

# CSBC2000

Week 1 | Class 2

Distributed Ledger Technology as an  
Abstraction of Blockchain



# Recap

- Bitcoin is a cryptocurrency, backed by a distributed ledger
- The Bitcoin blockchain uses PoW consensus
- Miners are incentivized to maintain the ledger by miner fees + block rewards (as long as they last)
- Blockchains can be controlled by miner(s) who have more hashing power than the rest of the network

# This class

- We'll look at the blockchain as a *state machine*
- Understand quirks of the Ethereum ecosystem
- More consensus models
- Separate DLT from blockchain

# Ethereum

- Ethereum was developed by Vitalik Buterin in 2013 with a goal of building decentralized applications
- Buterin argued that Bitcoin and blockchain could benefit from other applications besides money and needed a scripting language for application development that could lead to attaching real-world assets, such as stocks and property, to the blockchain.

# State

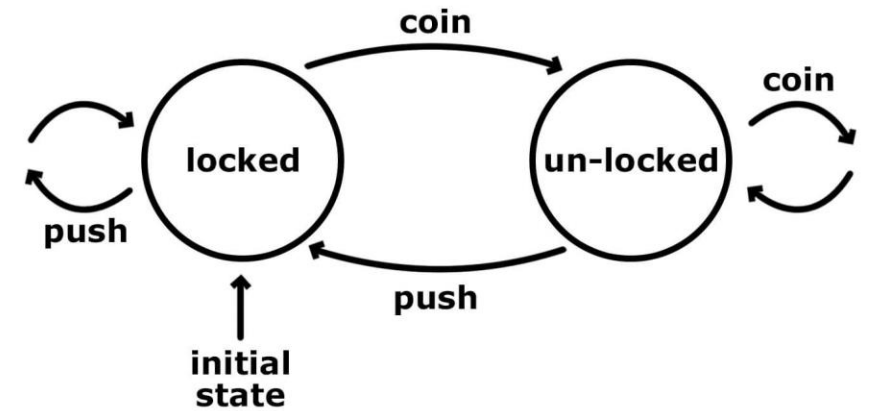
- A program's state is the collection of events and interactions during the program lifecycle that it stores in some retrievable format
- To bring this to blockchain, the transaction data that is stored on the ledger is the *state* of the ledger
- Ethereum Whitepaper (2013): "The "state" in Bitcoin is the collection of all coins (technically, "unspent transaction outputs" or UTXO) that have been mined and not yet spent, with each UTXO having a denomination and an owner"

# State

- Vitalik wanted a blockchain that took the concept of state more generally
- Specifically, he wanted for the blockchain state to store arbitrary information
- This way, one could run an app that stores crucial state information on the blockchain as opposed to just UTXO information

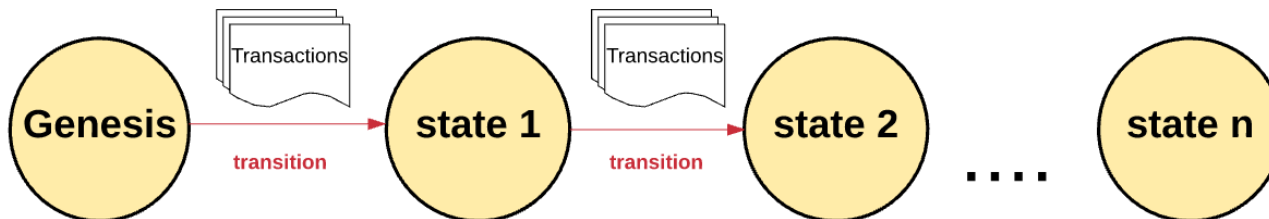
# State Machine

- A state machine describes the lifecycle of a system by defining every possible state it can have (based on its variables) as well as every possible state transition



# State Machine

- The Ethereum state machine operates with this underlying principle
- The Genesis block is hence equivalent to a blank state
- Anyone can deploy applications that write content to the Ethereum blockchain, represented as transactions





