Computing for Decentralized Systems

Alejandro Avilés (@OmeGak)
7th ~ 8th March 2018

Distributed Systems

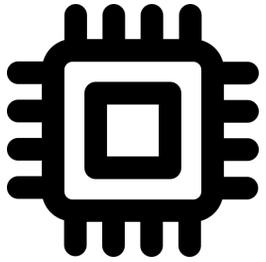
Distribute /dɪˈstrɪb.juːt/

To give something out to several people, or to spread or supply something.

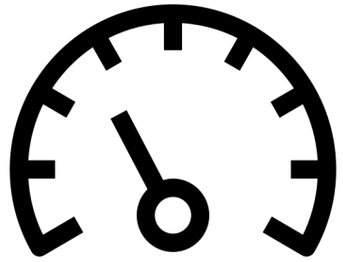
Distributed system

Hardware or software components located at networked computers communicating and coordinating their actions to achieve a common goal only by passing messages.

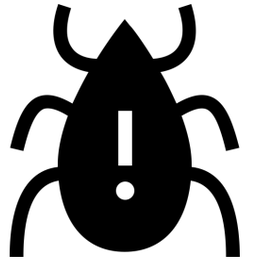
Advantages



Sharing resources

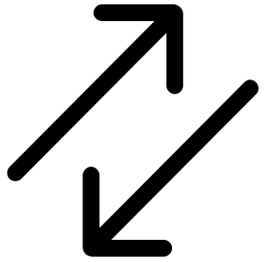


Lower latency



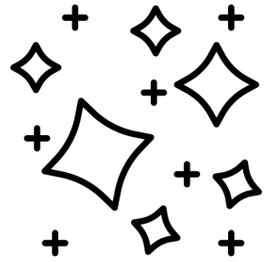
Fault tolerance

Complications



Concurrency

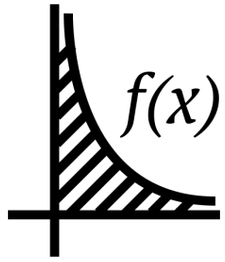
No global clock



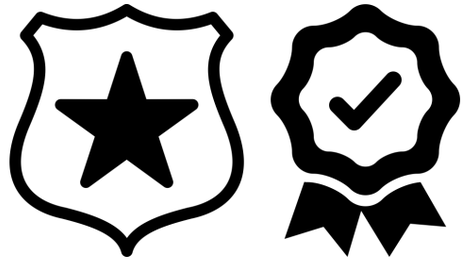
Independent failures

Security model

Interfaces

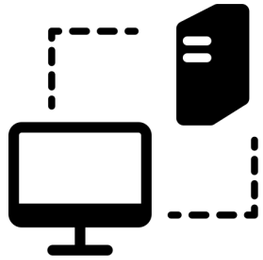


Cryptography

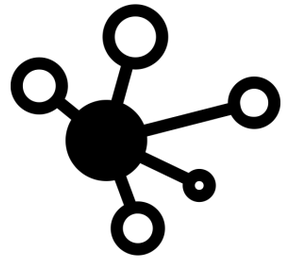


Control and trust

Role-based architectures



Client-server



Peer-to-peer

Decentralized Systems

Decentralize /ˌdiːˈsen.trə.laɪz/

To move the control of an organization or government from a single place to several smaller ones.

