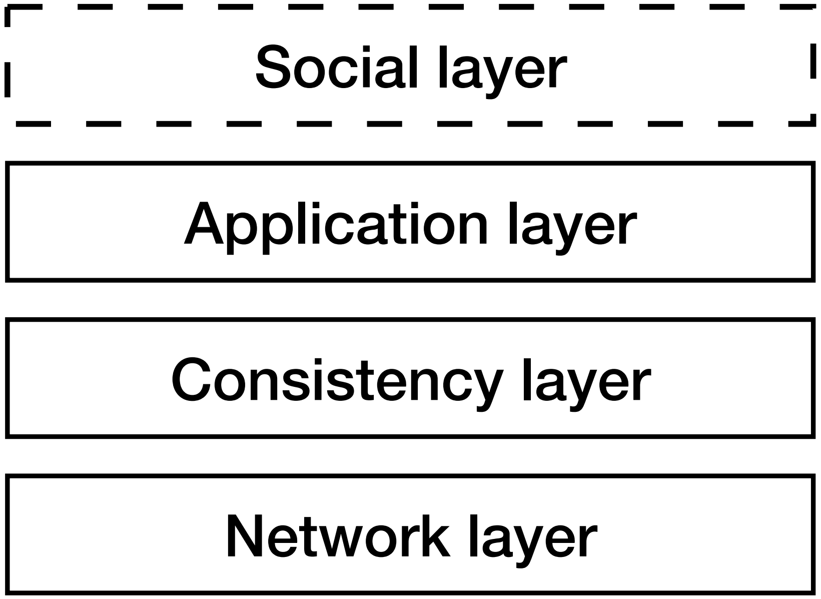
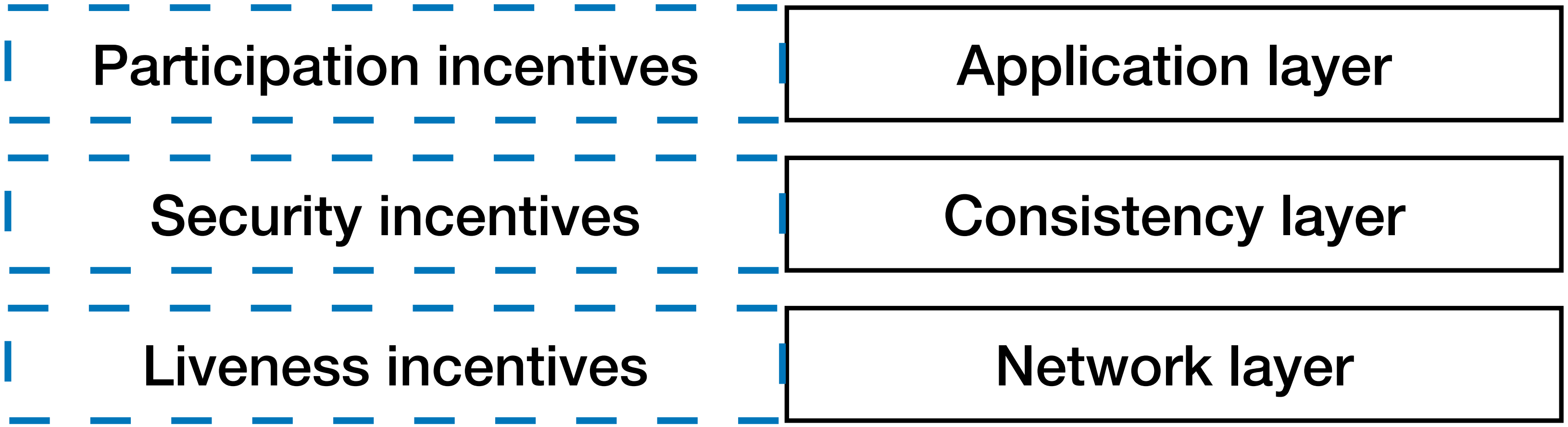
Web3, Tokenomics, and Incentives

Generic model of a distributed system

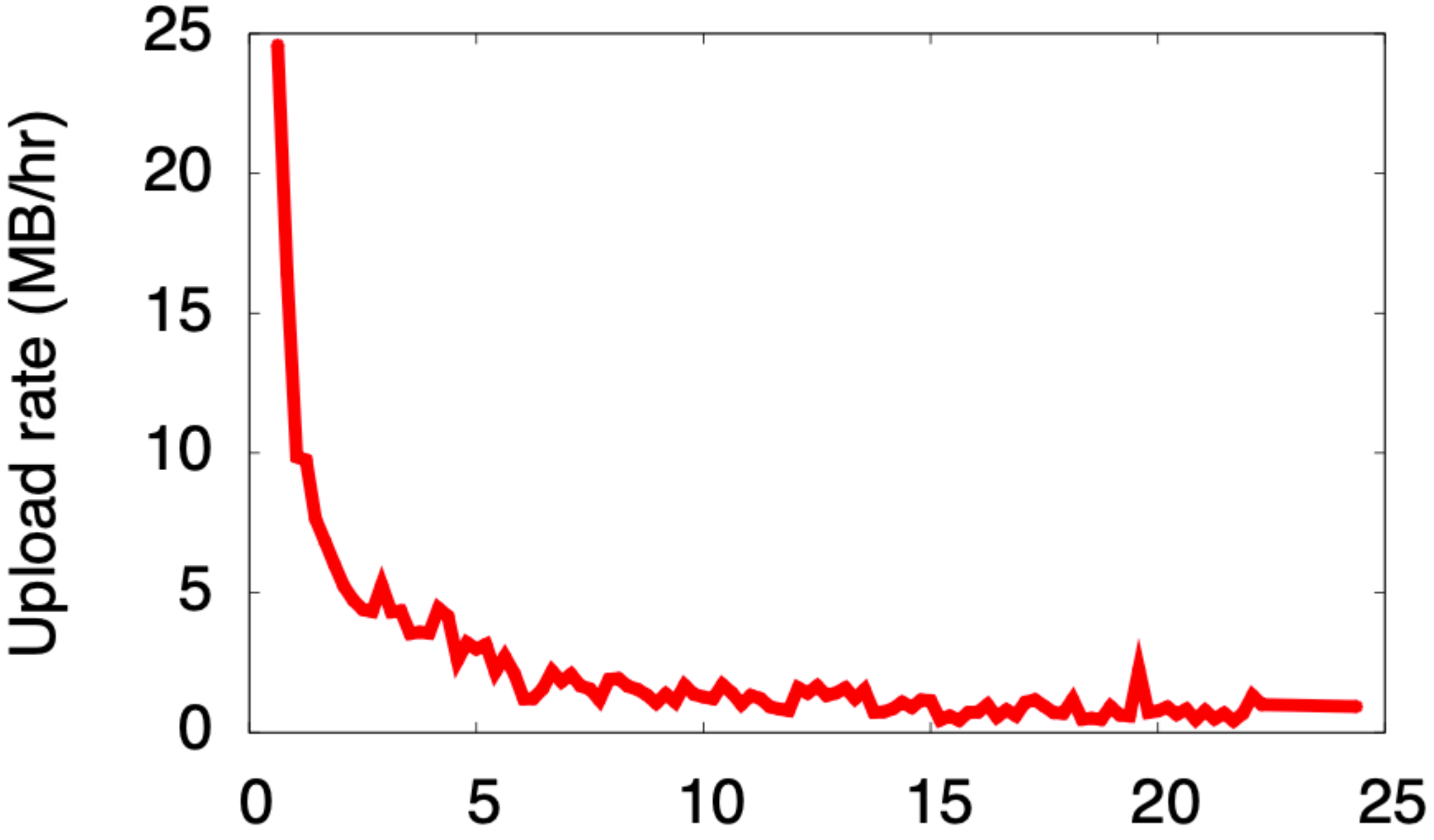


Blockchain model



Participation incentives	Application layer
Security incentives	Consistency layer
Liveness incentives	Network layer

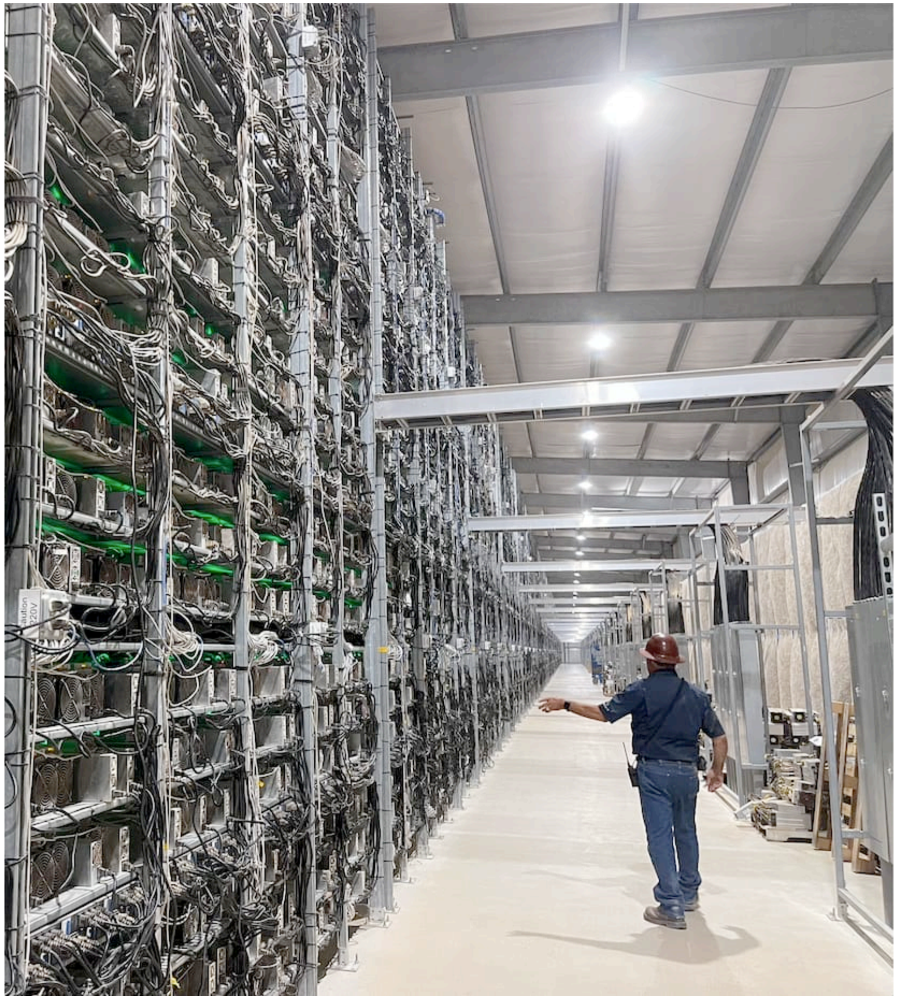
First generation of incentives in P2P Torrents



Why incentives mechanisms in torrents fail

- Supposedly: tit-for-tat
- In fact: managed economy by torrent trackers

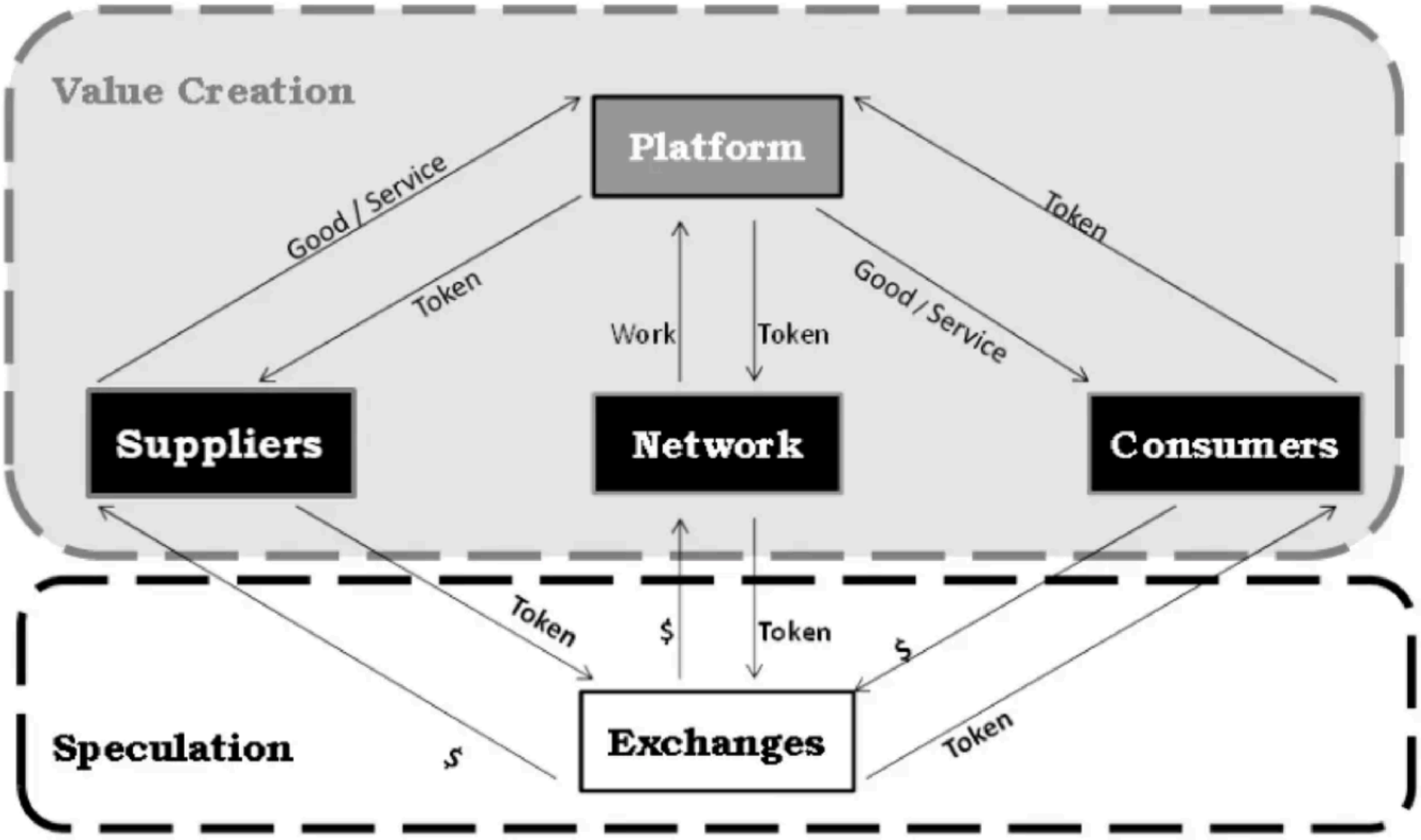
☑ All ☐ Audio ☐ Video ☐ Applications ☐ Games ☐ Other ☐ (search titles only)



