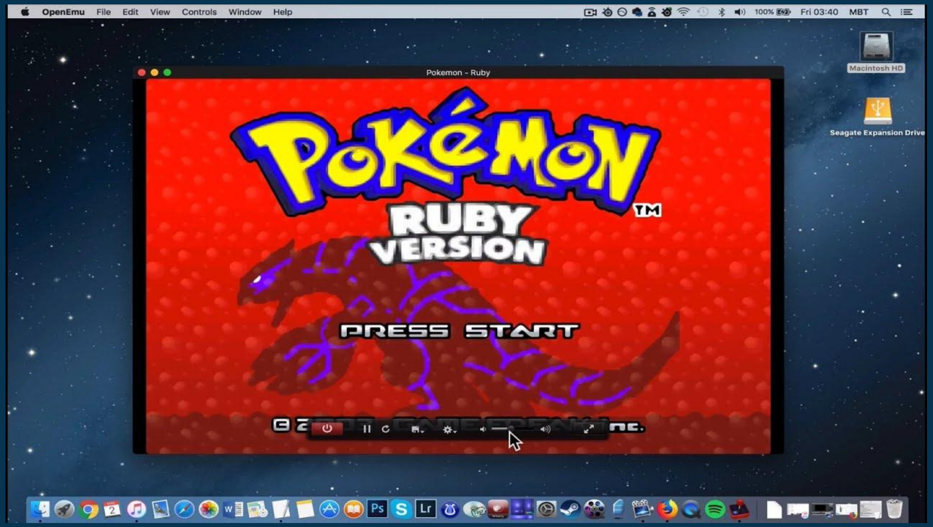
  (Invented by OG cryptographer from last week using hashing!)

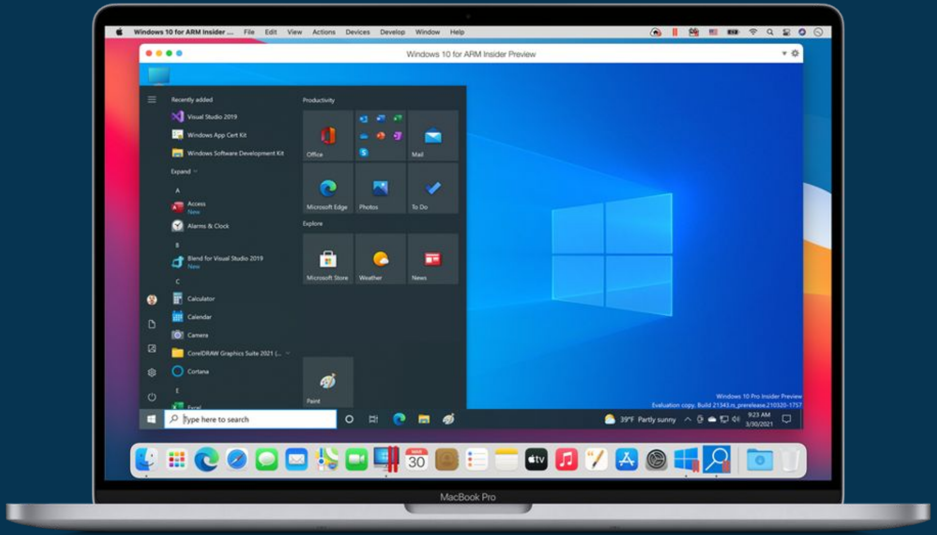
- Consensus (mech. 2) only orders transactions, state built by running txs sequentially
- Full nodes enforce state transitions are valid

Virtual Machines... halting problem

Virtual machines define what changes to state can be made

Let you run fake computer on real computer!





Why blockchain VMs

Metering - pay fee based on # of opcodes you use

Makes outputs deterministic - consensus 😄

Turing complete - compute only limited by cost

Ethereum Virtual Machine (EVM)

Higher level language - Vyper
High level language - Solidity
Low level language - Yul
Assembly code - opcodes
Bytecode (0s & 1s)
Instruction set ('fake' hardware)

VMs are the developers playgrounds

Defines what language they code in

- Compatibility/toolchain/community!

Stuck in a bad playground?

- transpilers (high level -> high level)
- compilers (Custom VMs)

Takeaways

Virtual Machines are Crazy

What did we learn today?

How blockchains work!

Social consensus formed by users (mech. 1)
Technical consensus formed by protocol (mech. 2)
What you can do is defined by state machine (mech. 3)

Onboarding Checklist

- ✅ Week 1: Introductions
- ✅ Week2: What blockchains solve
- ✅ Week3: How a blockchain works
- Week4: How to use a blockchain
- Week5: Social layer

Run a node! Post screenshot in discord when you get it up and running

15 minutes of twitter

you wanna read a book so bad
you wanna develop critical thinking skills
ifunny.co