Types of (de)centralization

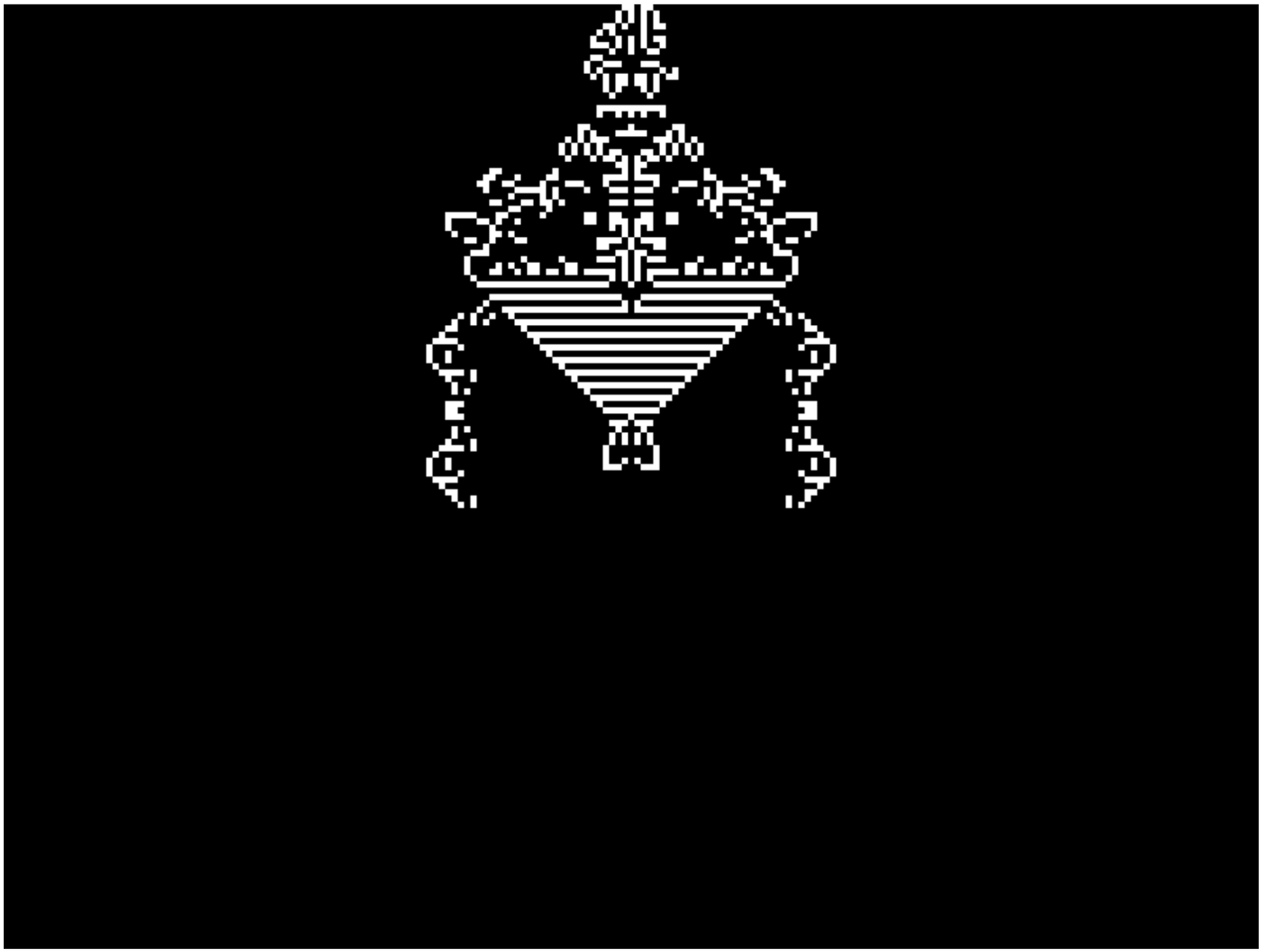
Architectural
(Location)

Political
(Authority)

Logical
(Consensus)