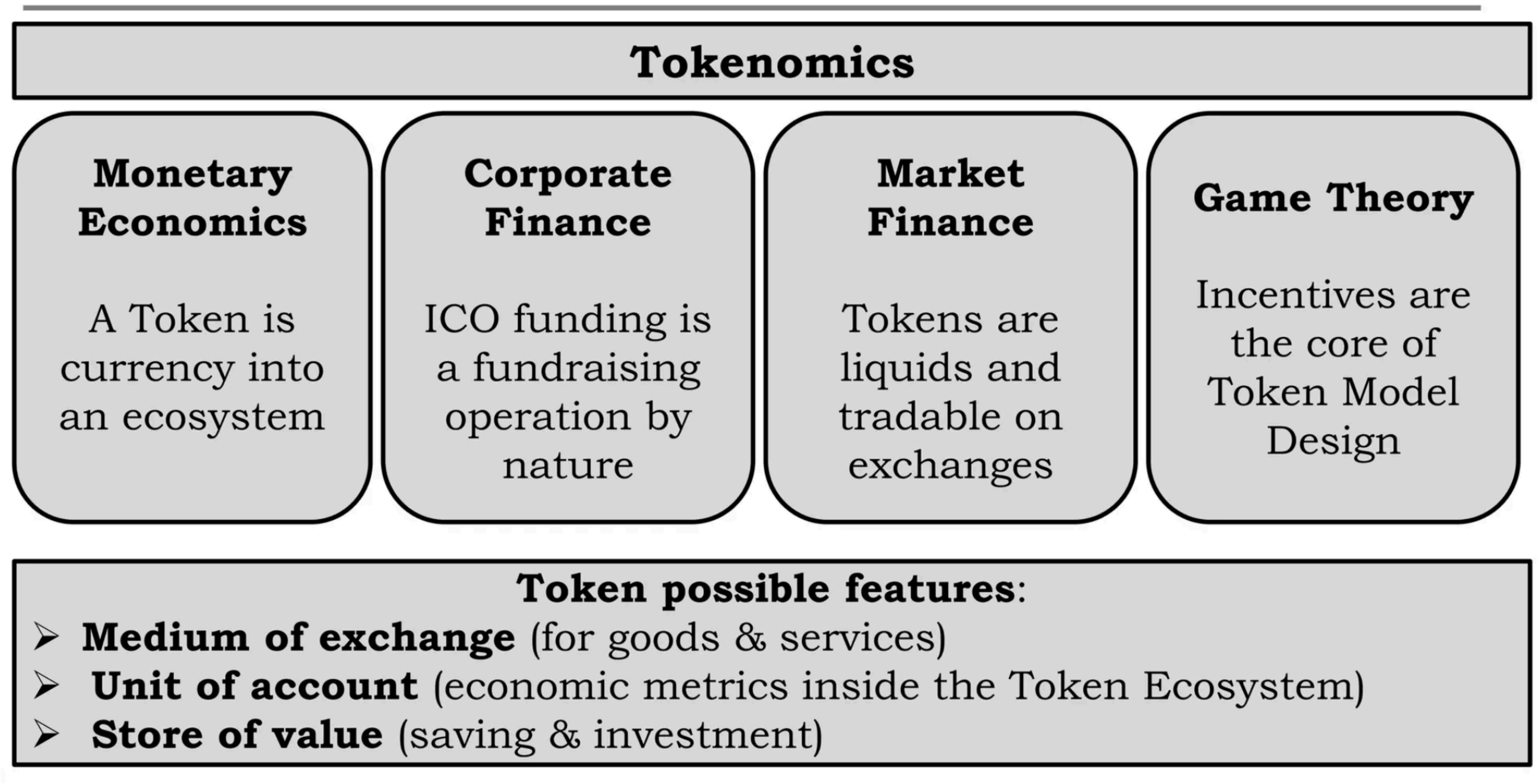
Blockchains

- Scalable incentives
- Incentives engineering
- Decentralised economy

Tokenomics


Value Creation
Platform
Good / Service
Token
Work
Token
Good / Service
Token
Suppliers
Network
Consumers
Token
$
Token
$
Speculation
$
Exchanges
Token

Definition - study of incentiveization in blockchains



Tokenomics

Monetary Economics

A Token is currency into an ecosystem

Corporate Finance

ICO funding is a fundraising operation by nature

Market Finance

Tokens are liquids and tradable on exchanges

Game Theory

Incentives are the core of Token Model Design

Token possible features:

- **Medium of exchange** (for goods & services)
- **Unit of account** (economic metrics inside the Token Ecosystem)
- **Store of value** (saving & investment)

- Game theoretical analysis describes some aspects of Bitcoin mechanisms (To a degree)
- Behaviour of human participants in blockchain system is constrained by the rules of the protocol

"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."
S. Nakamoto

Bitcoin desirable properties

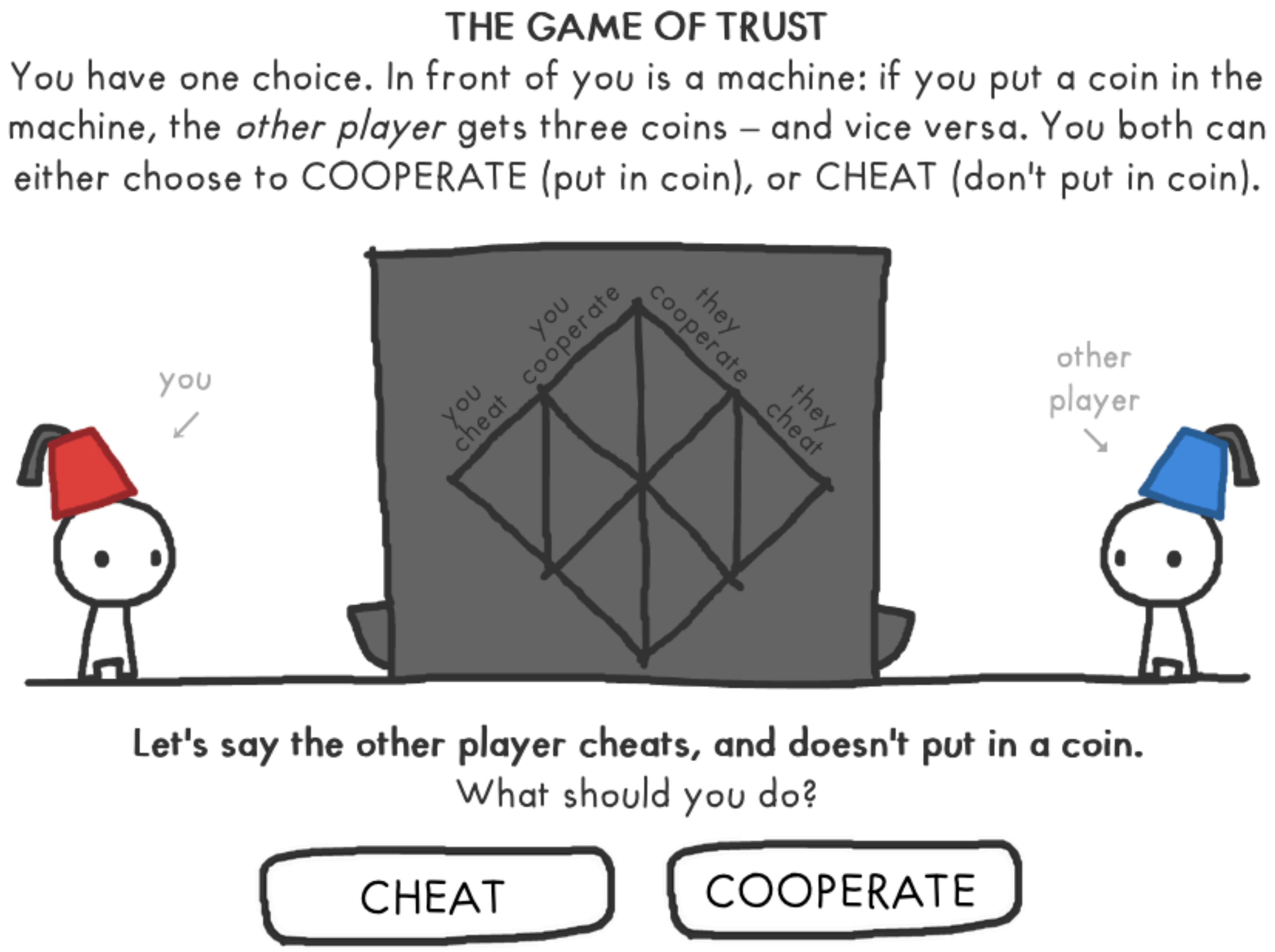
Eventual consistency. At any time, all compliant nodes agree upon a prefix of what will become the eventual “true” blockchain.

Exponential convergence. The probability of a fork of depth n is O(2−n). This gives users high confidence that a simple “k confirmations” rule will ensure their transactions are settled permanently.

Liveness. New blocks will continue to be added and valid transactions with appropriate fees will be included in the blockchain within a reasonable amount of time.

Correctness. All blocks in the chain with the most cumulative proof of work will only include valid transactions.

Fairness. A miner with X% of the network’s total computational power will mine approximately X% of blocks.



THE GAME OF TRUST

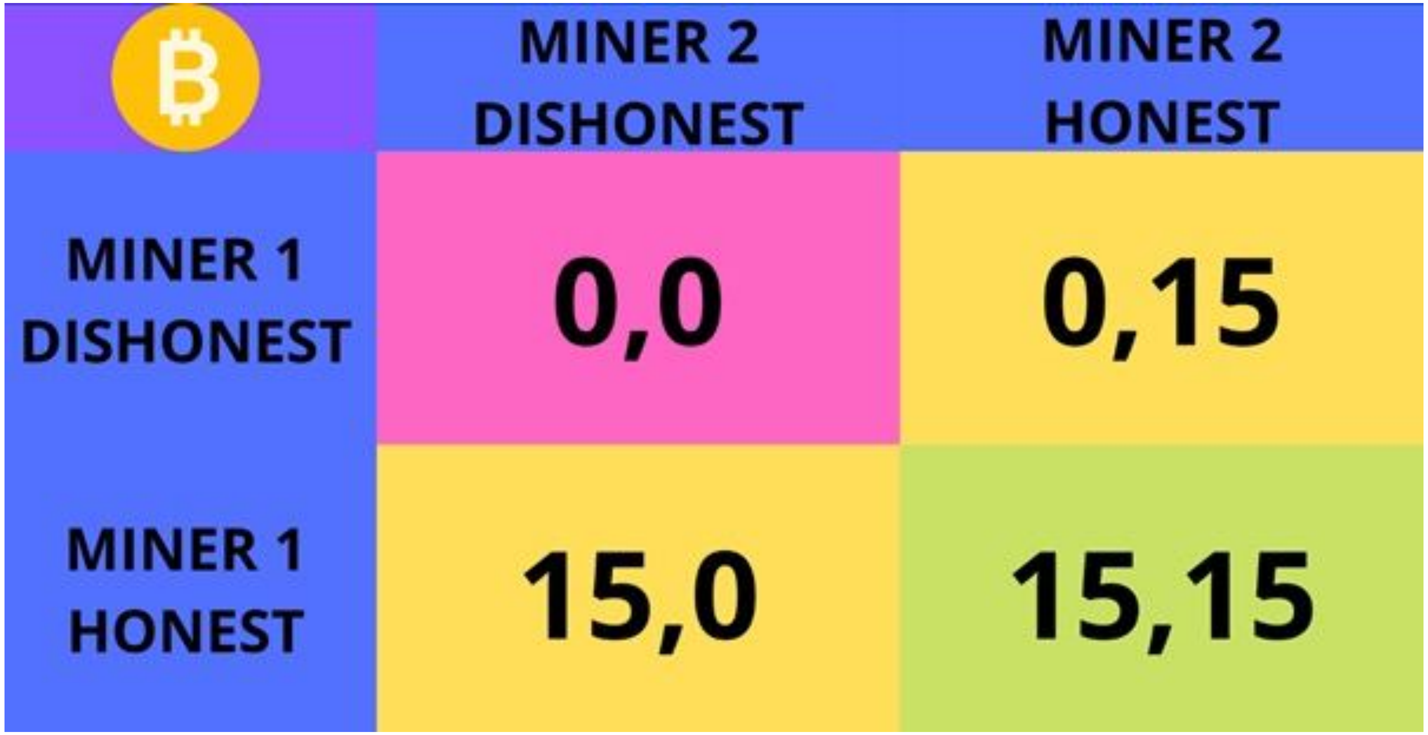
You have one choice. In front of you is a machine: if you put a coin in the machine, the *other player* gets three coins – and vice versa. You both can either choose to COOPERATE (put in coin), or CHEAT (don't put in coin).

Let's say the other player cheats, and doesn't put in a coin.

What should you do?

https://ncase.me/trust/

Game theory in Bitcoin



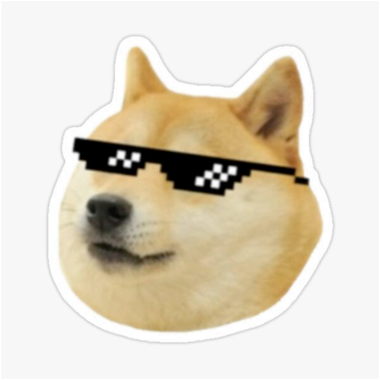
₿	MINER 2 DISHONEST	MINER 2 HONEST
MINER 1 DISHONEST	0,0	0,15
MINER 1 HONEST	15,0	15,15

Bitcoin incentives model

To provide a means for trusted coordination, Blockchains need to provide **incentives**:

(1) for the validators to operate the system (over the alternatives of doing other things, free riding, or misbehaving);

(2) and for users to choose to use the system (over other alternatives of using other systems).



Bitcoin incentives model

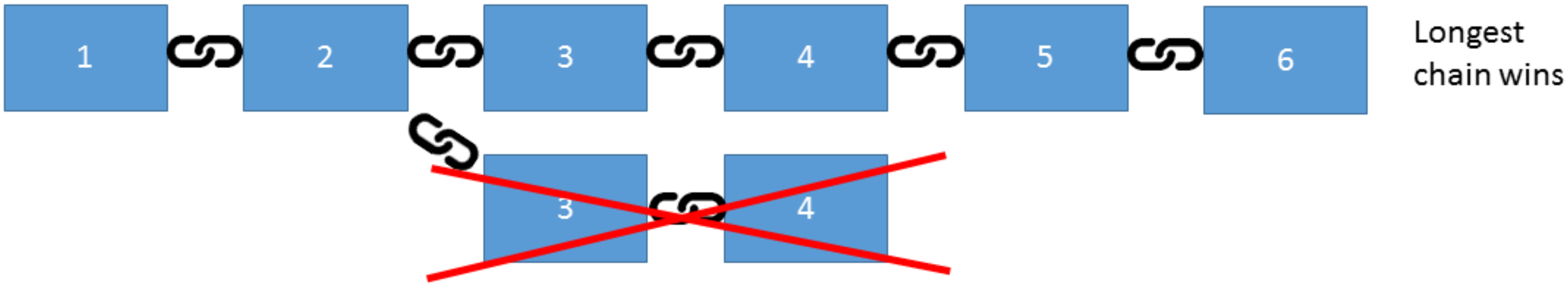
Let’s consider two types of dishonest behaviour:

1) Double-spend attack (client-miner collusion)

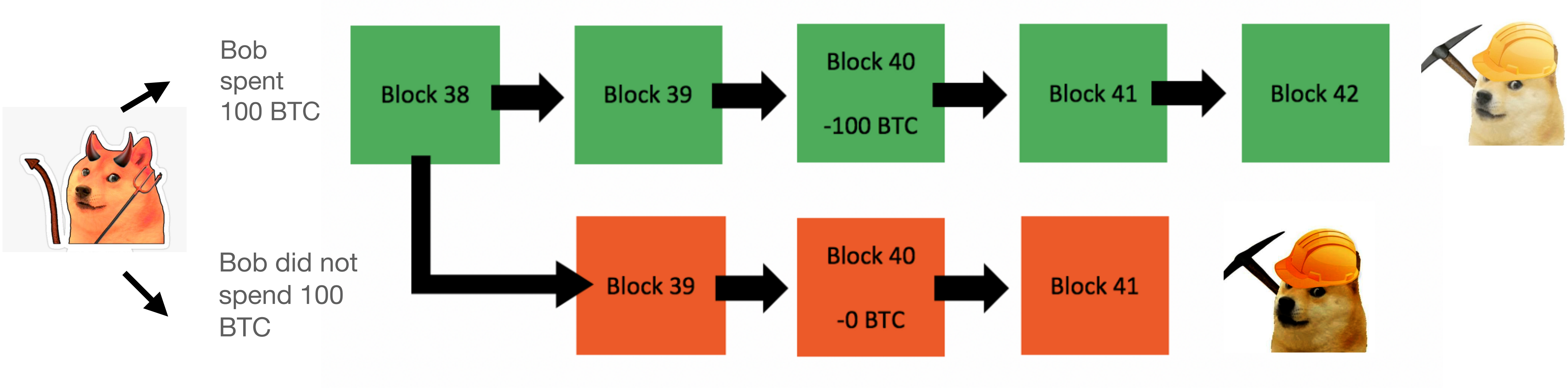
2) Selfish mining (miners collusion)

Longest chain rule

- What if two miners find the same block at (roughly) the same time?
- Now, different miners will build upon different blocks
- Selection rule by miners: **longest chains wins**