# The Ethereum Virtual Machine

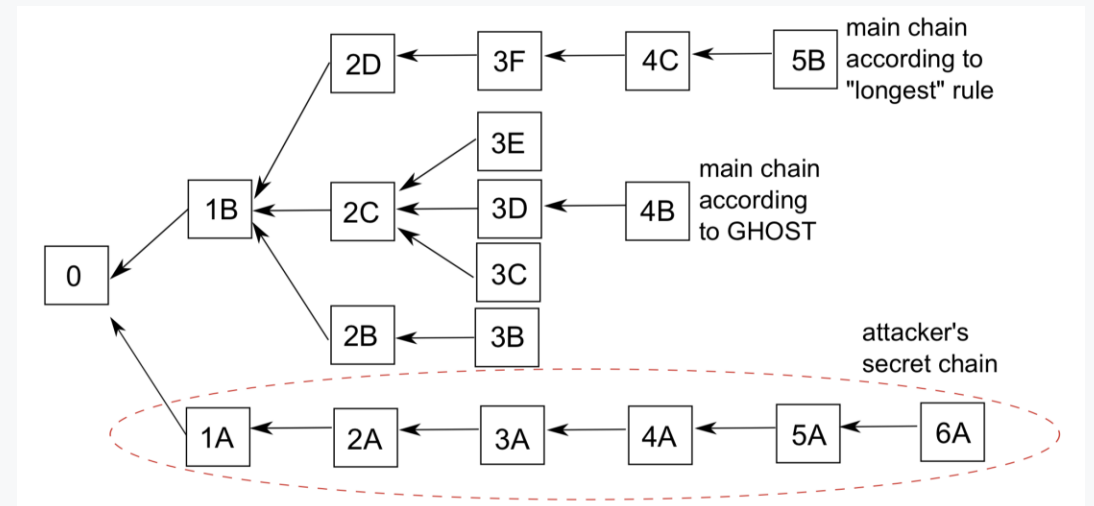
- We have developed this concept of the Ethereum state machine, it is formally known as the EVM
- It is a "Virtual Machine" as the Ethereum state machine has its own opcodes (just like x86 and ARM/RISC-V)
- This is because apps write arbitrary data onto the Ethereum blockchain, we need a common data format

# Smart Contracts

- You might have heard of the term smart contract in blockchain; this is actually just an EVM state transition!
- Since we have a Virtual Machine with its own bytecode, apps need to convert instructions that they want on the blockchain
- That's why Ethereum developers created a new language: Solidity
- You can describe the logic of "on-chain" state and state transitions using this abstract language
  - This gets compiled into EVM opcodes so that they can modify the EVM state
- More to come on Thursday

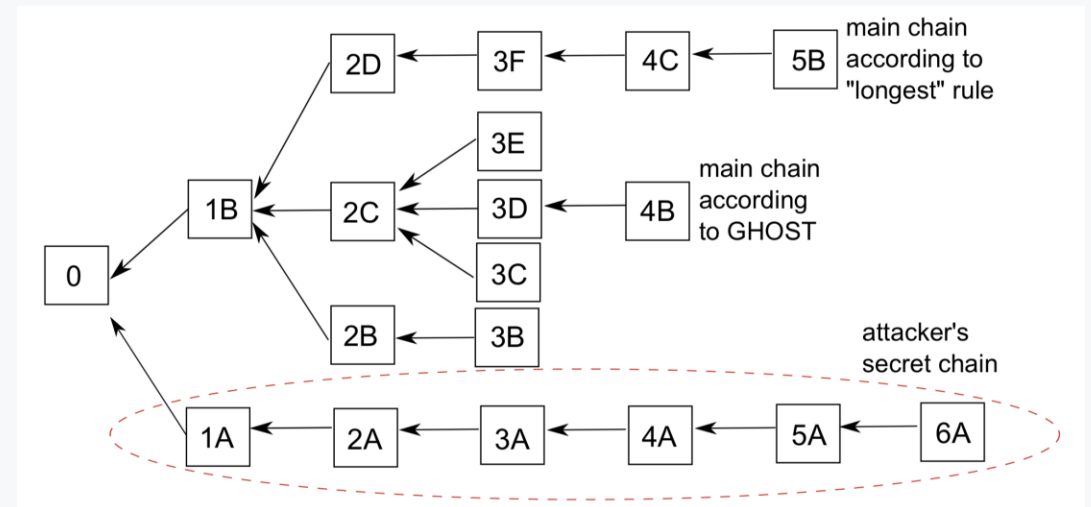
# Ethereum Consensus: GHOST

- "Greedy Heaviest Observed Subtree" • Still Proof of Work!
- Lots of wasted computation in BTC blockchain
  - Ethereum Whitepaper (2013): "if miner A mines a block and then miner B happens to mine another block before miner A's block propagates to B, miner B's block will end up wasted and will not contribute to network security"



# Ethereum Consensus: GHOST

- Eth WP: "GHOST solves the first issue of network security loss by including stale blocks in the calculation of which chain is the "longest"; that is to say, not just the parent and further ancestors of a block, but also the stale descendants of the block's ancestor (in Ethereum jargon, "uncles") are added to the calculation of which block has the largest total proof of work backing it"
- Further, the "uncle" and "nephew" blocks also receive a portion of the block reward



# Gas Costs

- Storing data on the blockchain is expensive
  - Big computational cost for PoW
  - Data is immutable, stored forever
- Every opcode incurred in a state transition of the EVM has a cost represented by "gas"
  - 1 opcode is roughly 1 gas
  - Gas prices are denoted in Gwei, which itself is a denomination of ETH - each Gwei is equal to 0.000000001 ETH ( $10^{-9}$  ETH).