Centralized systems

Decentralized systems

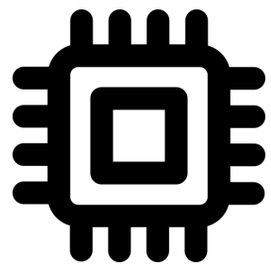


https://youtu.be/C2vgICfQawE

Decentralization in Nature

Decentralization in Society

Decentralization in Computing

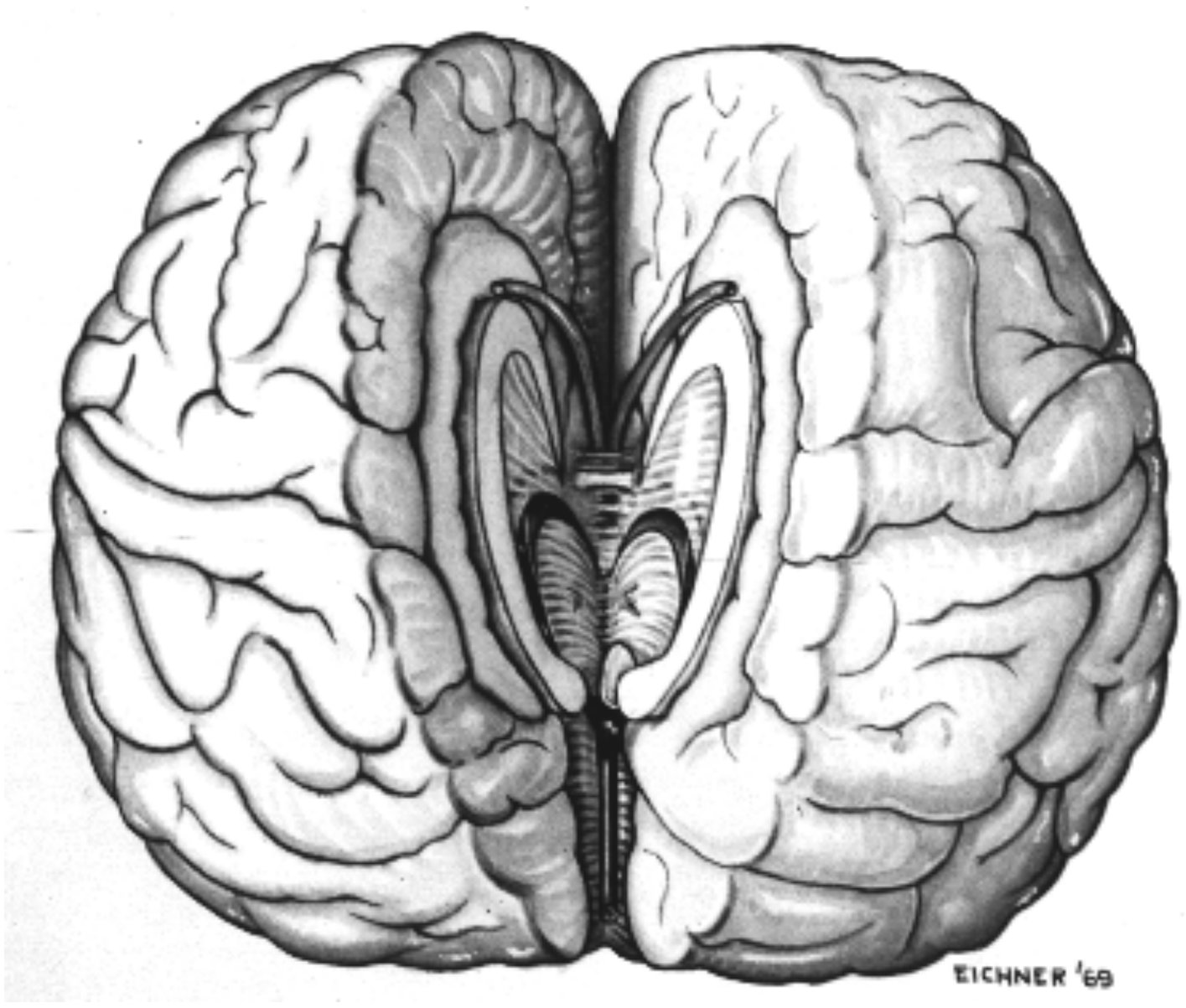


Consensus and Byzantine Fault Tolerance

Consensus /kənˈsen.səs/

A generally accepted opinion or decision among a group of people.

Network splits



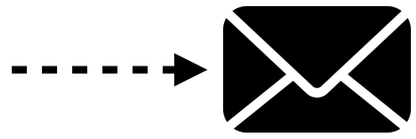
Strong consistency

Authority?

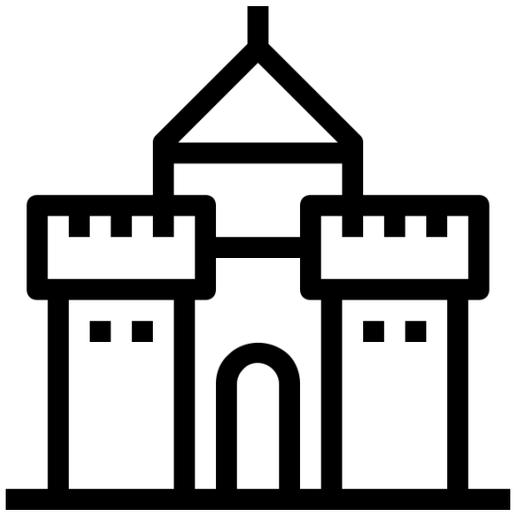
Consensus algorithms

Trust?

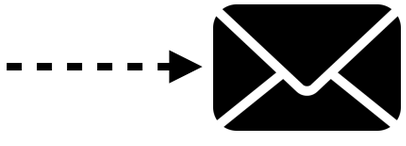
The two generals problem



Attack at dawn



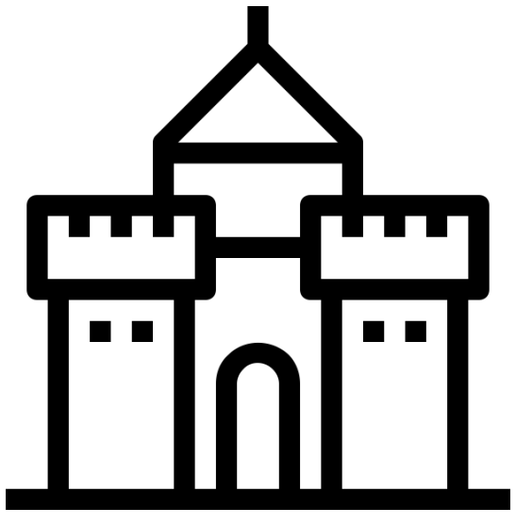
ACK



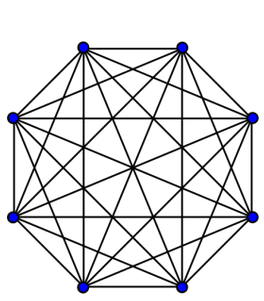
ACK'

ACK''