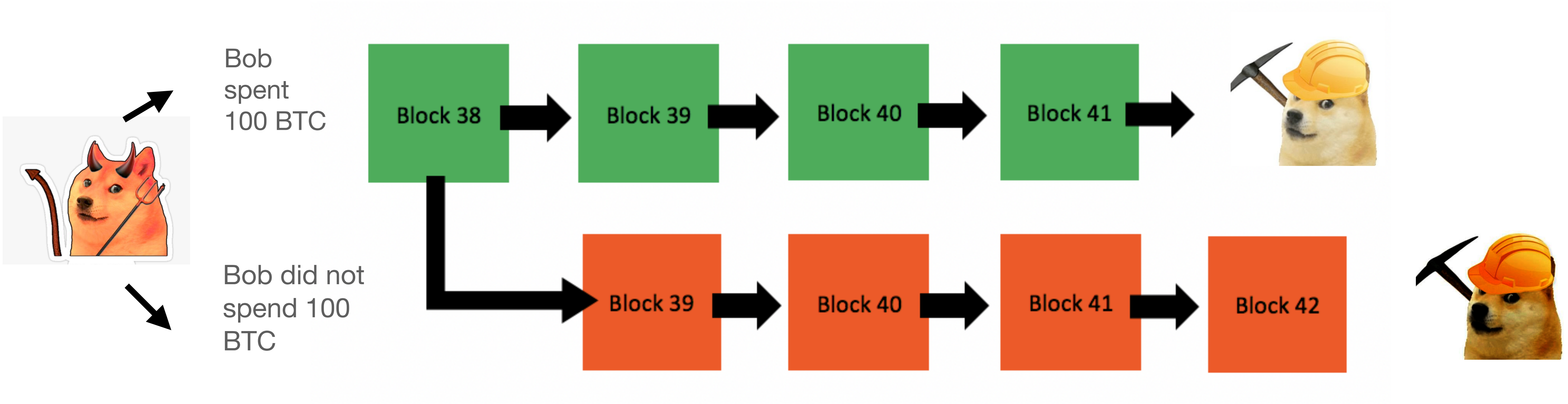


Double-spending attack



1) The valid chain is being extended by honest nodes as green blocks and fraudulent branch is secretly mined by an attacker

Double-spending attack

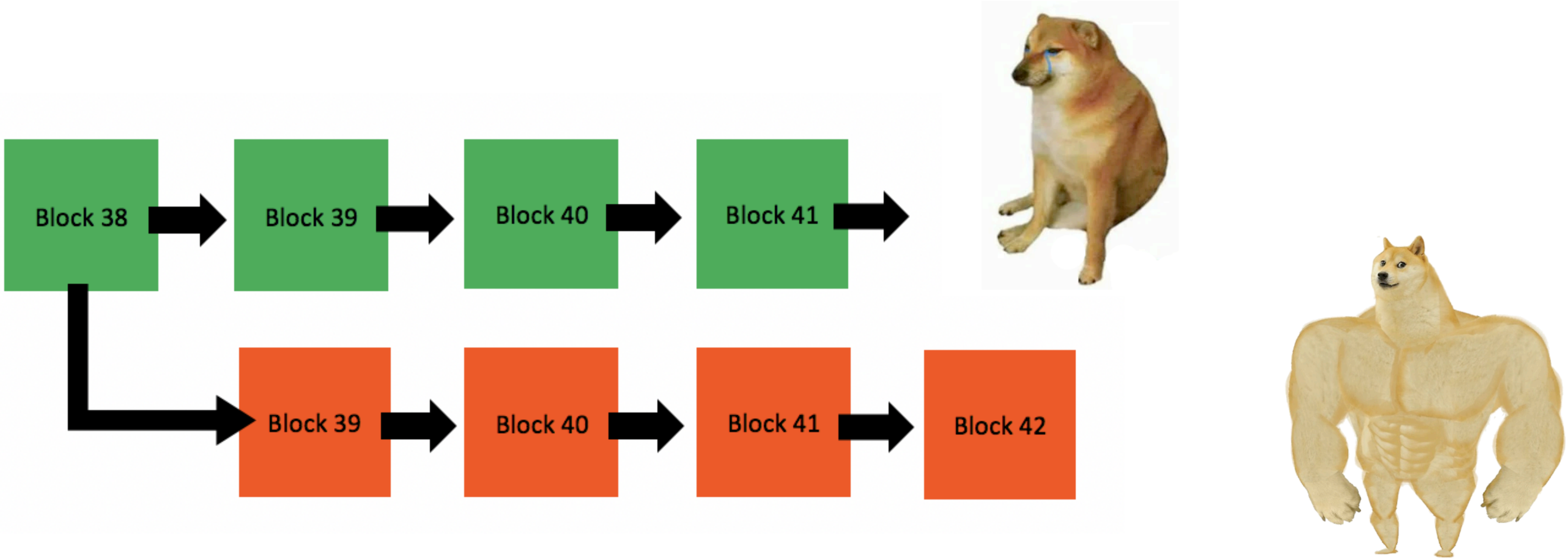


Bob spent 100 BTC

Bob did not spend 100 BTC

2) The attacker succeeds in making the fraudulent chain longer as specified in red blocks

Double-spending attack



> 50 % hash power

3) Attackers branch is published and is considered valid

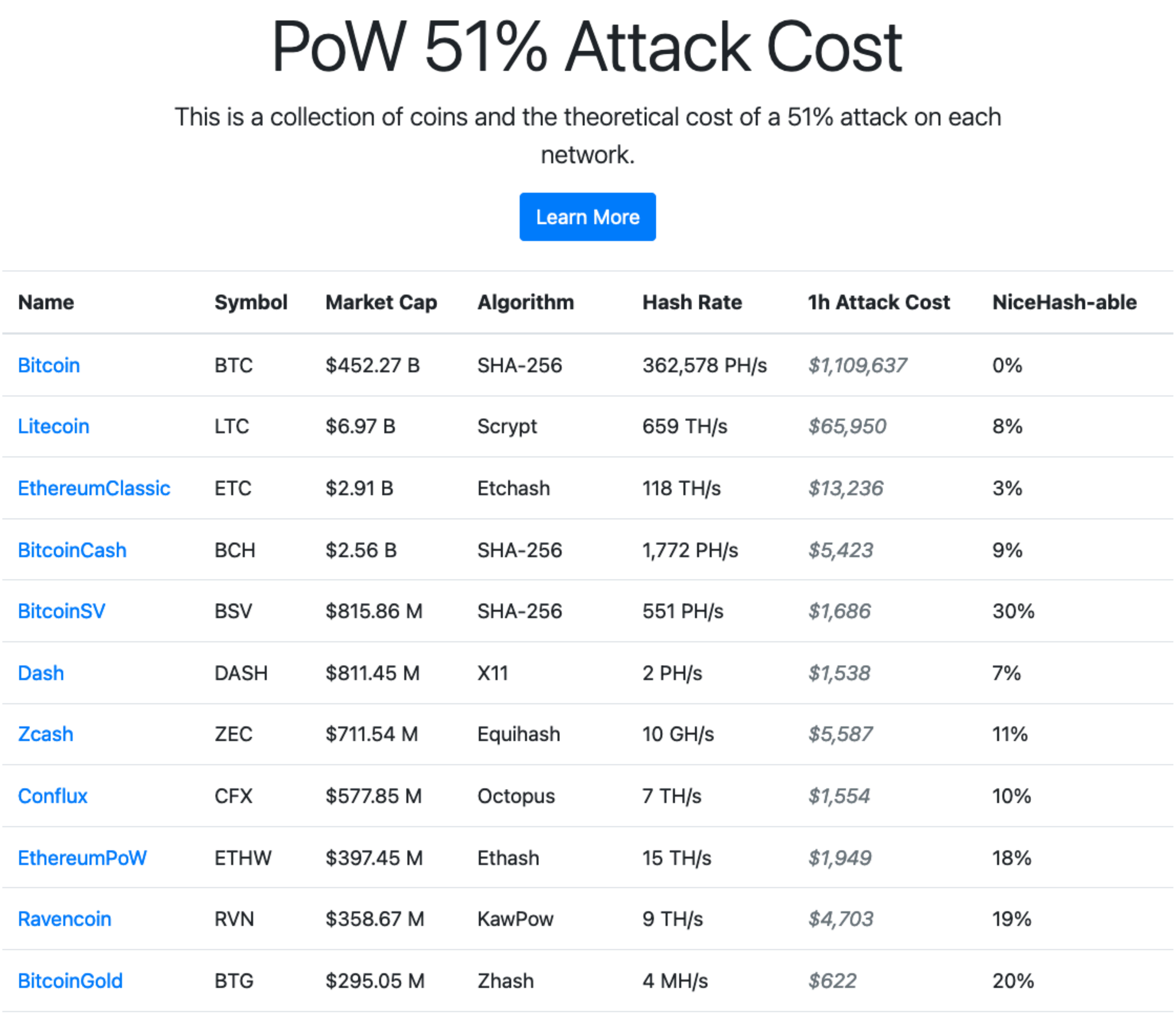
Double spend
51 % attack prevention

- The security of Bitcoin against the reversal of payments (so-called double spending attacks) relies on having more computational power held by honest nodes than by misbehaving nodes.

- Miners' rewards incentivize more honest participants to invest additional computational resources in mining, and thus support the security of Bitcoin.

Bitcoin security

Theorem 1 (informal). As long as the attacker holds less than 50% of the computational power, and all honest nodes can communicate quickly (compared to the expected time for block creation), the probability of a transaction being reversed decreases exponentially with the number of confirmations it has received.



PoW 51% Attack Cost

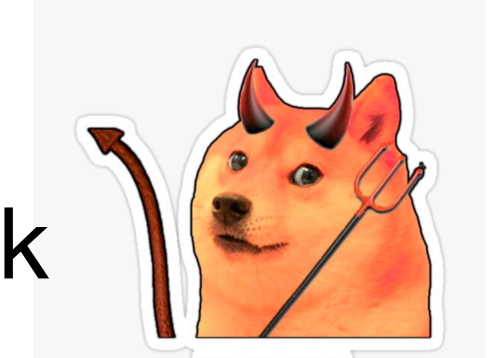
This is a collection of coins and the theoretical cost of a 51% attack on each network.

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$452.27 B	SHA-256	362,578 PH/s	*$1,109,637*	0%
Litecoin	LTC	$6.97 B	Scrypt	659 TH/s	*$65,950*	8%
EthereumClassic	ETC	$2.91 B	Etchash	118 TH/s	*$13,236*	3%
BitcoinCash	BCH	$2.56 B	SHA-256	1,772 PH/s	*$5,423*	9%
BitcoinSV	BSV	$815.86 M	SHA-256	551 PH/s	*$1,686*	30%
Dash	DASH	$811.45 M	X11	2 PH/s	*$1,538*	7%
Zcash	ZEC	$711.54 M	Equihash	10 GH/s	*$5,587*	11%
Conflux	CFX	$577.85 M	Octopus	7 TH/s	*$1,554*	10%
EthereumPoW	ETHW	$397.45 M	Ethash	15 TH/s	*$1,949*	18%
Ravencoin	RVN	$358.67 M	KawPow	9 TH/s	*$4,703*	19%
BitcoinGold	BTG	$295.05 M	Zhash	4 MH/s	*$622*	20%

https://www.crypto51.app/

Successful attacks

Reorg = malicious hard fork

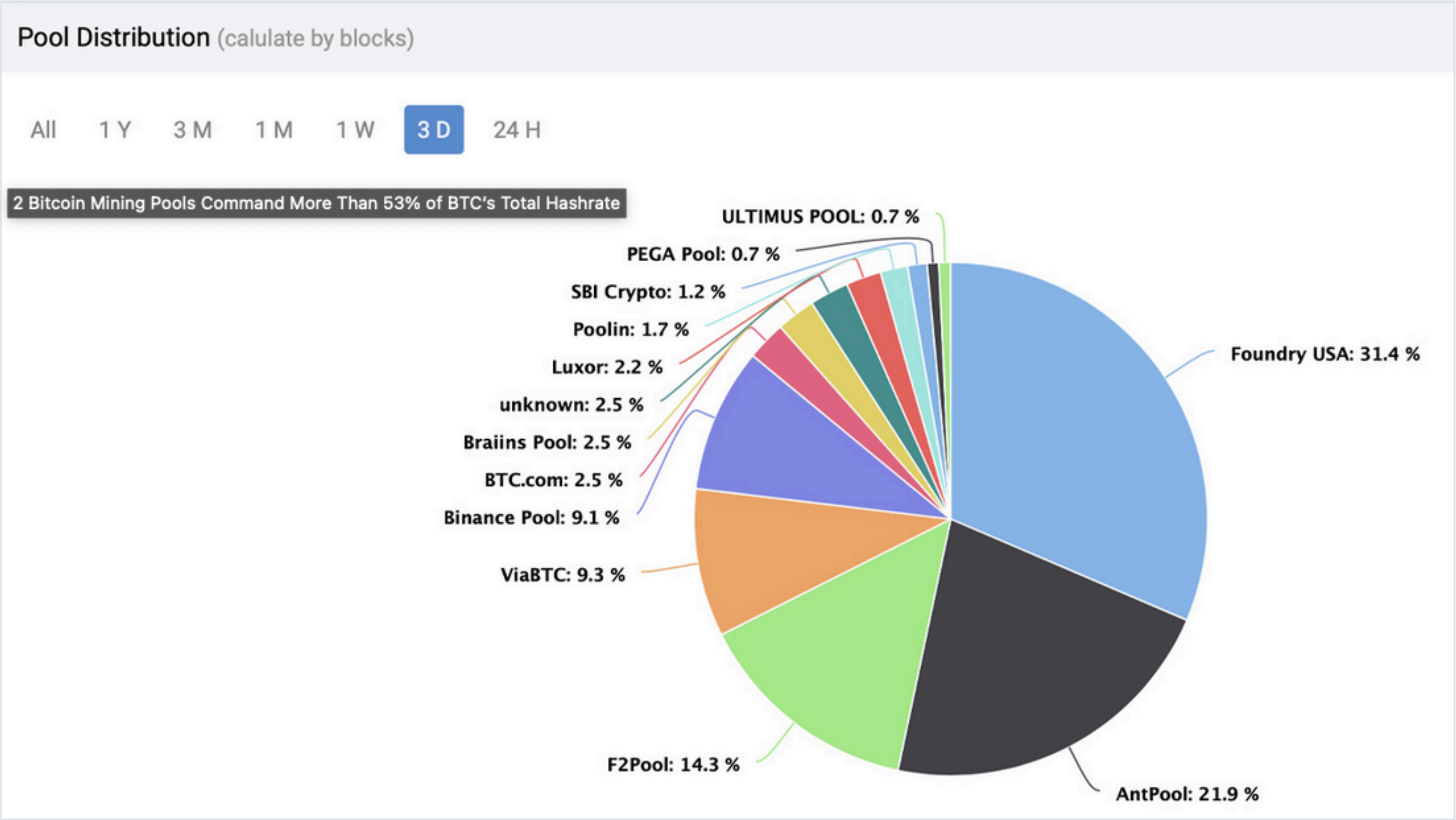


Since June 2019, over 40 reorgs that were 6 or more blocks deep on coins such as BTG, HANA, VTC, XVG, EXP and LCC. https://dci.mit.edu/51-attacks

Why is it not practical with Bitcoin ?

The 51% hashing power is more than 511,111 of the most powerful ASIC miners, which have a hashrate per unit of 255 TH/s and cost more than $10 billion in equipment only.