# Gas Costs

- In blockchains, the miner fee scales with the size of data intended to be stored on the ledger
- As a result, large data (e.g. files) are not directly stored on the blockchain. Rather, a hash is stored on the chain and the data is stored in an immutable, highly available content storage (e.g. Ethereum Swarm) which is typically decentralized

# Cons of PoW

- PoW is highly computationally expensive, hence terrible for the environment
- Another pitfall is that it can be quite insecure; with small networks it can (and has been multiple times) be exploited via a 51% attack


Comment | Published: 29 October 2018

## Bitcoin emissions alone could push global warming above 2°C

Camilo Mora , Randi L. Rollins, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada & Erik C. Franklin





*Nature Climate Change* **8**, 931–933(2018) | [Cite this article](#)


7461 Accesses | 52 Citations | 2625 Altmetric | [Metrics](#)

**COINTELEGRAPH**  
The future of money

BTC	ETH	LTC	XRP
\$38,854	\$1,615	\$150.48	\$0.43
+0.73%	-0.14%	-0.56%	-0.56%



News ▾ Markets ▾ Magazine People ▾ Cryptopedia ▾ Industry ▾ Consult ▾

    **Get more when you invest in crypto.** We've got a sp

 JACK MARTIN JAN 27, 2020

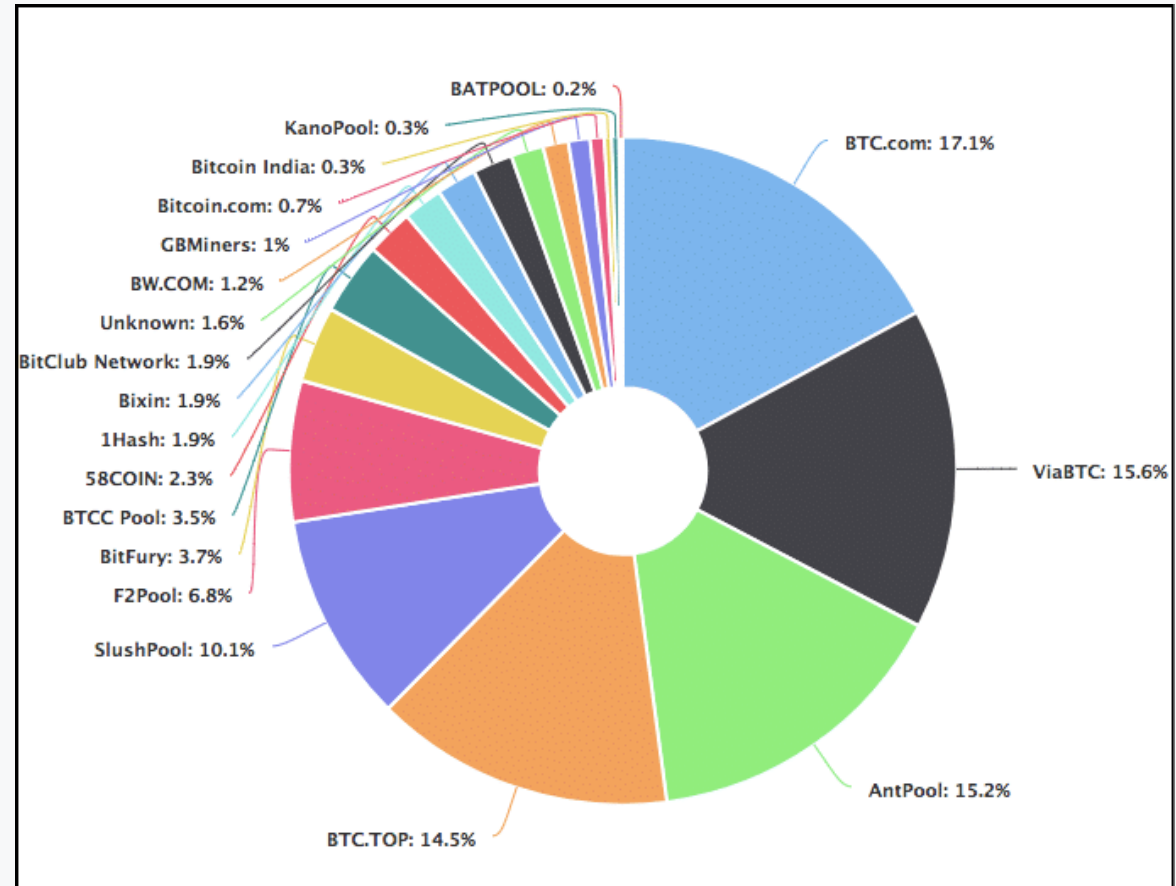
### Bitcoin Gold Blockchain Hit by 51% Attack Leading to \$70K Double Spend

The Bitcoin Gold blockchain suffered a second 51% attack in two years, leading to \$70,000 worth of BTG being double spent.