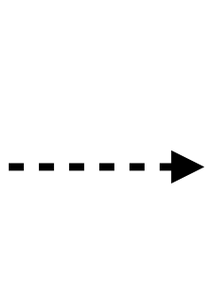
The Byzantine generals problem



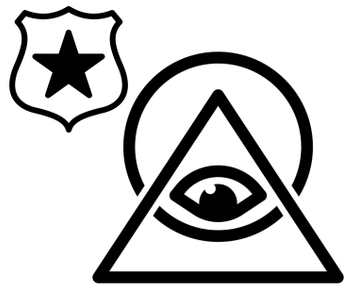
Scalability of trust



Complexity of trust
$O(N^2)$



Trusted generals



Centralization of authority

Governance, Economics, and Proof-of-Work

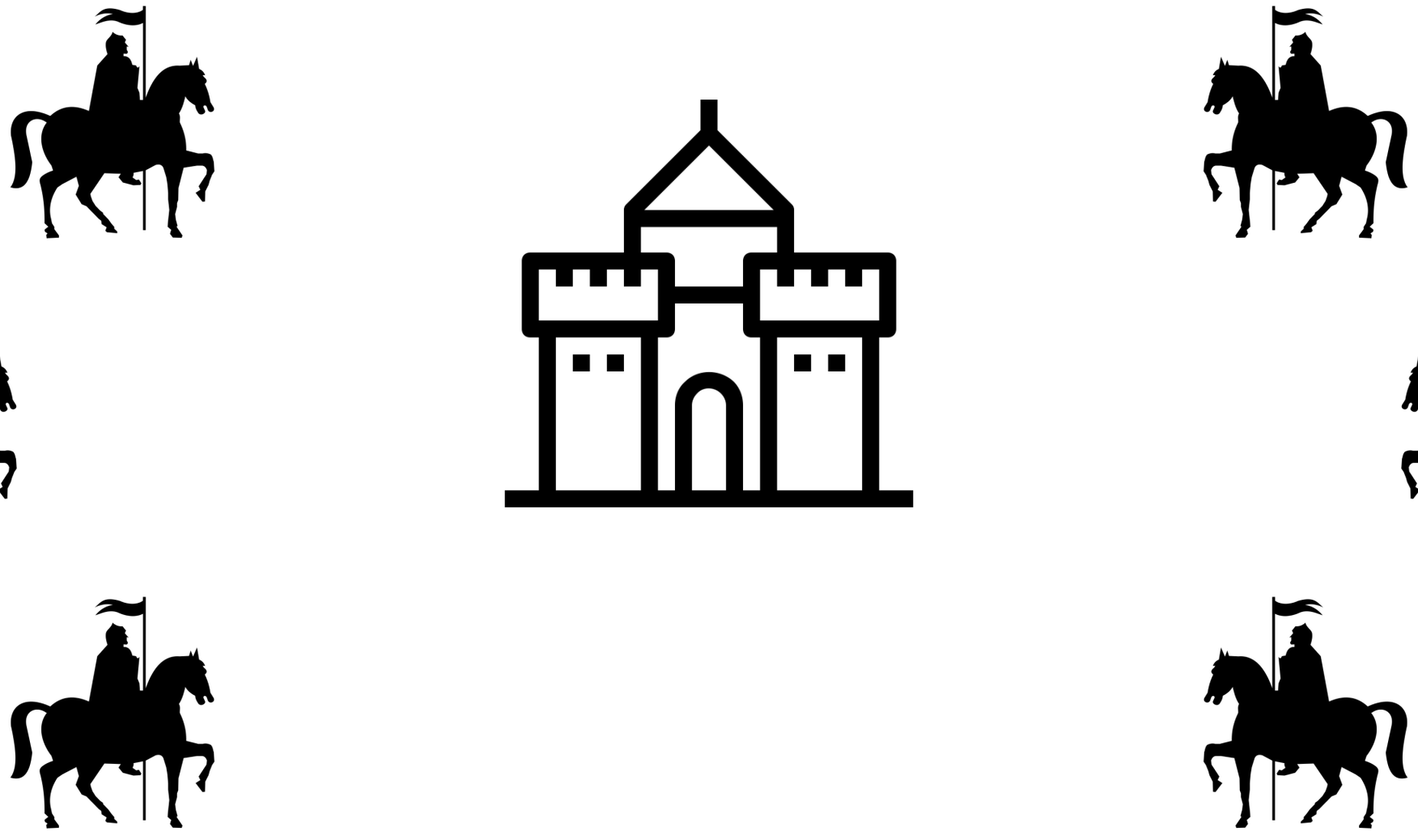
Governance /ˈgʌv.ɚ.nəns/

The way that organizations or countries are managed at the highest level.

Economics /ˌiː.kəˈnɑː.mɪks/

The social science that studies the production, distribution, and consumption of goods and services focusing on the behaviour and interactions of economic agents.