(As of Sep. 22, 2022)

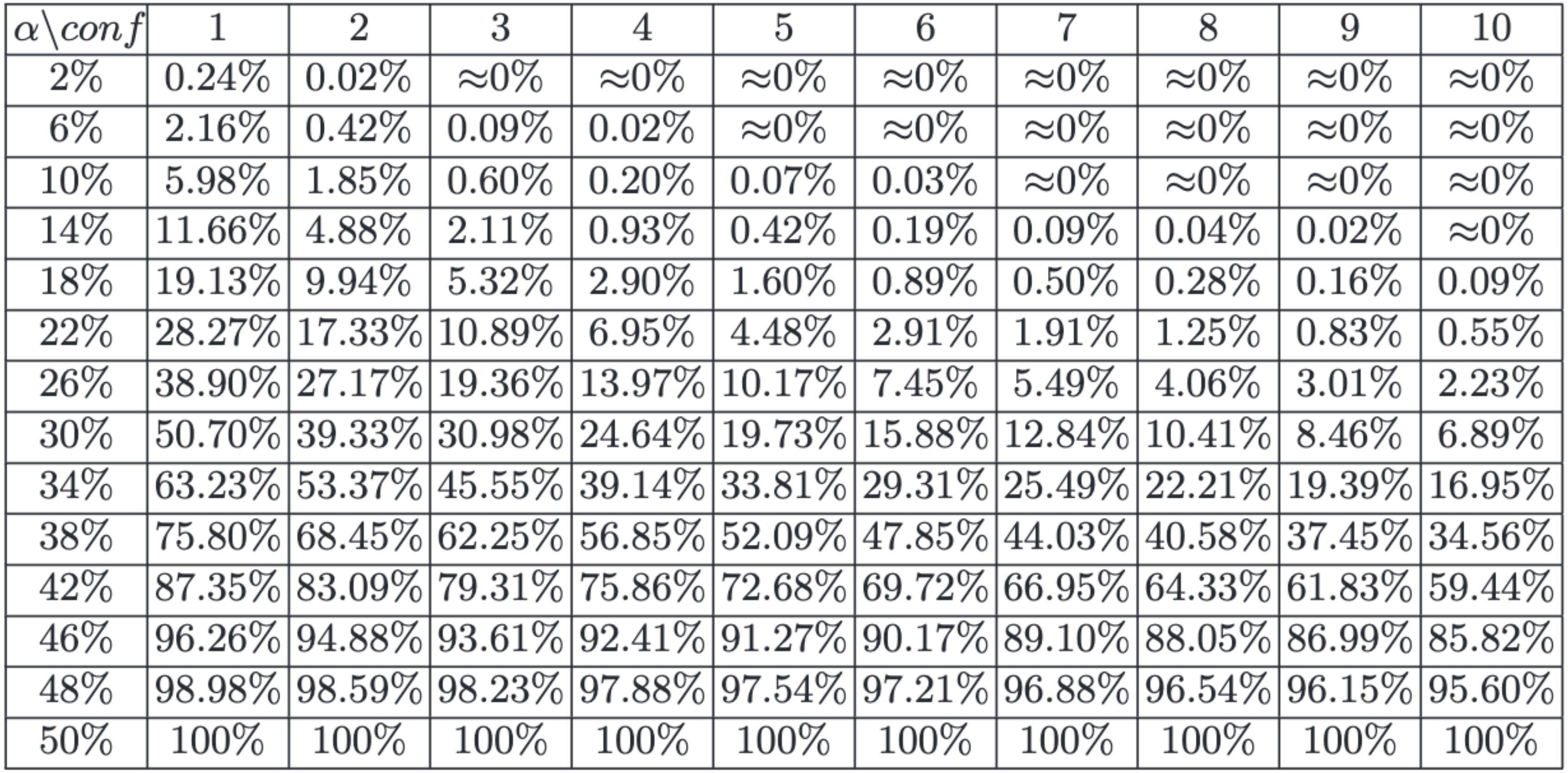


Pool Distribution (calulate by blocks)

2 Bitcoin Mining Pools Command More Than 53% of BTC's Total Hashrate

Bitcoin Pool Distribution records on Dec. 29, 2022. (3-day stats) https://github.com/TheBlueMatt/bips/blob/master/bip-XXXX.mediawiki

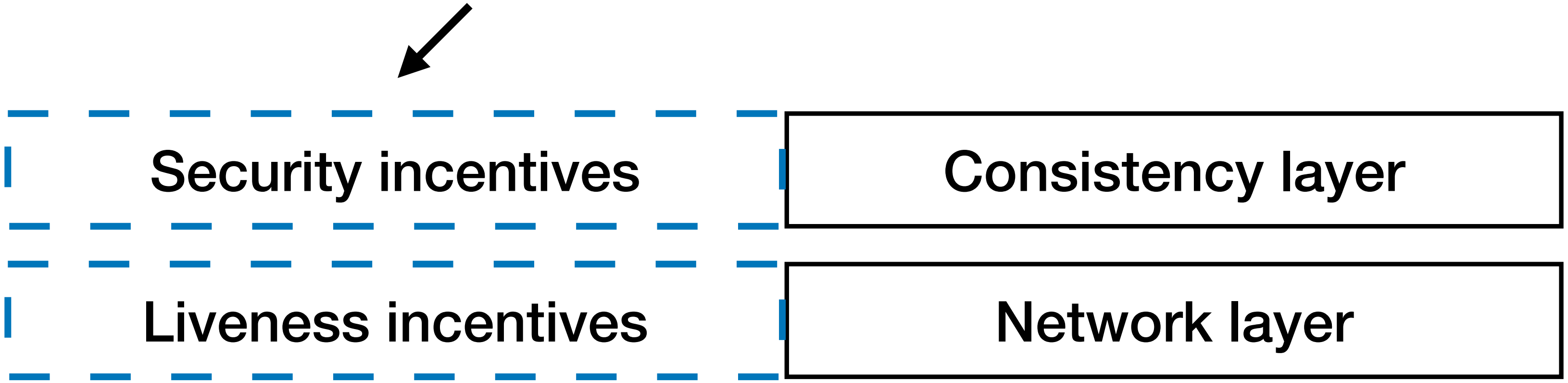
The probability of a successful attack on an arbitrary block, given the attacker’s hashrate (α) and the number of confirmations the acceptance policy waits for (conf).



$\alpha \backslash conf$	1	2	3	4	5	6	7	8	9	10
2%	0.24%	0.02%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%
6%	2.16%	0.42%	0.09%	0.02%	≈0%	≈0%	≈0%	≈0%	≈0%	≈0%
10%	5.98%	1.85%	0.60%	0.20%	0.07%	0.03%	≈0%	≈0%	≈0%	≈0%
14%	11.66%	4.88%	2.11%	0.93%	0.42%	0.19%	0.09%	0.04%	0.02%	≈0%
18%	19.13%	9.94%	5.32%	2.90%	1.60%	0.89%	0.50%	0.28%	0.16%	0.09%
22%	28.27%	17.33%	10.89%	6.95%	4.48%	2.91%	1.91%	1.25%	0.83%	0.55%
26%	38.90%	27.17%	19.36%	13.97%	10.17%	7.45%	5.49%	4.06%	3.01%	2.23%
30%	50.70%	39.33%	30.98%	24.64%	19.73%	15.88%	12.84%	10.41%	8.46%	6.89%
34%	63.23%	53.37%	45.55%	39.14%	33.81%	29.31%	25.49%	22.21%	19.39%	16.95%
38%	75.80%	68.45%	62.25%	56.85%	52.09%	47.85%	44.03%	40.58%	37.45%	34.56%
42%	87.35%	83.09%	79.31%	75.86%	72.68%	69.72%	66.95%	64.33%	61.83%	59.44%
46%	96.26%	94.88%	93.61%	92.41%	91.27%	90.17%	89.10%	88.05%	86.99%	85.82%
48%	98.98%	98.59%	98.23%	97.88%	97.54%	97.21%	96.88%	96.54%	96.15%	95.60%
50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

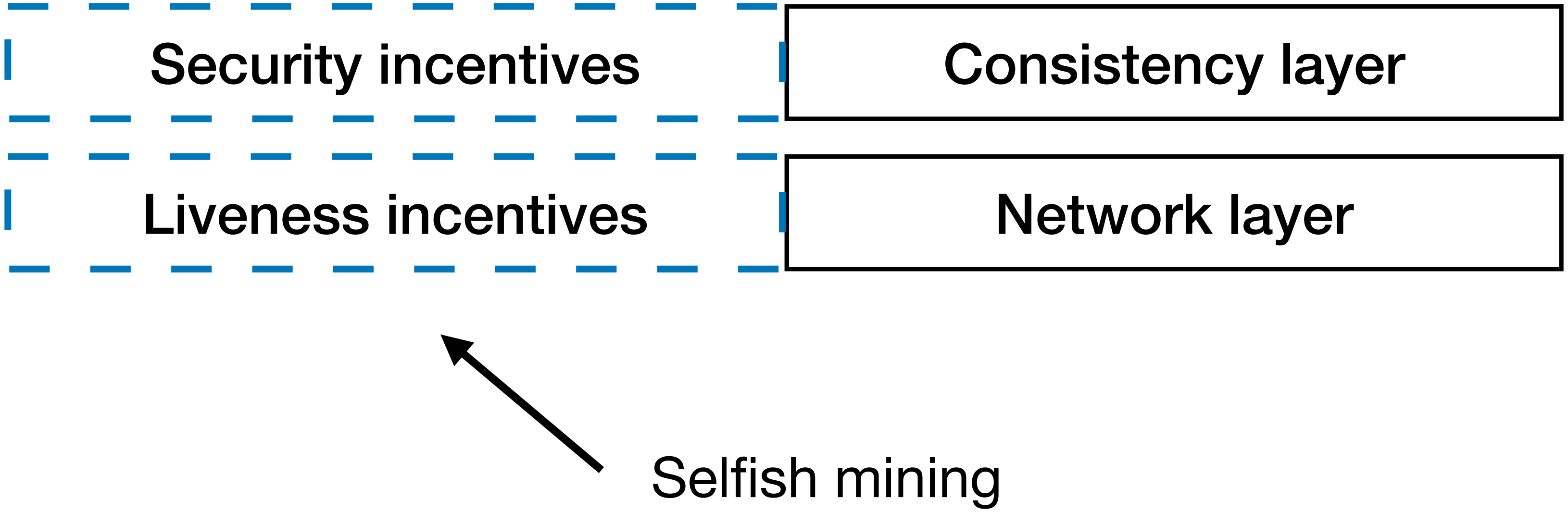
Sompolinsky, Yonatan, and Aviv Zohar. "Bitcoin's security model revisited." *arXiv preprint arXiv:1605.09193* (2016).

Attacks at different layers



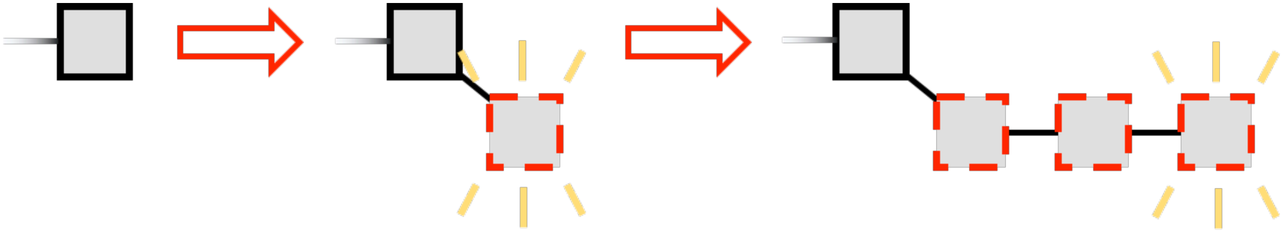
Double spending attacks as an example

Attacks at different layers



Selfish mining

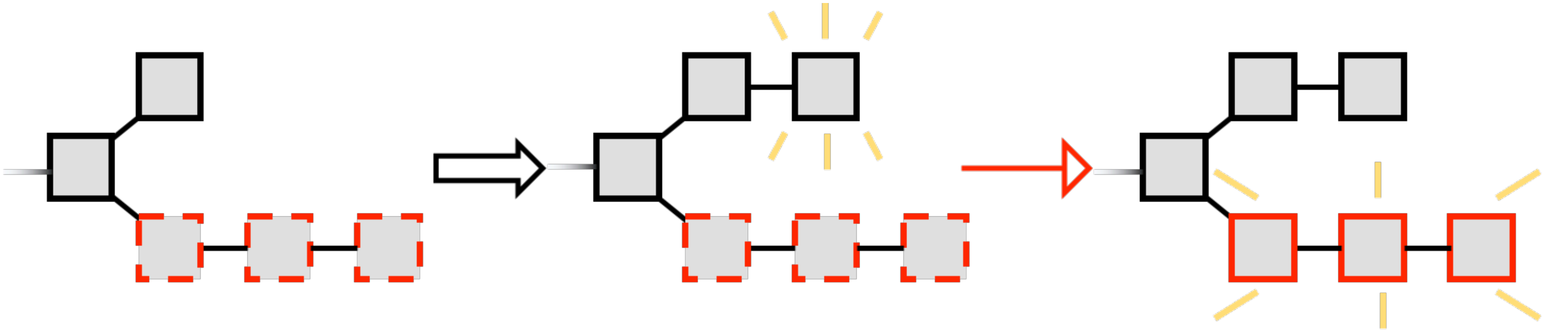
1) Selfish miner doesn’t publish the block generated and keeps it secret from others, and then tries to extend it further, forming a **secret branch.**

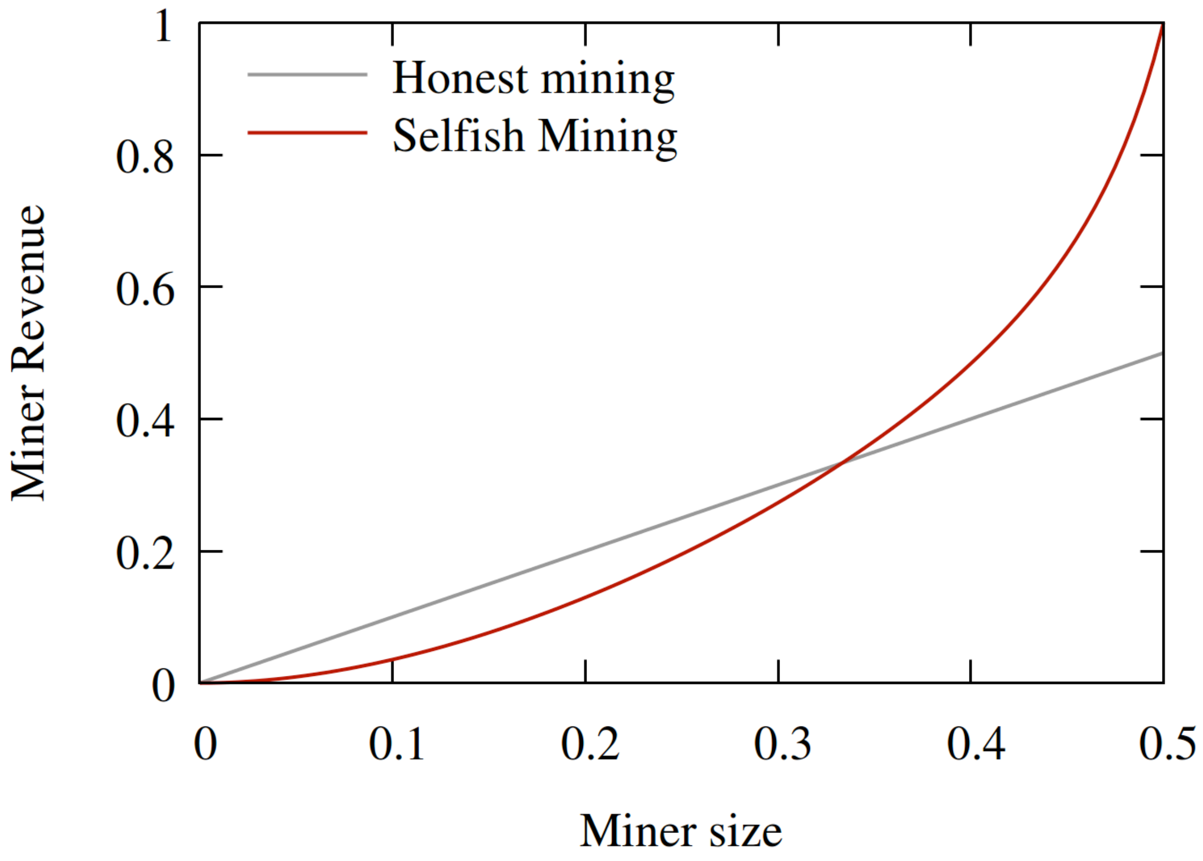


Selfish mining

2) The selfish miner keeps extending his chain, which reaches a point where it is longer than the public chain.