7678 Total views 229 Total shares [Listen to article](#)   2:44

# Cons of PoW

- Plus, it's not really that decentralized





# Proof of Stake

- Proof of Stake serves as a simple modification over PoW that solves these problems
- PoS allows for miners to get a block reward proportional to the amount of currency that they already own
- 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.
- More hashing power != more mining rewards

# Ethereum 2.0: Casper the Friendly GHOST

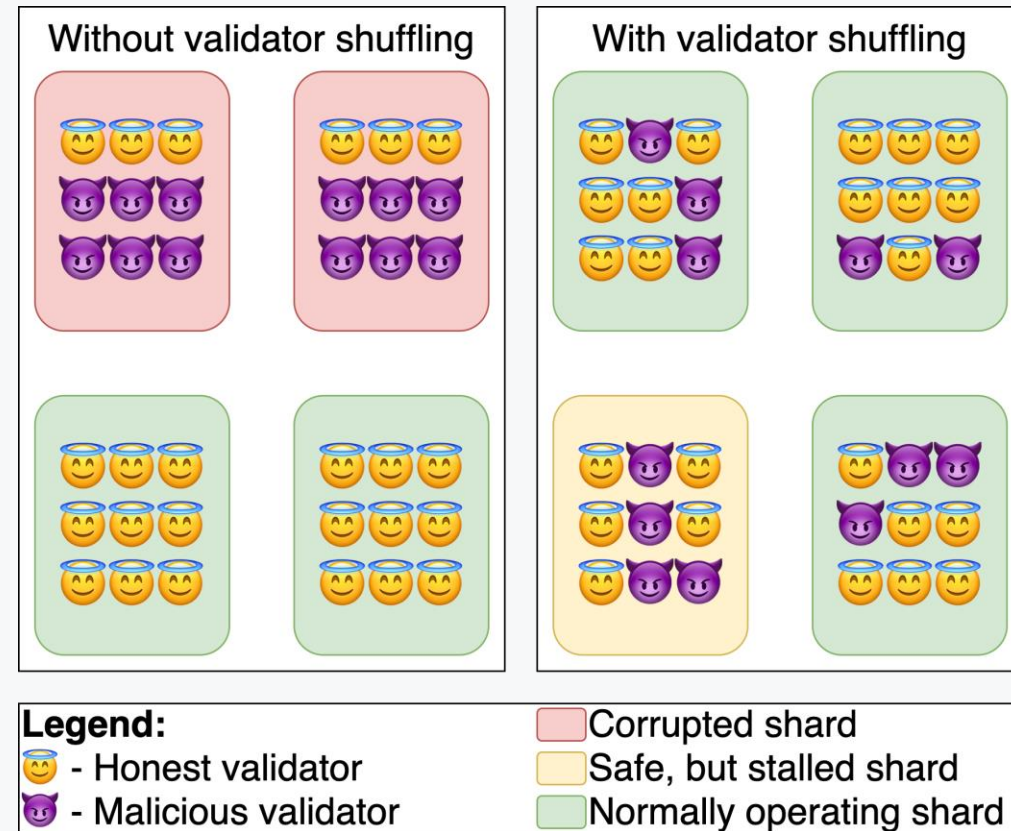
- In Ethereum's Proof-of-Stake, the concept of mining is done away with
- Instead, Ether holders who are running a validator node are able to place bets with their Ether
- Each bet represents which block they think will be mined next
- If their bet is correct, they get their stake back plus the block reward
- If they are incorrect, they just get their stake back
- This new system is called the "Beacon Chain"

# Nothing at Stake Problem

- However, validators do not have anything at stake when the network forks; they can simply bet on all the forked chains since they have no incentive mechanism to choose
- Some versions of Casper punish users who engage in such behaviour as it can lead to lack of protection against double spend
- Casper is still in development and the rollout is an ongoing process