The siege

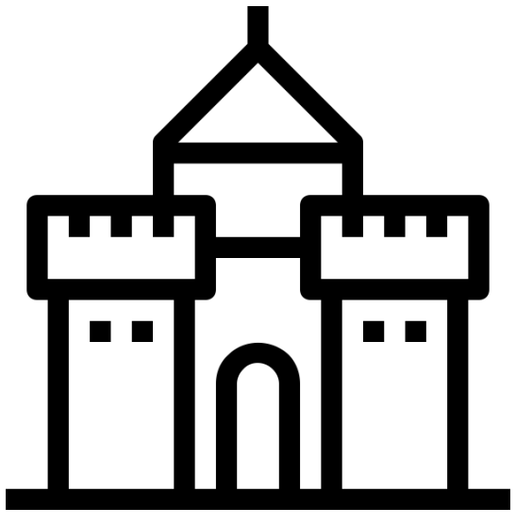


Attack or retreat?

Abort!

Go go go!

🤞



Let's go back!

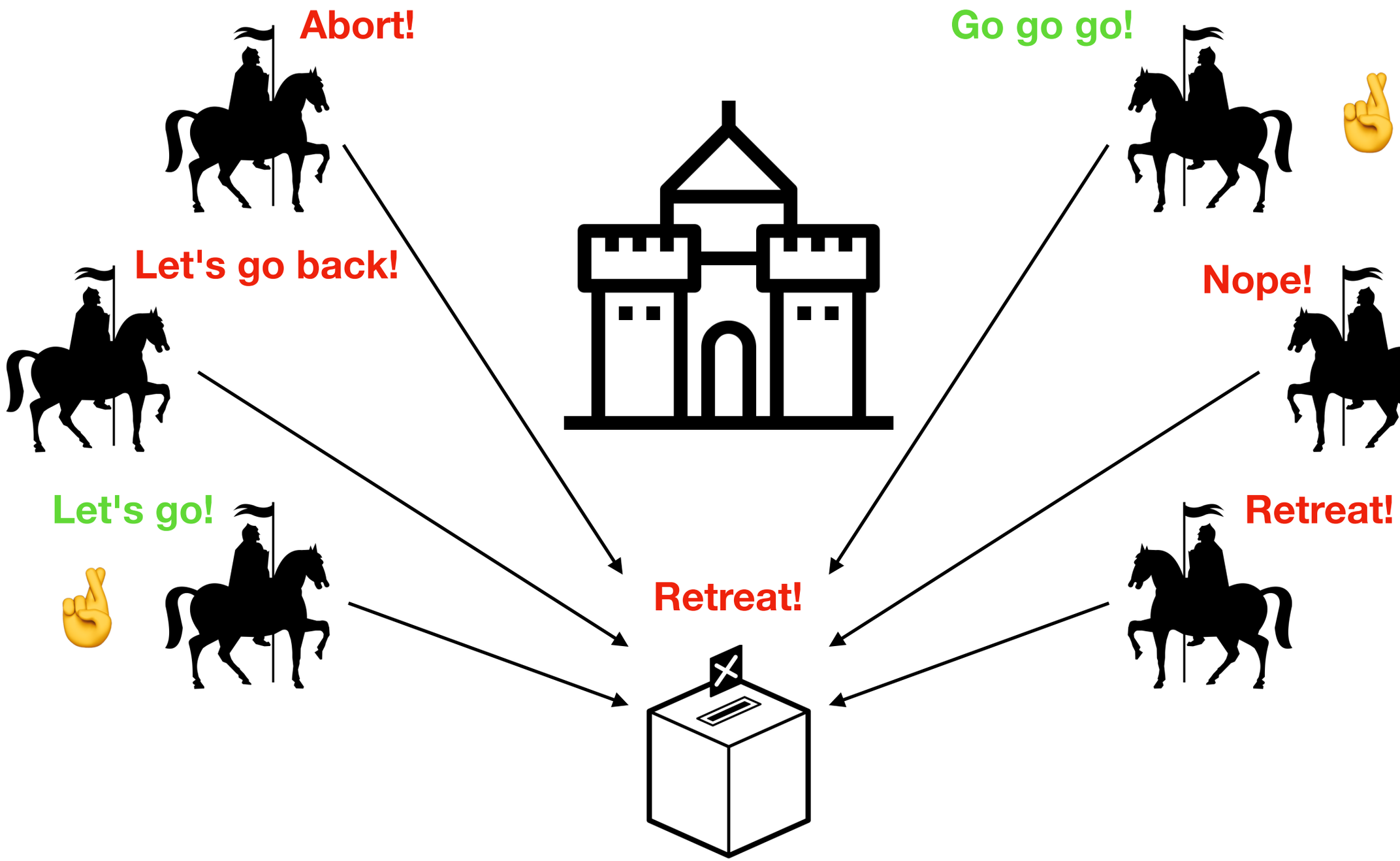
Nope!

Let's go!