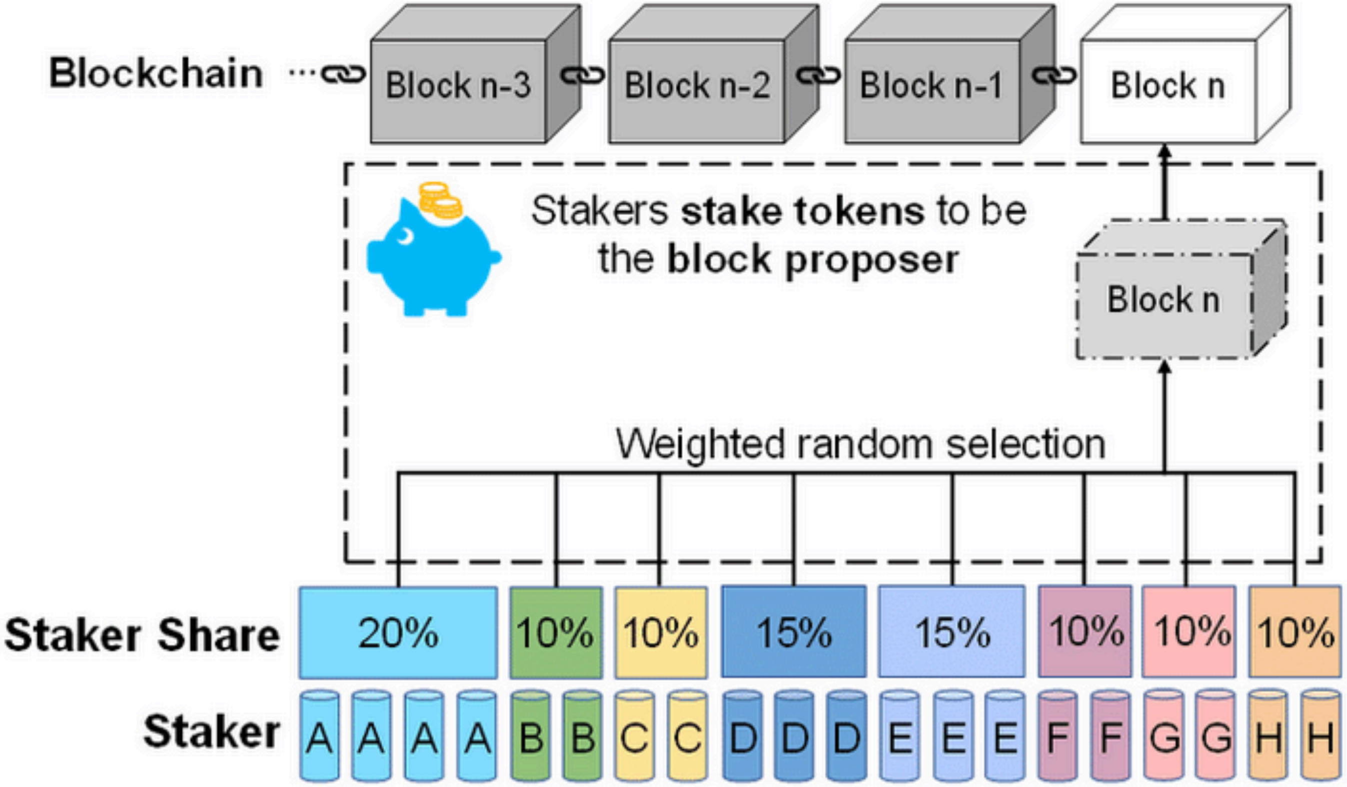
3) the attacker creates a deliberate fork, and (sometimes) manages to force the honest network to abandon and discard some of its blocks.





A selfish miner larger than 1/3 of the mining power would increase revenue by deviating from the prescribed protocol

Incentives in Proof of Stake (Pos)


Blockchain
Block n-3
Block n-2
Block n-1
Block n
Stakers **stake tokens** to be the **block proposer**
Block n
Weighted random selection
Staker Share
20%
10%
10%
15%
15%
10%
10%
10%
Staker
A A A A B B C C D D D E E E F F G G H H

Ethereum PoS

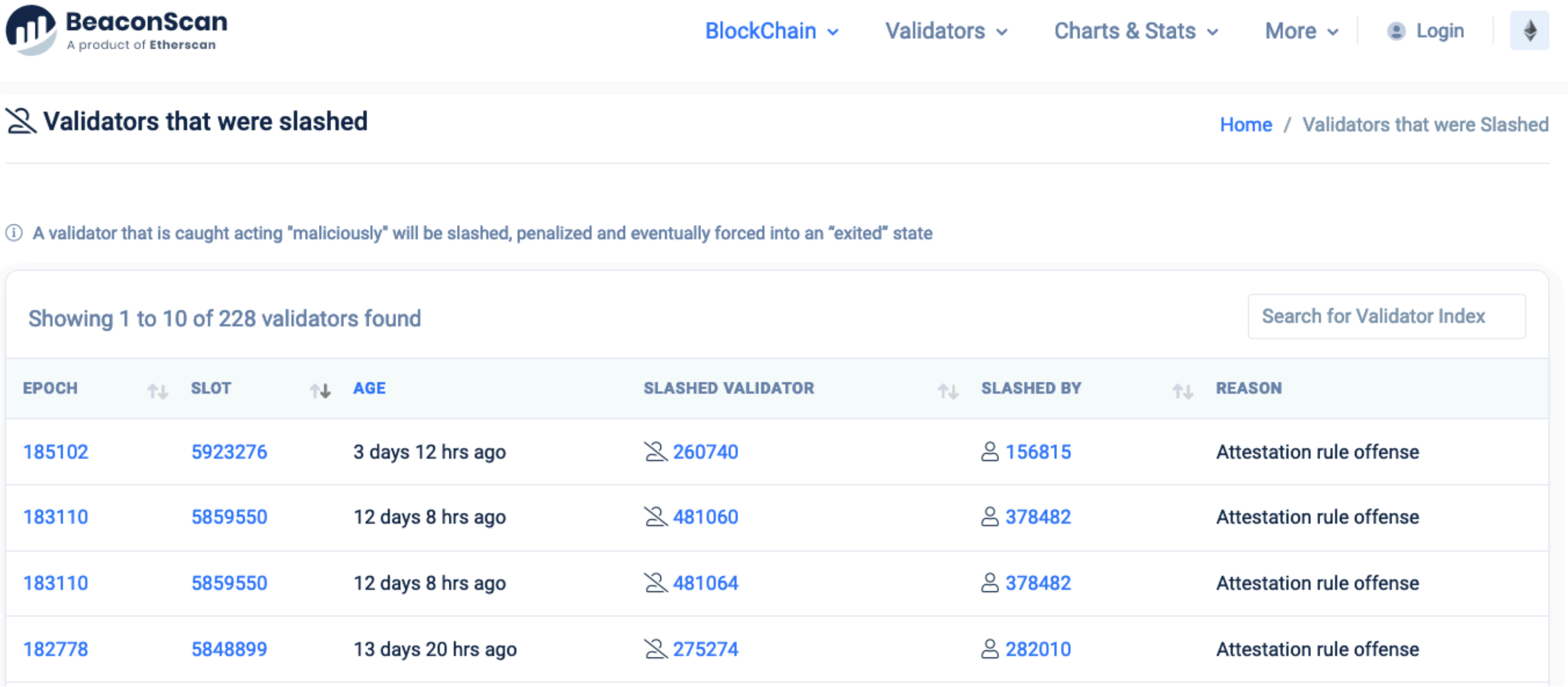
Slashing conditions

- By proposing and signing two different blocks for the same slot

- By attesting to a block that "surrounds" another one (effectively changing history)

- By "double voting" by attesting to two candidates for the same block

Ethereum 2.0 slashing



Validators that were slashed

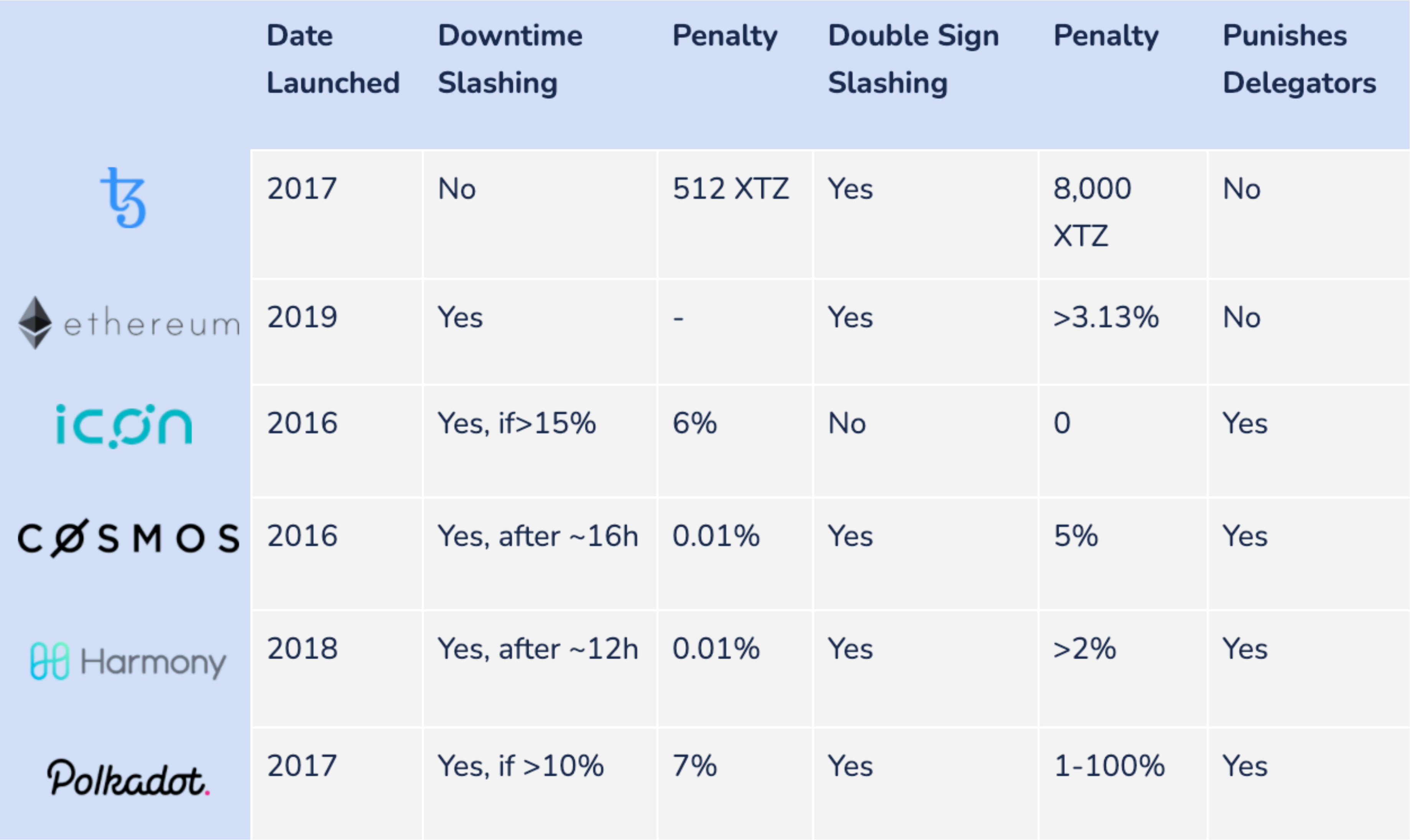
Home / Validators that were Slashed

ⓘ A validator that is caught acting "maliciously" will be slashed, penalized and eventually forced into an “exited” state

Showing 1 to 10 of 228 validators found

Search for Validator Index

EPOCH	SLOT	AGE	SLASHED VALIDATOR	SLASHED BY	REASON
185102	5923276	3 days 12 hrs ago	260740	156815	Attestation rule offense
183110	5859550	12 days 8 hrs ago	481060	378482	Attestation rule offense
183110	5859550	12 days 8 hrs ago	481064	378482	Attestation rule offense
182778	5848899	13 days 20 hrs ago	275274	282010	Attestation rule offense



	Date Launched	Downtime Slashing	Penalty	Double Sign Slashing	Penalty	Punishes Delegators
ꜩ	2017	No	512 XTZ	Yes	8,000 XTZ	No
ethereum	2019	Yes	-	Yes	>3.13%	No
icon	2016	Yes, if>15%	6%	No	0	Yes
COSMOS	2016	Yes, after ~16h	0.01%	Yes	5%	Yes
Harmony	2018	Yes, after ~12h	0.01%	Yes	>2%	Yes
Polkadot.	2017	Yes, if >10%	7%	Yes	1-100%	Yes

Problems with incentives in PoS

- Nothing at stake problem
- Censorship resistance
- Incentive for re-centralization

Part 2

What is Web 3?

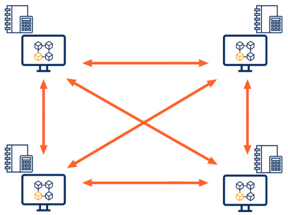
Liquidity pools
Decentralized Stablecoins

Tokens for various types of systems

Application	UNISWAP	
Software	DAppNode	INSTADAPP
Presentation	ENS	ERC20
Processing	0x	polygon (MATIC) crypto
Information	the graph	Filecoin
Network	INFURA	API3
Data Link	BITMAIN	
Physical	helium	FOAM

Web3 VS Current web

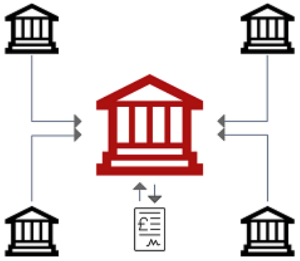
Web3



Peer to Peer

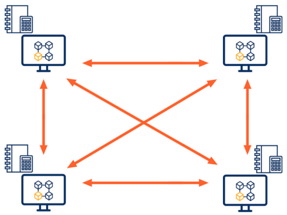
Current web

Client-Server architectures



VS

Web3



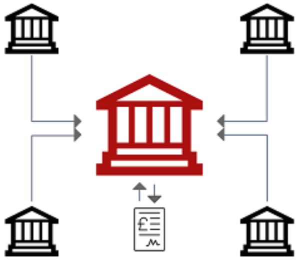
Peer to Peer

Permissionless

VS

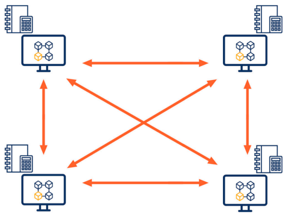
Current web

Client-Server architectures



Identity based

Web3



Peer to Peer

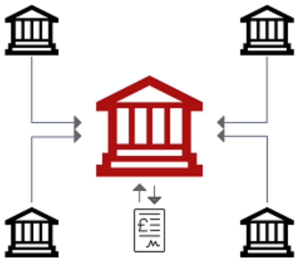
Permissionless

Protocol value
captured by users

VS

Current web

Client-Server
architectures

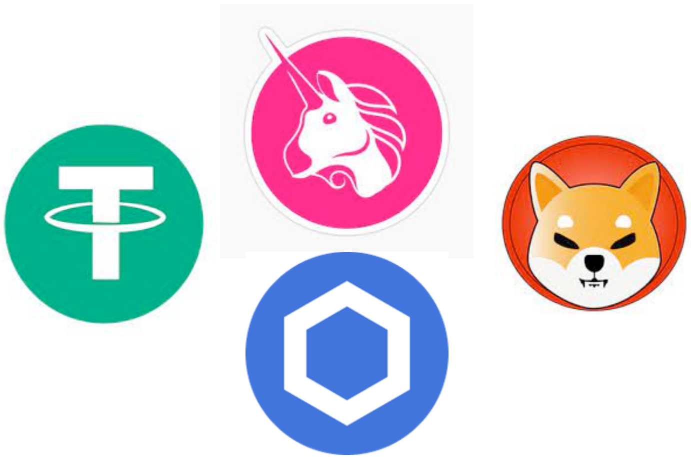


Identity based

Platforms capture
all value

Some examples of tokens on ETH

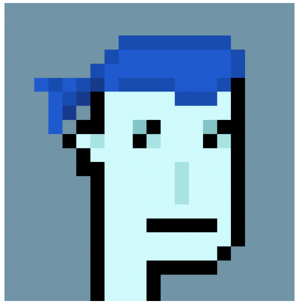
- ERC20 smart contract standard for *fungible tokens,* that can represent different things:
    - Currency
    - Voting rights
    - Deed of ownership and etc.