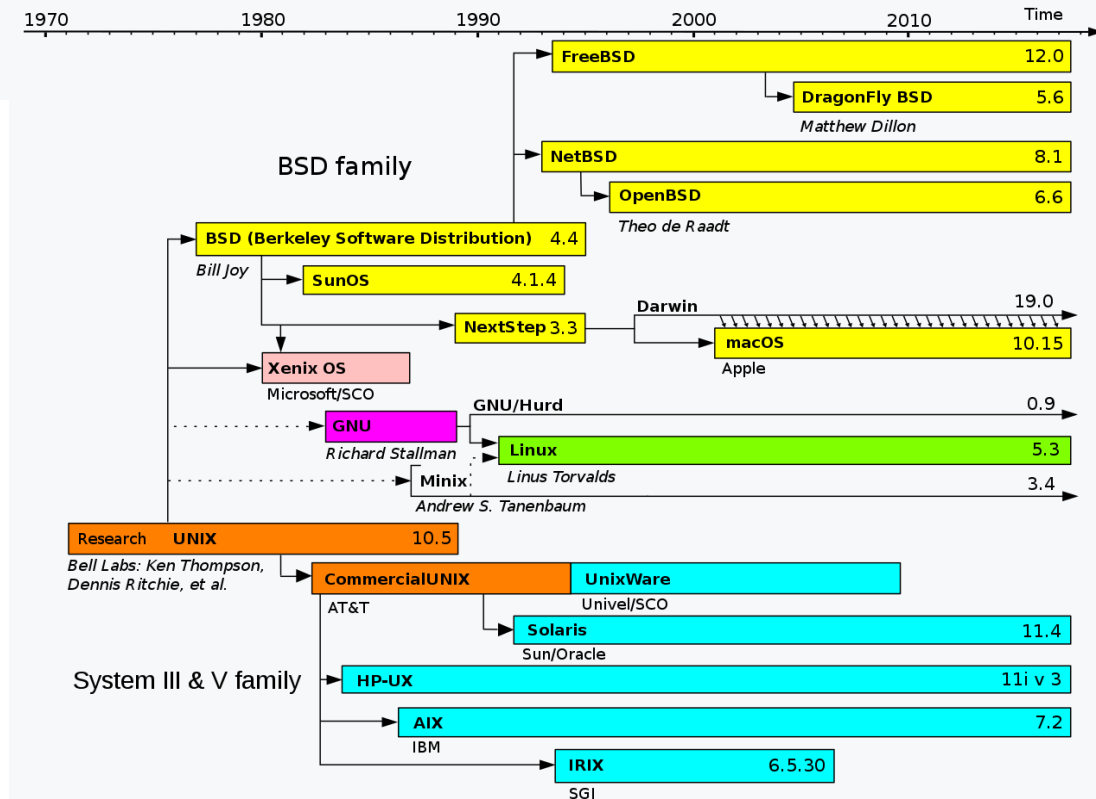
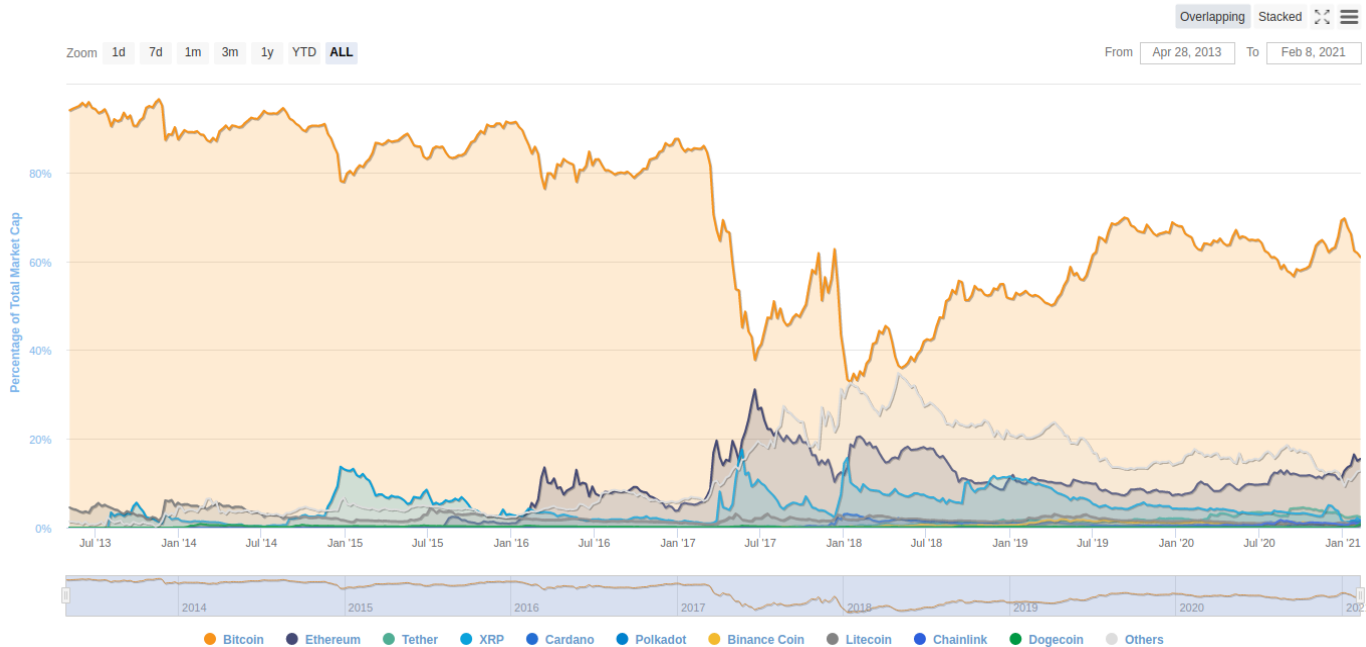
# Validator Shuffling

- Validators can be malicious; the Beacon Chain protects against this by assigning validators to committees
- Committees make decisions on blocks and Casper ensures that all validators are randomly distributed in such a way that "committees are more or less an accurate statistical representation of the overall validator set"



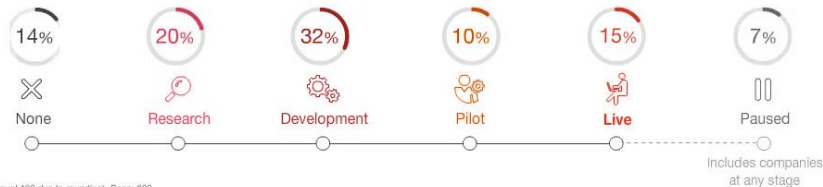
# Blockchain Wars

Percentage of Total Market Capitalization (Dominance)