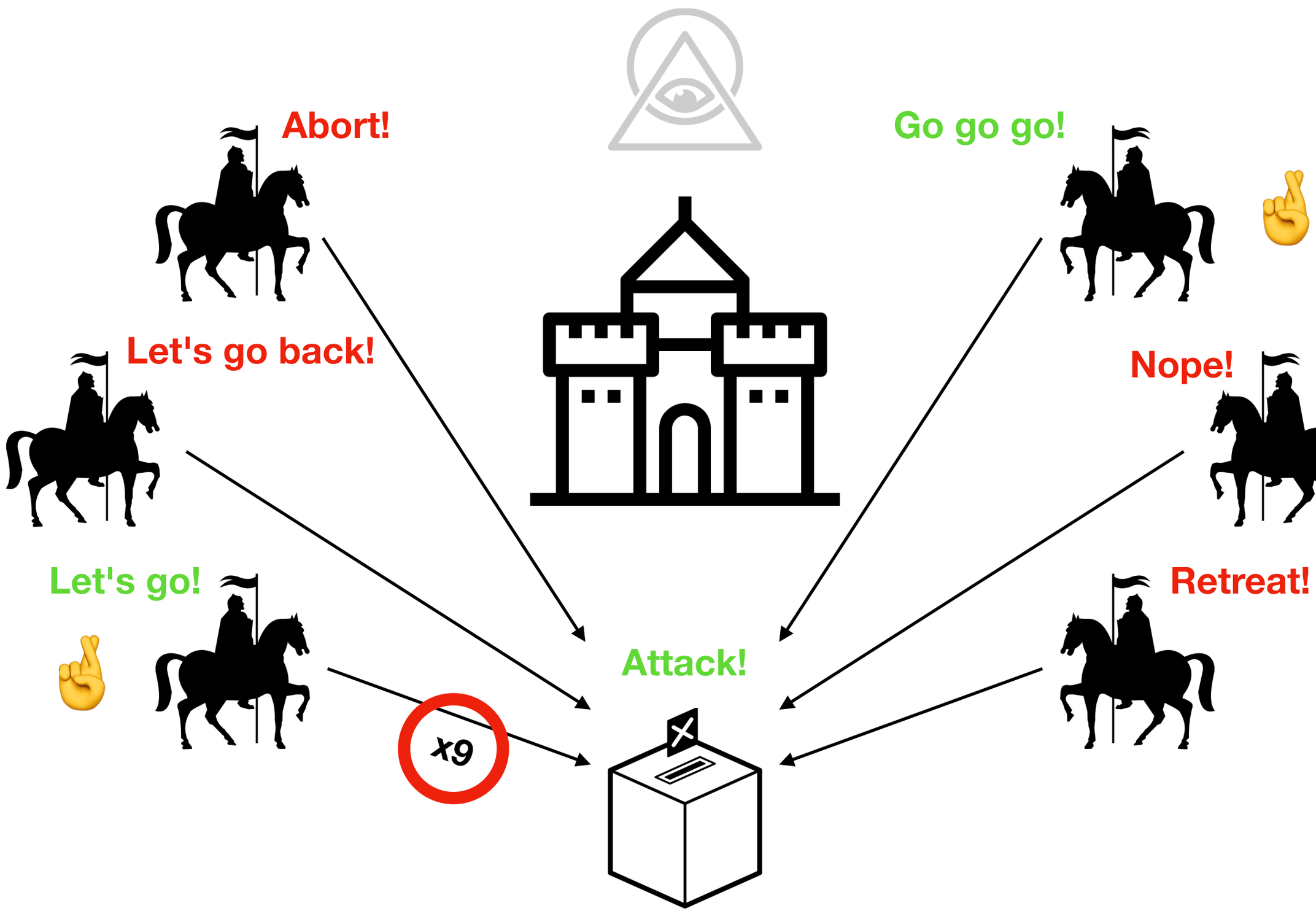
🤞

Retreat!