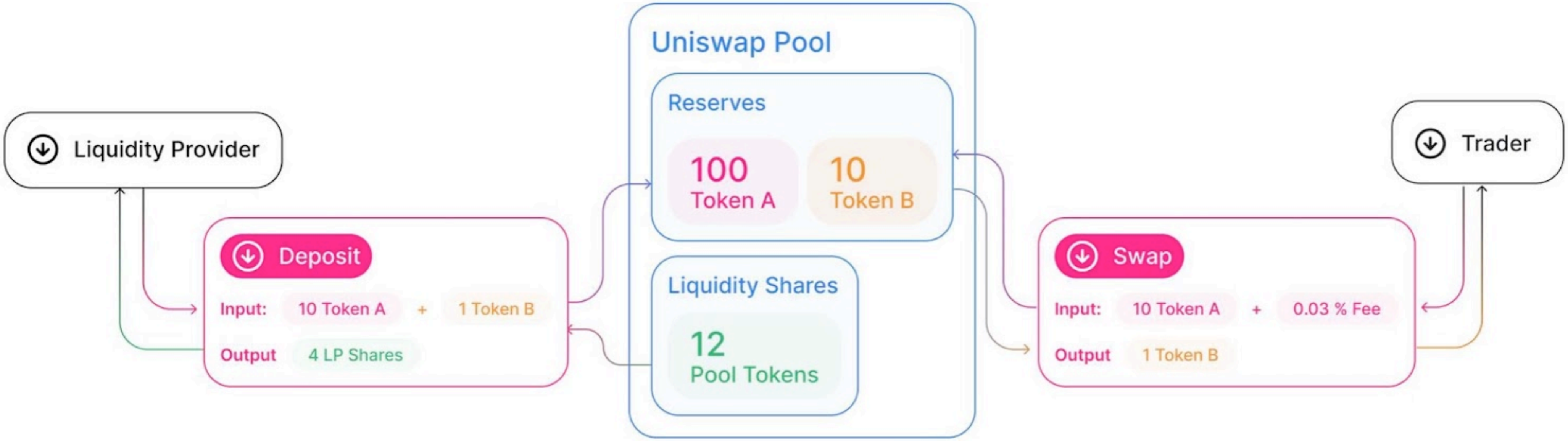
Some examples of tokens on ETH

- ERC721 smart contract standard for *non-fungible tokens*, that can represent:

  - Collectibles
  - Credentials
  - Loans
  - In-game items

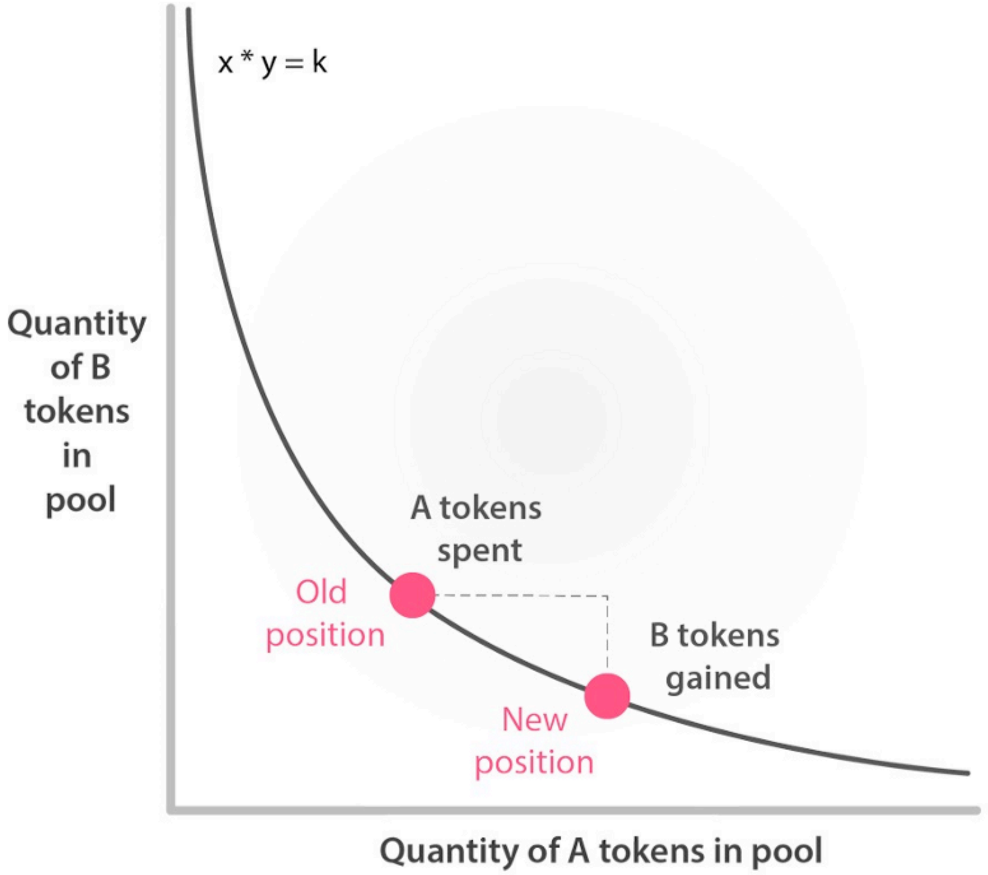


Decentralised Exchange

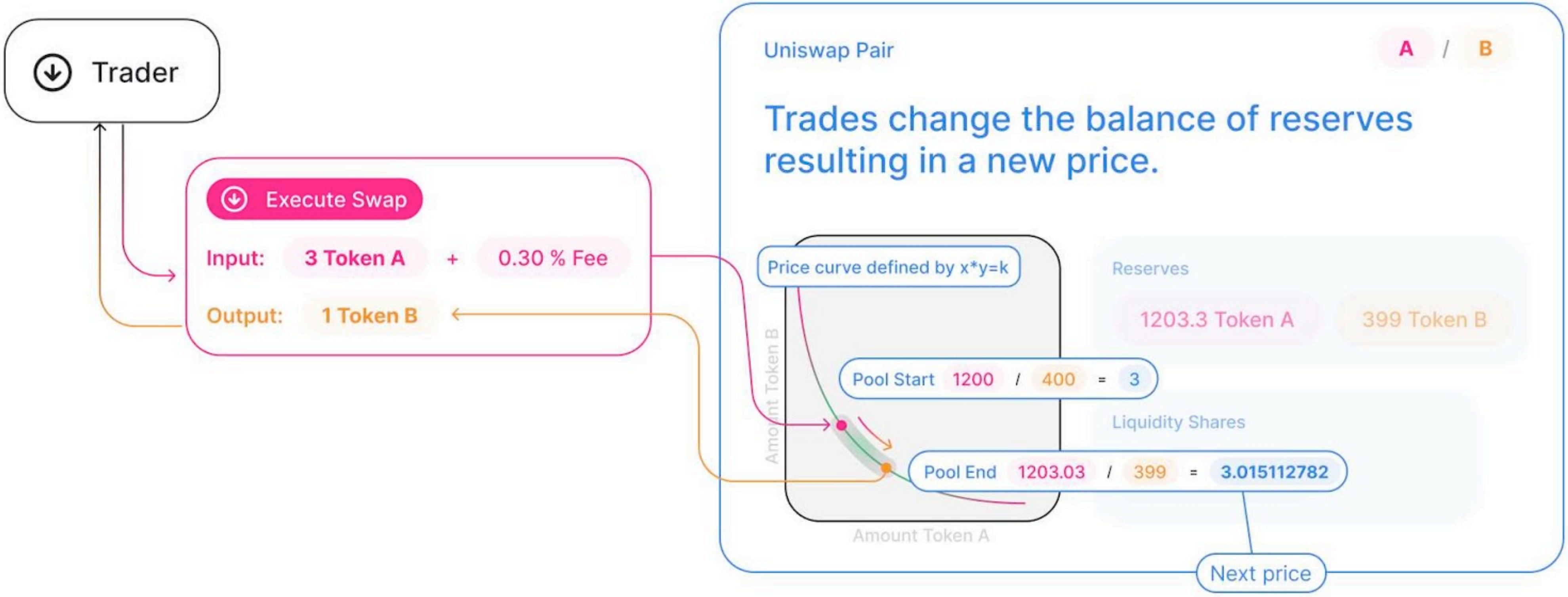


- Liquidity providers accrue fees from swaps (0.30% fee in uniswap V2)

Automated Market Maker



Uniswap flow

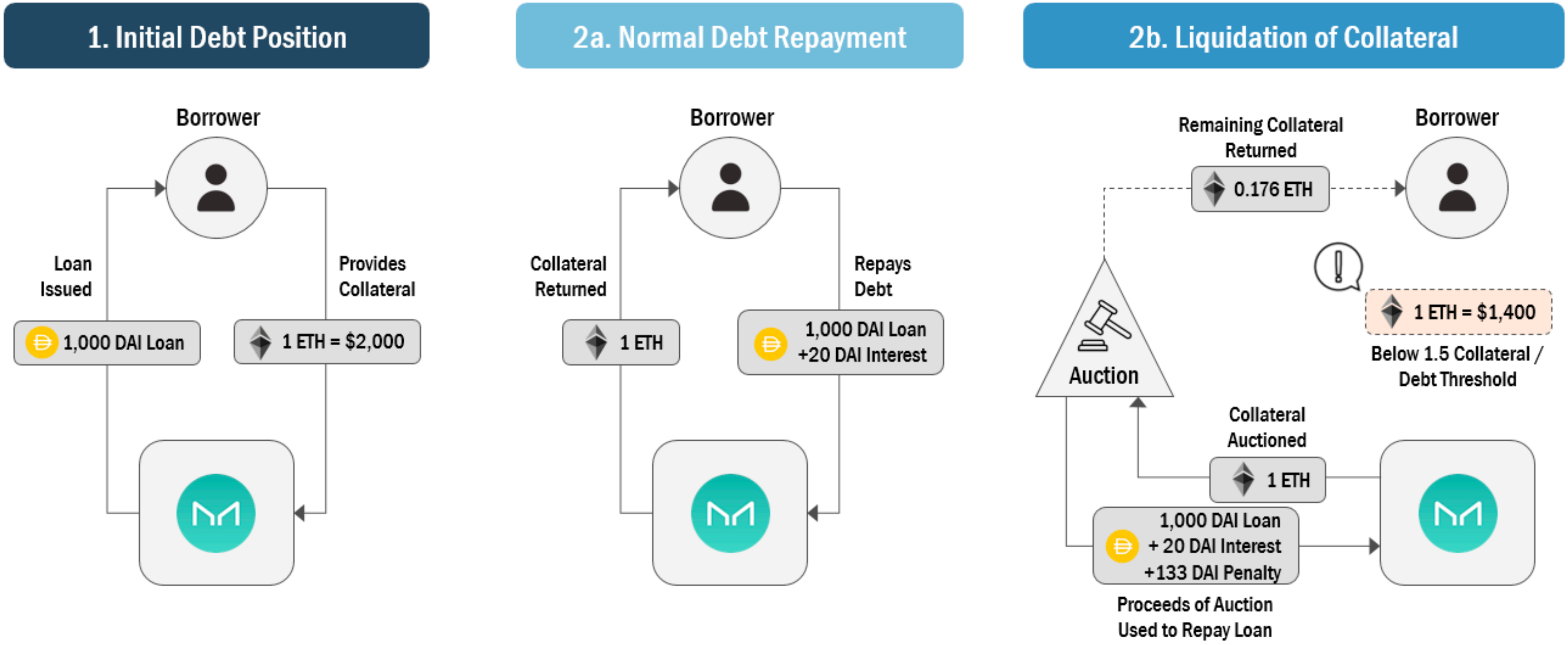


Lending protocols

MAKER

- DAI Stablecoin pegged to USD
- Users generate DAI by locking cryptocurrency in a Maker Vault
- To get crypto collateral back, repay user repay the withdrawn DAI.