# Blockchain Wars

## How far along are companies with blockchain?



Note: Numbers are rounded (sum does not equal 100 due to rounding). Base: 600.  
Q: How would you describe your organisation's current involvement with blockchain?  
Source: PwC Global Blockchain survey, 2018

statista

Search Statistics

Prices & Access

Statistics

Reports

Outlooks

Tools

Infographics

Services

Global Survey

NEW



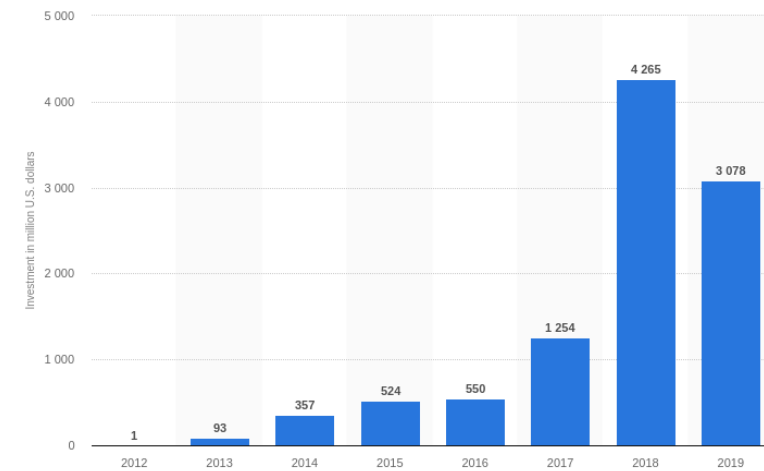
Login

Technology & Telecommunications > Software

PREMIUM

## Equity funding and investment of blockchain startup companies worldwide from 2012 to 2019

(in million U.S. dollars)



© Statista 2021

Additional Information

Show source

### DOWNLOAD



### Sources

Show sources information

Show publisher information

### Release date

January 2020

### Region

Worldwide

### Survey time period

2012 to 2019

### Supplementary notes

2017 to 2019 figures were calculated by Statista by adding up quarterly figures provided by the source.

# Other Consensus Models

- DPoS
- PoST
- Iota
- Avalanche
- Tendermint
- ...

# Delegated PoS

## Electing witnesses in a Delegated Proof-of-Stake network

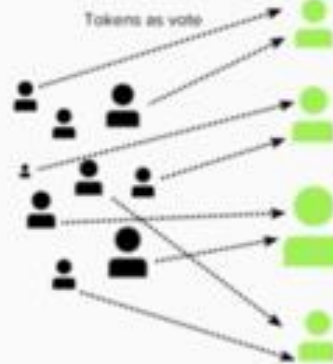
nichanank.com

1.



Nodes express interest in becoming a witness and begin lobbying, making positive contributions to the network and engaging the community.

2.



People in the network allocate their tokens as **votes** for witnesses

The more tokens they have, the higher their voting weight - hence *proof of stake*\*

3.

### Witness

1.	0x912x9x8a90...
2.	0x2as9d8fais...
3.	0x8aust240...
4.	0x9240sfak3...
5.	0x9028408zdf...
...	
	0x98sfa...
	0x9028408zdf...
	0xa982402...

\*These are wallet addresses owned by individual witnesses. Can think of them as an ID number to identify nodes.

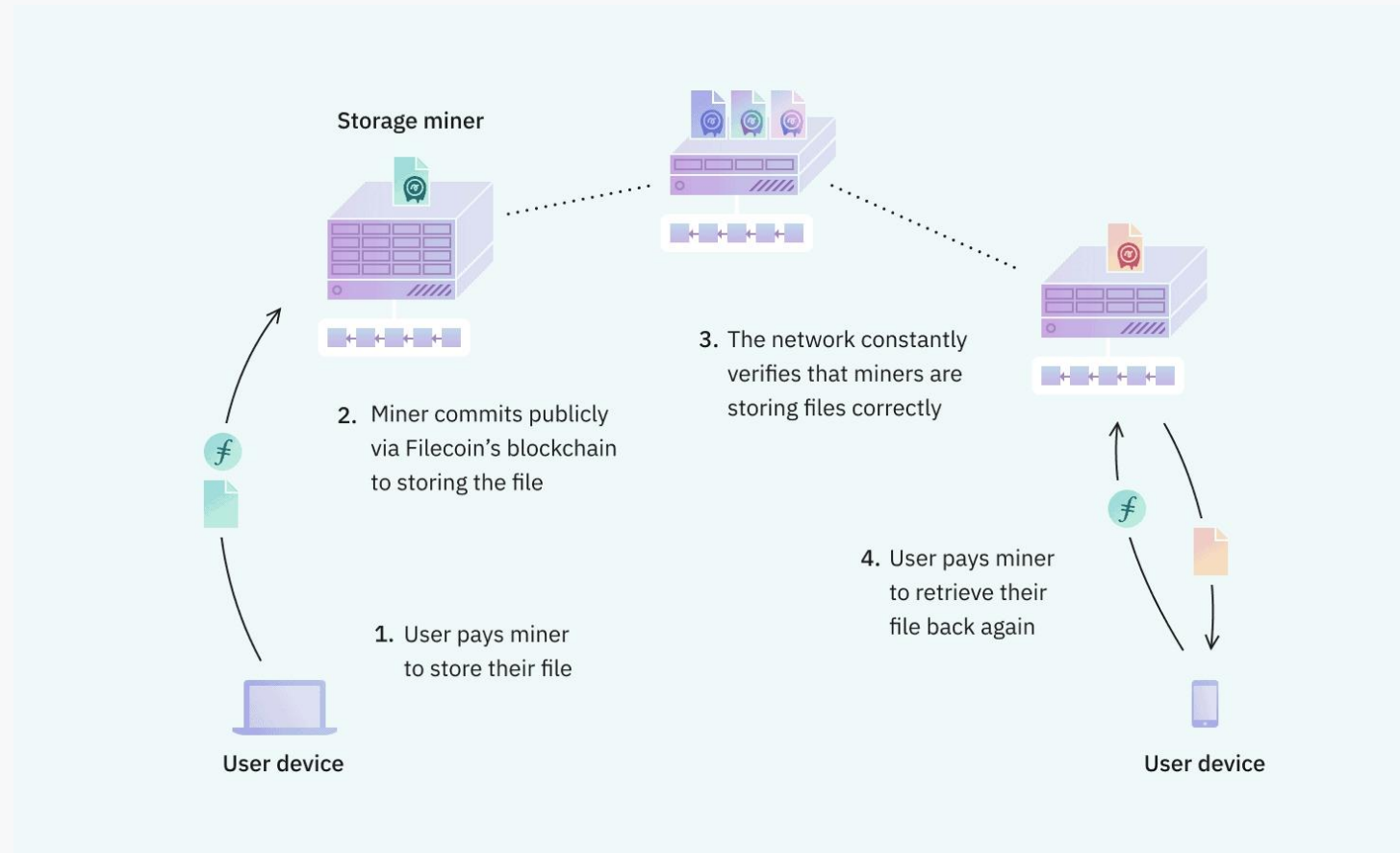
We end up with a ranking of nodes with the most votes (# tokens allocated to them).