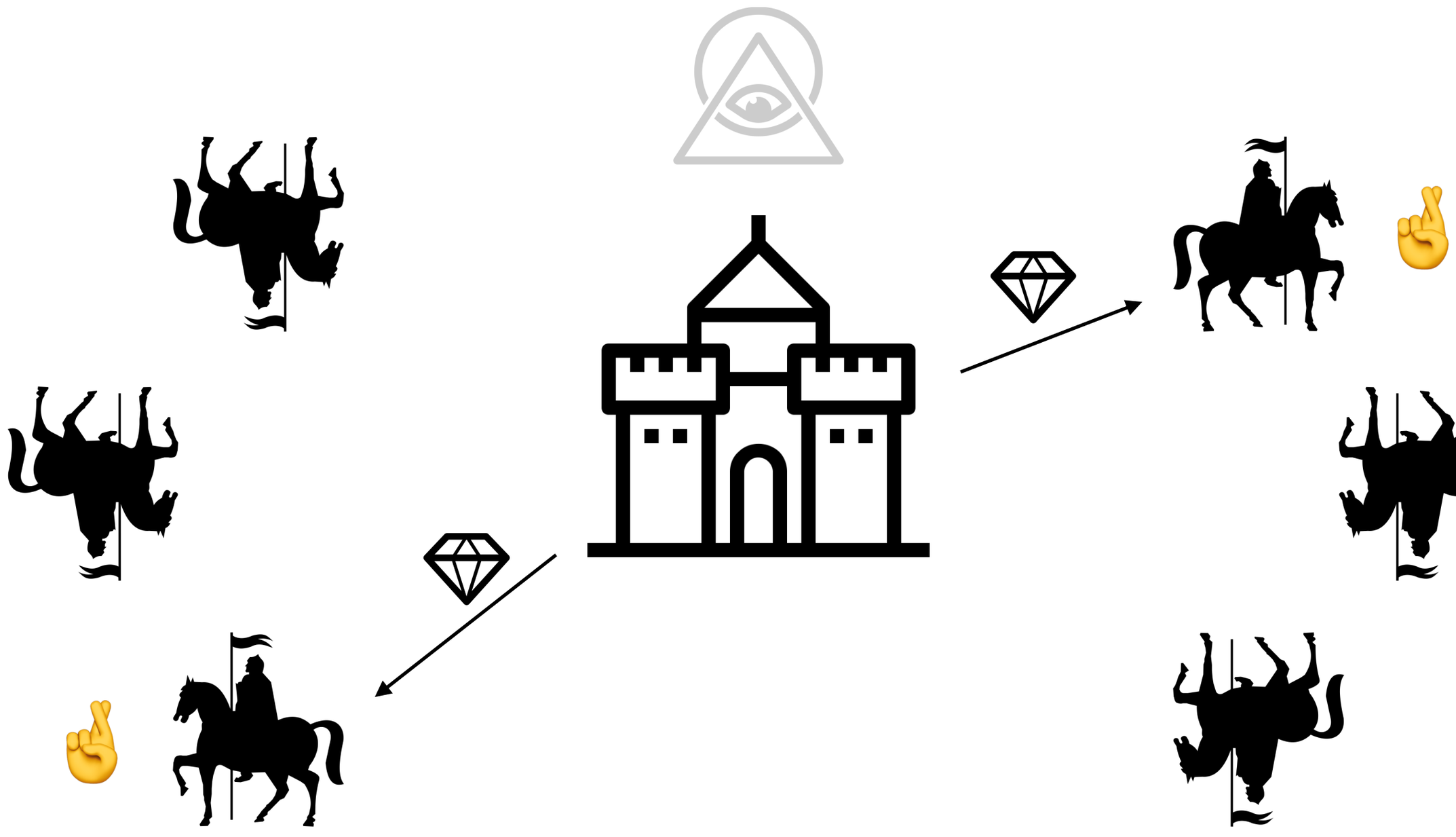
Let's vote


Abort!
Go go go!
Let's go back!
Nope!
Let's go!
Retreat!
Retreat!
Retreat!