Maker protocol flow



1. Initial Debt Position

Borrower

Loan Issued

1,000 DAI Loan

Provides Collateral

1 ETH = $2,000

2a. Normal Debt Repayment

Borrower

Collateral Returned

1 ETH

Repays Debt

1,000 DAI Loan
+20 DAI Interest

2b. Liquidation of Collateral

Remaining Collateral Returned

0.176 ETH

Borrower

1 ETH = $1,400

Below 1.5 Collateral / Debt Threshold

Auction

Collateral Auctioned

1 ETH

1,000 DAI Loan
+ 20 DAI Interest
+133 DAI Penalty

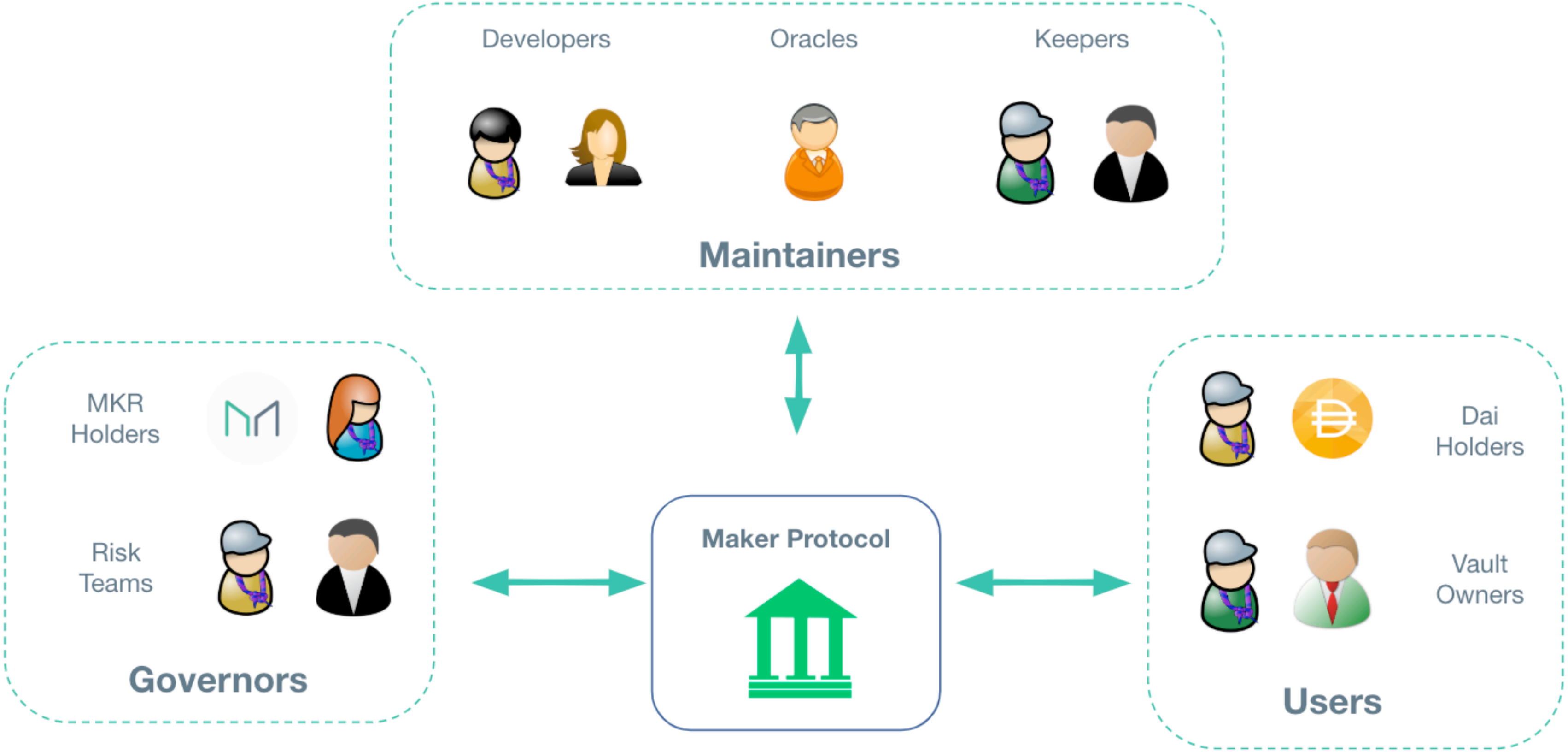
Proceeds of Auction Used to Repay Loan

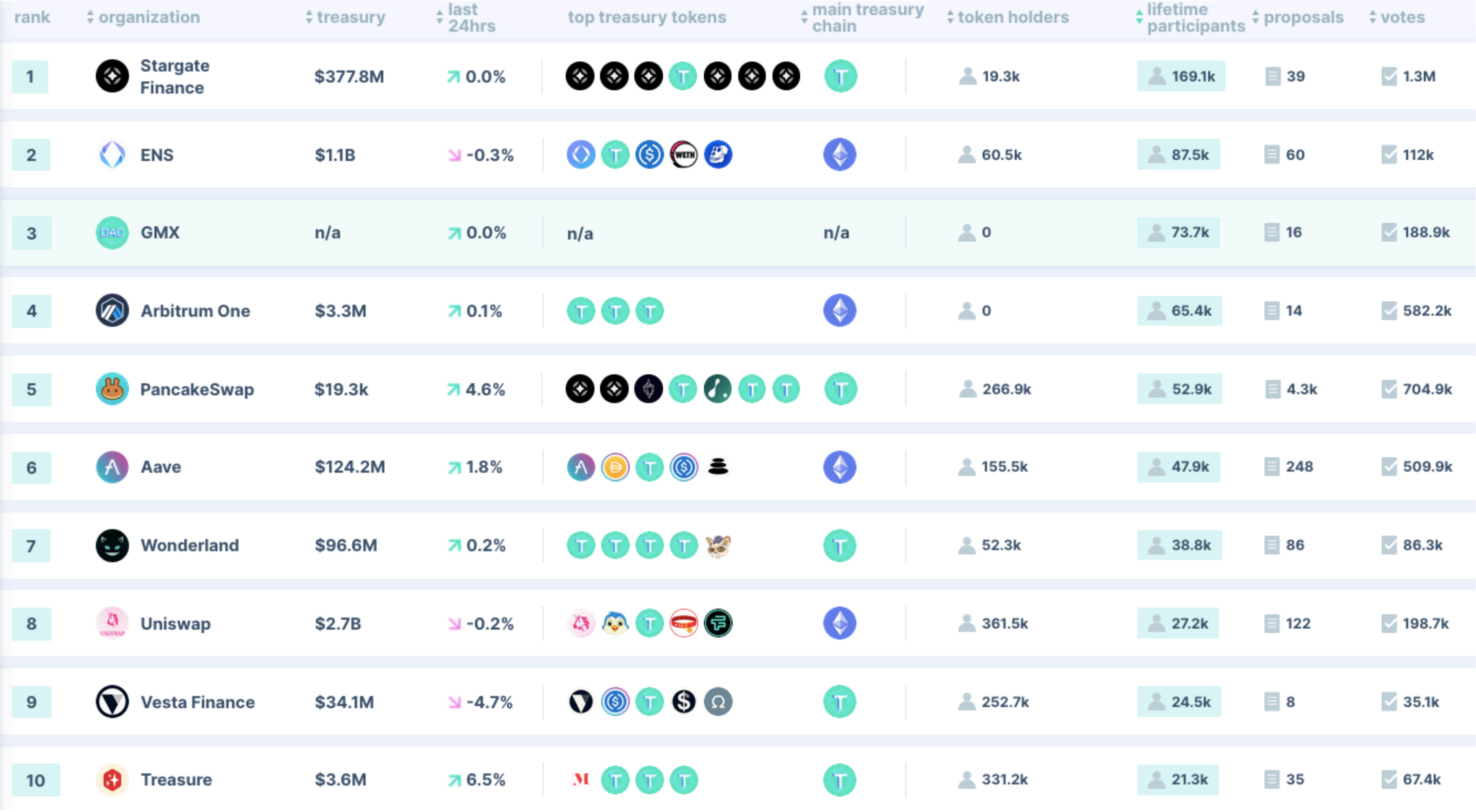
Decentralized Autonomous Organisation

DAO - can be understood as an organisation that operates on the basis of the collective input of its stakeholders, according to the rules encoded in its blockchain.

- Functioning without any central point of control (decentralised),
- Not dependent on any external regulatory structures (autonomous).

Adding governance tokens we get Maker DAO





rank	organization	treasury	last 24hrs	top treasury tokens	main treasury chain	token holders	lifetime participants	proposals	votes
1	Stargate Finance	$377.8M	↗ 0.0%			19.3k	169.1k	39	1.3M
2	ENS	$1.1B	↘ -0.3%			60.5k	87.5k	60	112k
3	GMX	n/a	↗ 0.0%	n/a	n/a	0	73.7k	16	188.9k
4	Arbitrum One	$3.3M	↗ 0.1%			0	65.4k	14	582.2k
5	PancakeSwap	$19.3k	↗ 4.6%			266.9k	52.9k	4.3k	704.9k
6	Aave	$124.2M	↗ 1.8%			155.5k	47.9k	248	509.9k
7	Wonderland	$96.6M	↗ 0.2%			52.3k	38.8k	86	86.3k
8	Uniswap	$2.7B	↘ -0.2%			361.5k	27.2k	122	198.7k
9	Vesta Finance	$34.1M	↘ -4.7%			252.7k	24.5k	8	35.1k
10	Treasure	$3.6M	↗ 6.5%			331.2k	21.3k	35	67.4k

https://deepdao.io/organizations

Limits of simple tokenomics

Dichotomy of current tokenomics

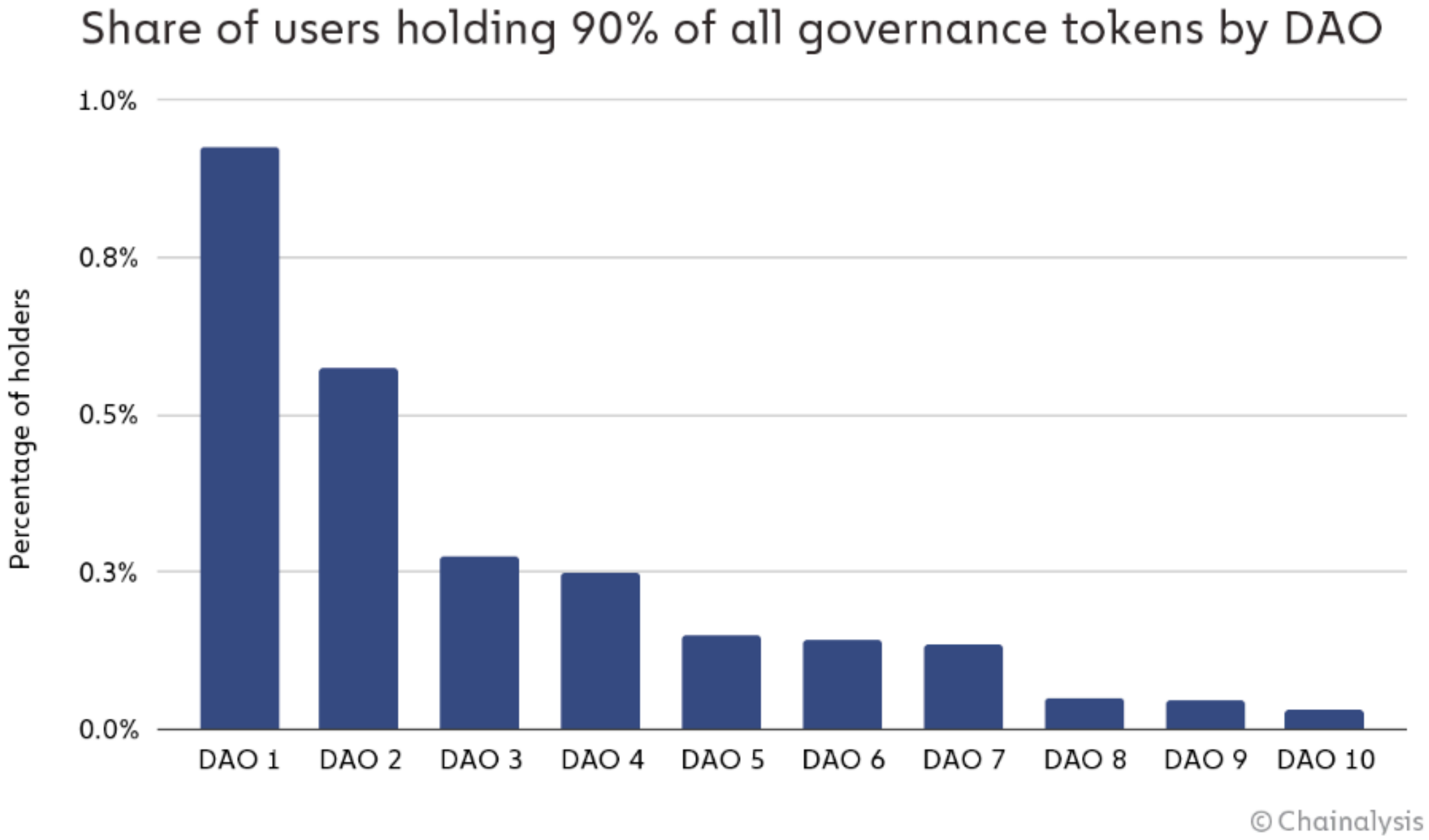
Economy

Economy

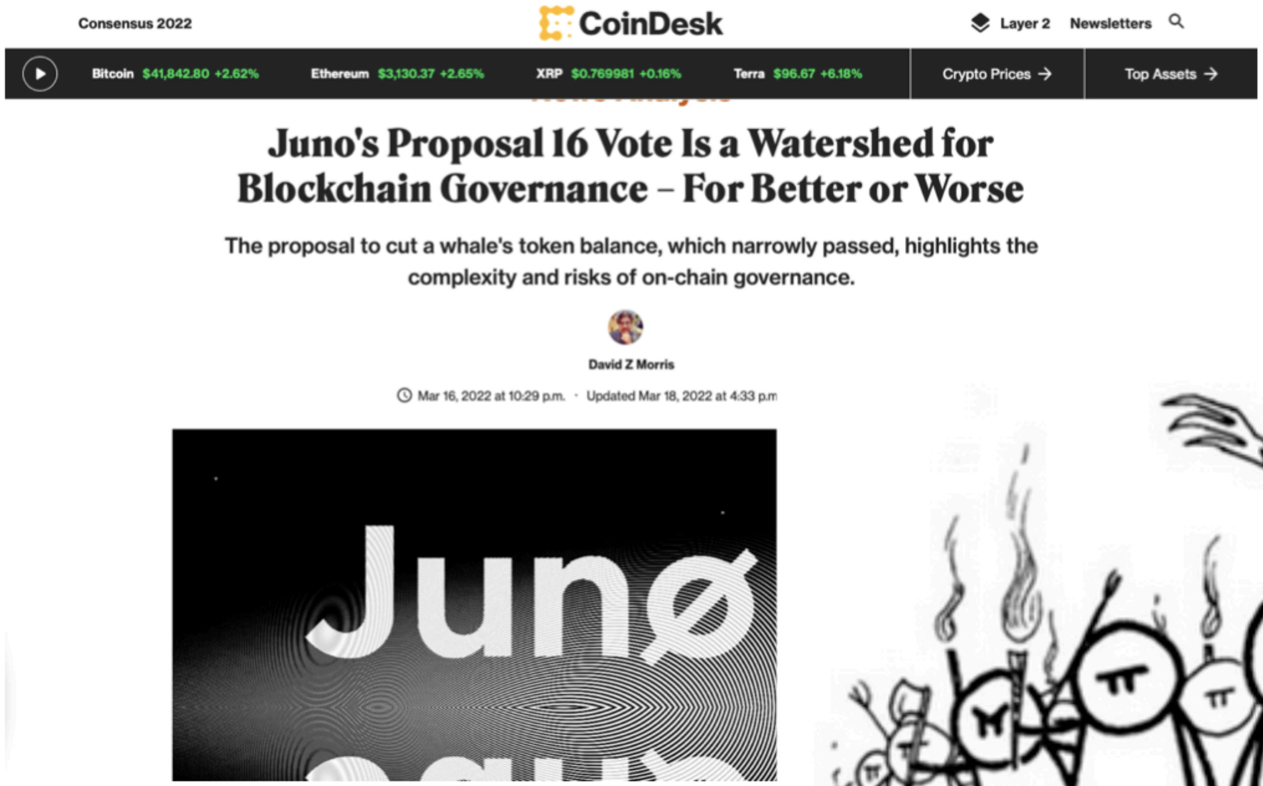
Bounded rationality

- Token voting is suboptimal
- Incentives are exploited
- Hierarchical modes of organization

Token voting



Governance

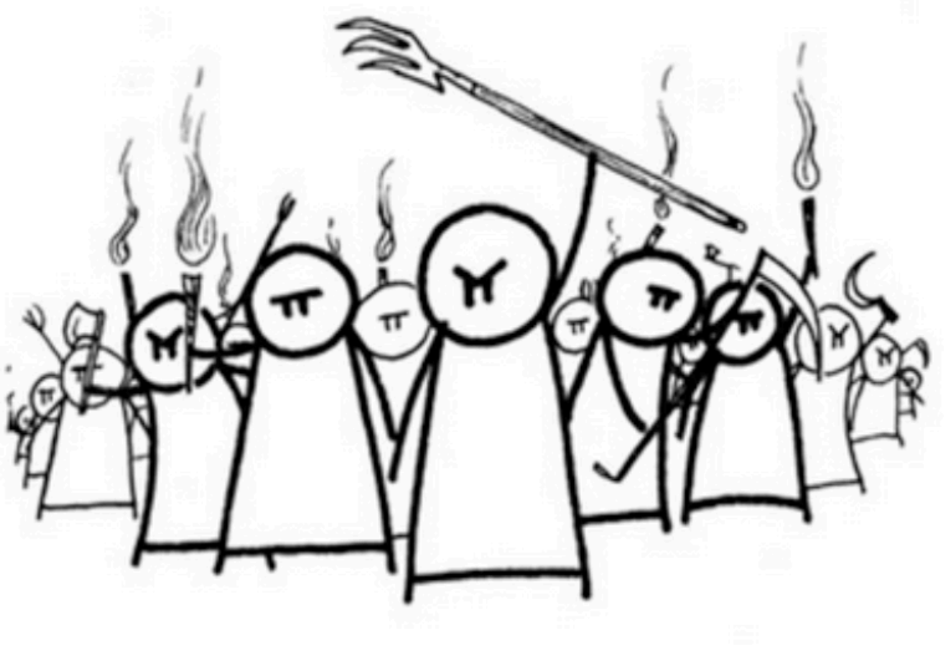


Juno's Proposal 16 Vote Is a Watershed for Blockchain Governance – For Better or Worse

The proposal to cut a whale's token balance, which narrowly passed, highlights the complexity and risks of on-chain governance.