The top N of these will become members of the elected witness panel. N depends on the network.

\*Participants are NOT giving tokens to their witnesses. They are merely allocating funds to their choices as an expression of their vote. They can reassign their tokens to another witness at any time.



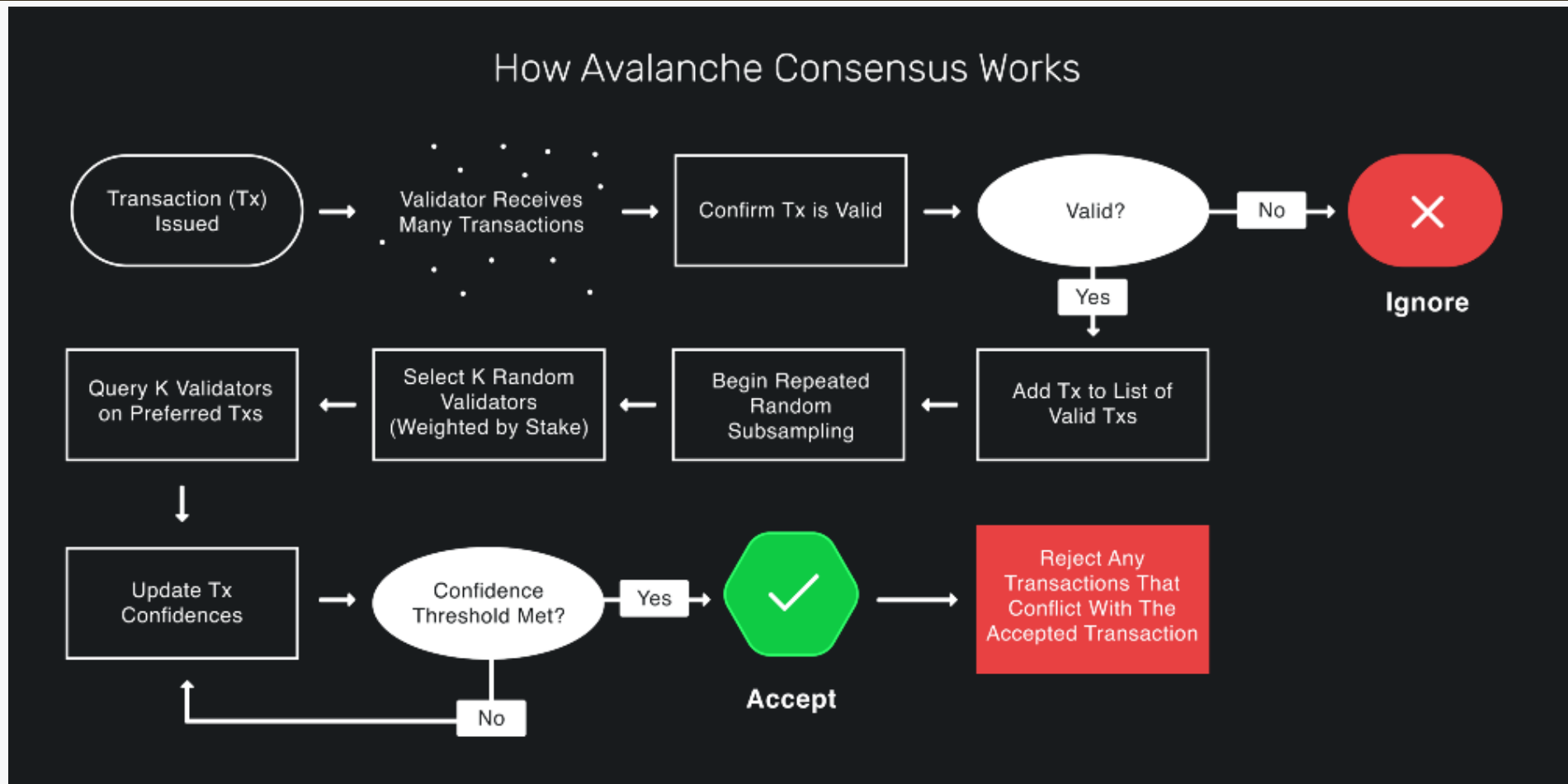
# Proof-of-Spacetime



# Proof-of-Spacetime

- "The idea of proof-of-capacity is to require network participants to demonstrate a financial interest in the success of the network by allocating some form of memory or disk space towards it"
- Miners have to "seal" data that enters the network and periodically have to "prove" they have the data

# Avalanche

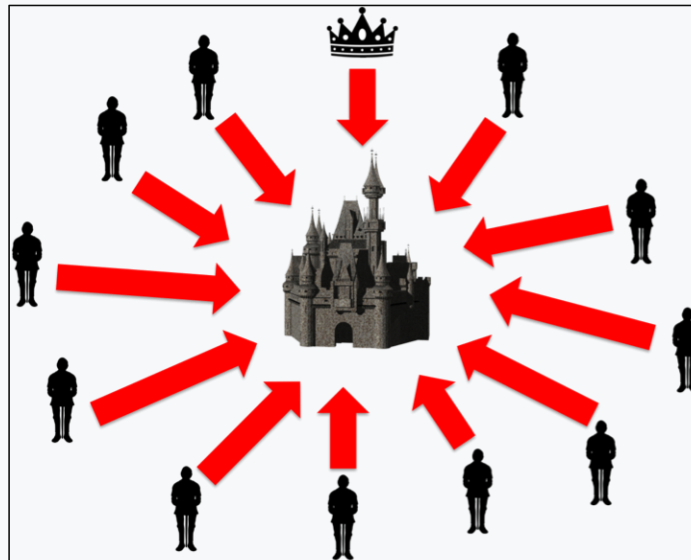


# Tendermint

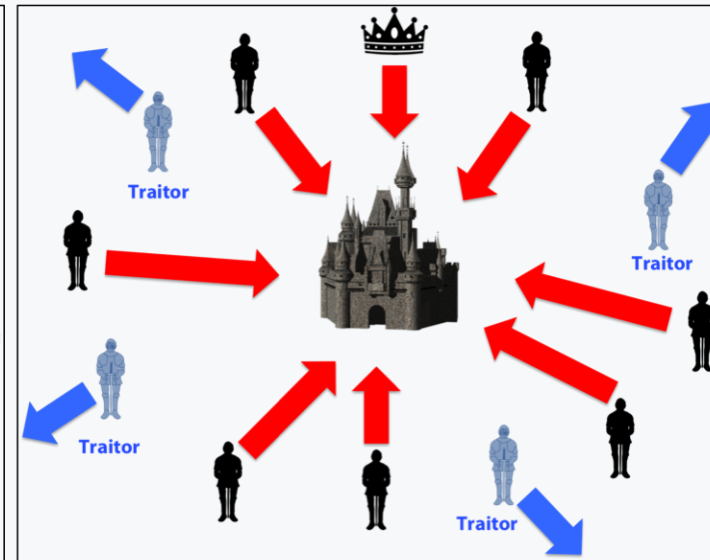
- Tendermint is software for securely and consistently replicating an application on many machine
  - works even if up to  $1/3$  of machines fail in arbitrary ways
  - every non-faulty machine sees the same transaction log and computes the same state
- The ability to tolerate machines failing in arbitrary ways, including becoming malicious, is known as Byzantine fault tolerance (BFT)
- BFT theory is pretty old (late 1970s)
- Blockchain technology is just a reformalization of BFT in a more modern setting

# Byzantine Generals Problem

- Coordination required for system to work



**Coordinated Attack Leading to Victory**



**Uncoordinated Attack Leading to Defeat**

# Tendermint

- Bitcoin is a cryptocurrency blockchain where each node maintains a fully audited Unspent Transaction Output (UTXO) database. If one wanted to create a Bitcoin-like system on top of ABCI, Tendermint Core would be responsible for
  - Sharing blocks and transactions between nodes
  - Establishing a canonical/immutable order of transactions (the blockchain)
- The application will be responsible for
  - Maintaining the UTXO database
  - Validating cryptographic signatures of transactions
  - Preventing transactions from spending non-existent transactions
  - Allowing clients to query the UTXO database.

**Questions / Comments?**

**Let's code!**