David Z Morris

Mar 16, 2022 at 10:29 p.m. · Updated Mar 18, 2022 at 4:33 p.m



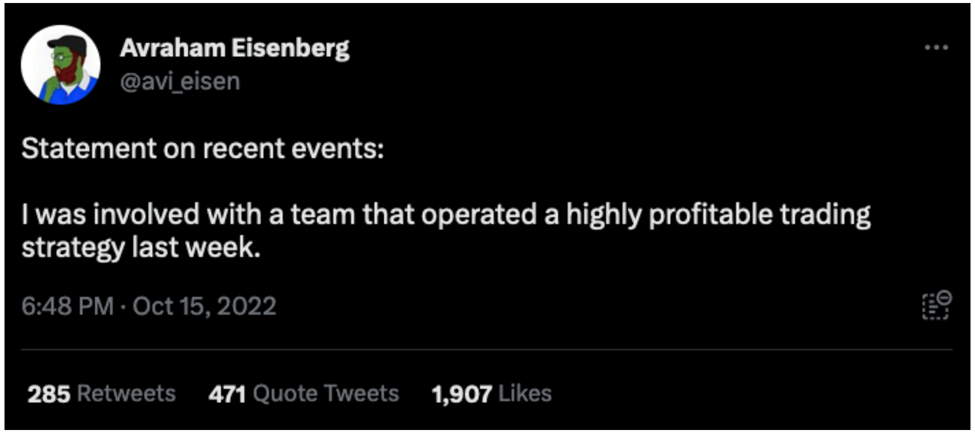
Mango markets exploit

1. Buy Mango MNGO tokens

2. Pump the price of the Mango MNGO token (thanks to low liquidity)

3. Borrow $116 million against these unrealised profits from Mango protocol

4. Withdraw all funds from Mango Markets.



Avraham Eisenberg
@avi_eisen

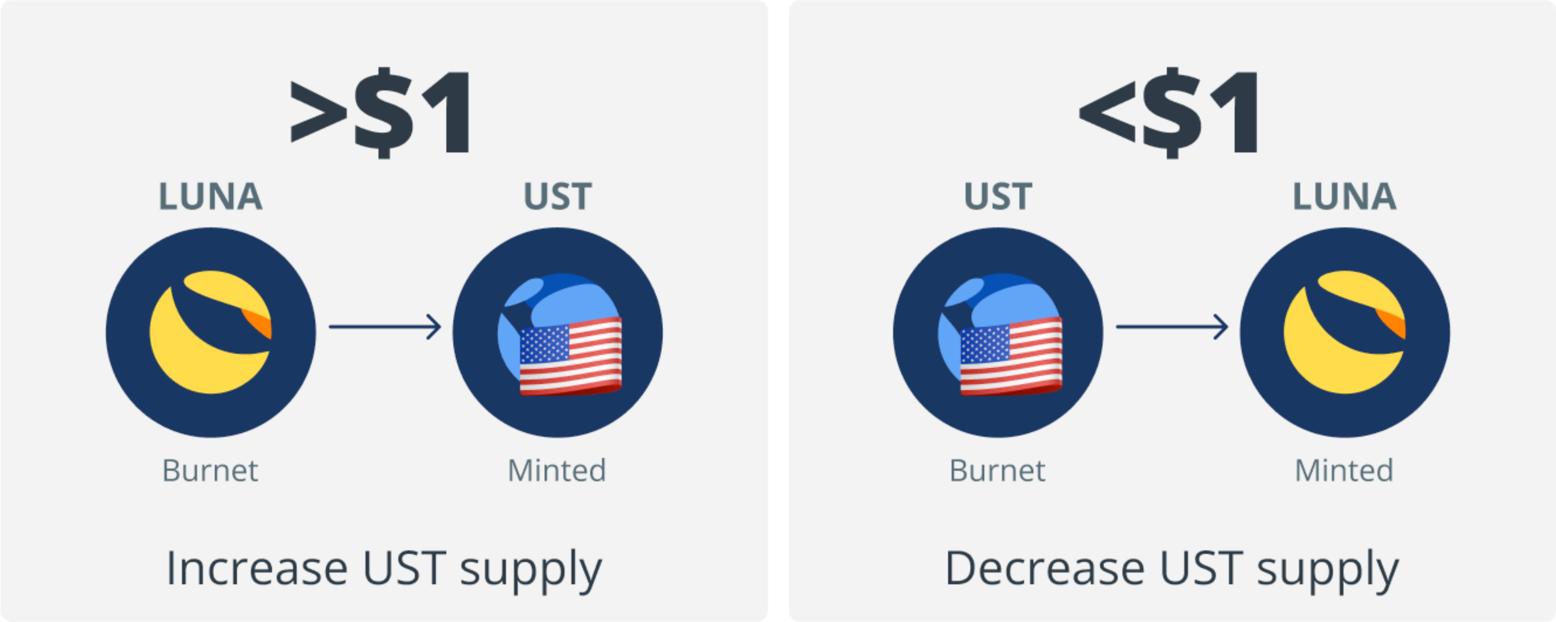
Statement on recent events:

I was involved with a team that operated a highly profitable trading strategy last week.

6:48 PM · Oct 15, 2022

285 Retweets 471 Quote Tweets 1,907 Likes

Luna alogrthmic stablecoin



>$1

LUNA → UST

Burnet → Minted

Increase UST supply

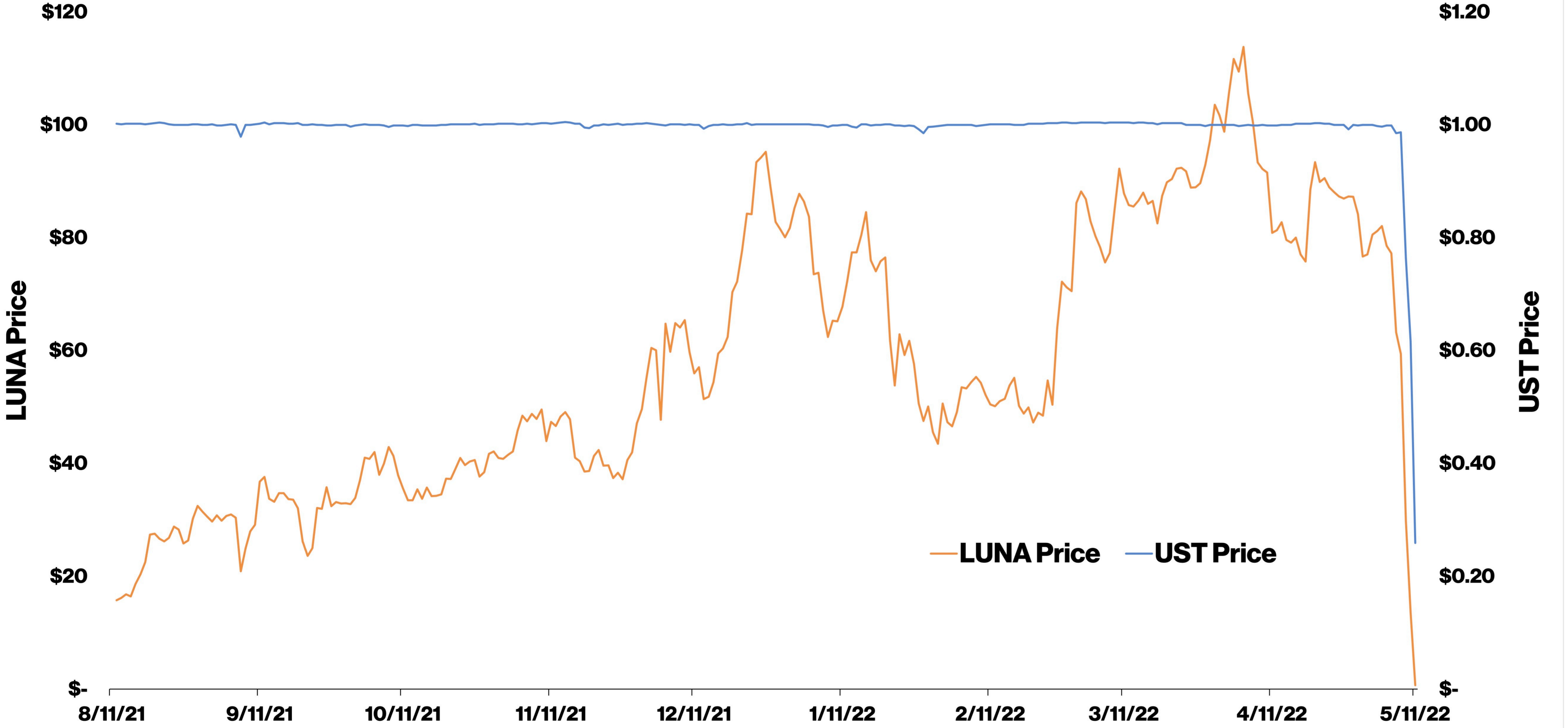
<$1

UST → LUNA

Burnet → Minted

Decrease UST supply

Luna collapse



CoinDesk

Source: CoinDesk Research, TradingView
As of May 11, 2022

Different types of incentives in P2P

- Reciprocity (tit for tat) 🤝
- Social acknowledgment 🏆
- Protocol-level reputation 😇

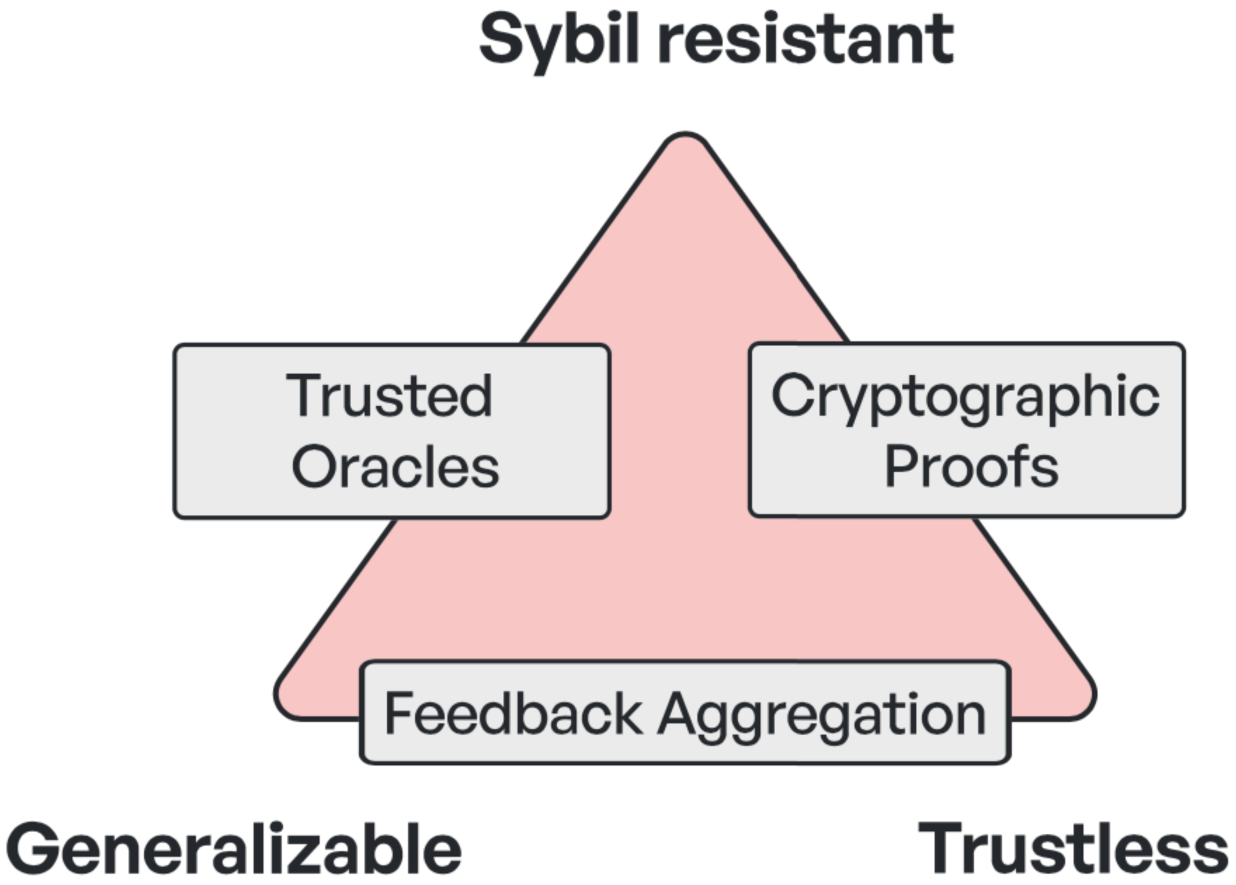
Reputation is also a highly-effective multitool

Selecting delegates
in PoS

Community building
in DAO

Reputation-based
network overlay

Decentralised reputaiton trilemma



Sybil resistant

Trusted Oracles

Cryptographic Proofs

Feedback Aggregation

Generalizable

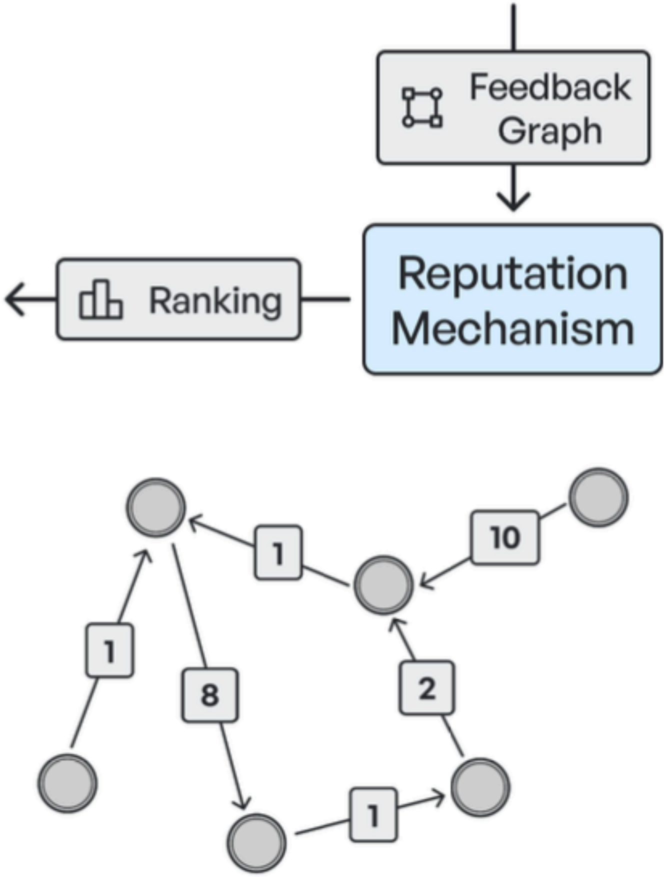
Trustless

Meritrank feedback graph reputation

- Sybil-tolerant reputation algorithm

- Does not require strong identity (permissionless)

- Allows context-specific reputation

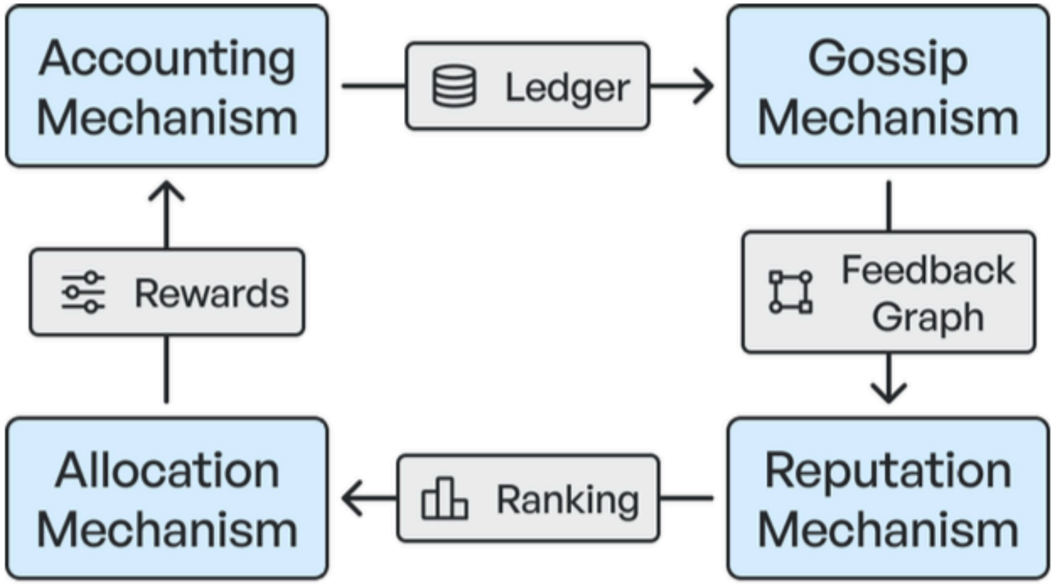


Feedback Graph

Reputation Mechanism

Ranking

Reputation in Merit-Based Tokenomics Context


Accounting Mechanism

Ledger

Gossip Mechanism

Feedback Graph

Reputation Mechanism

Ranking

Allocation Mechanism

Rewards