No central authority

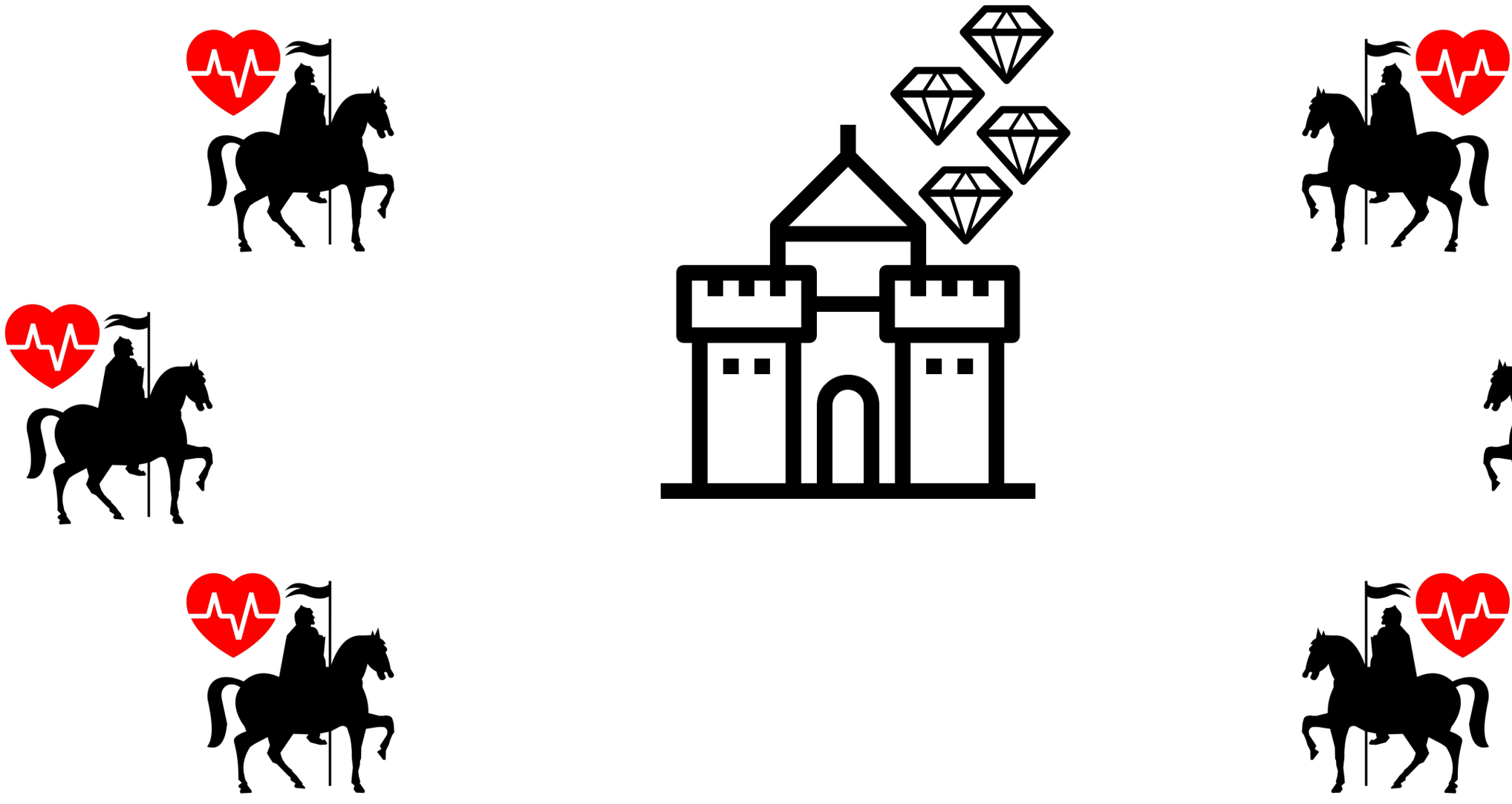


Treason ensues!

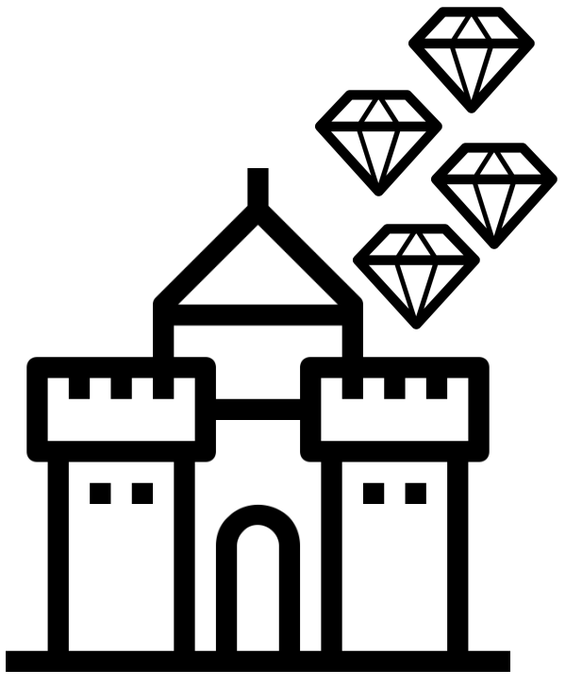


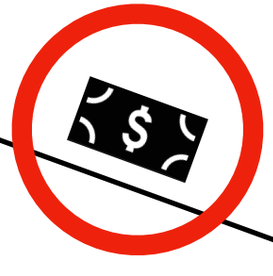
Proof of Work~ish

Economics in war

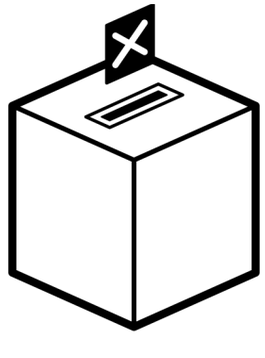


Expensive voting





Consensus!

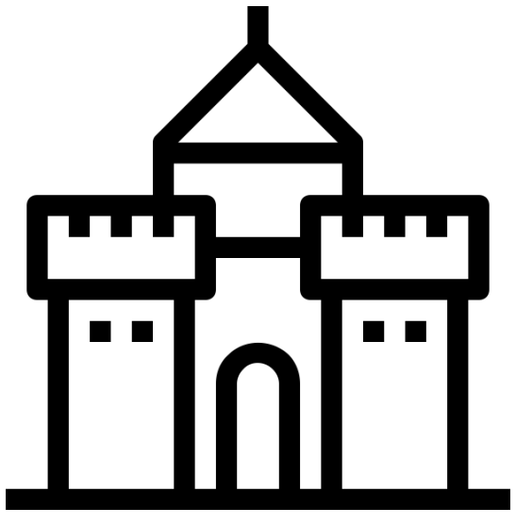


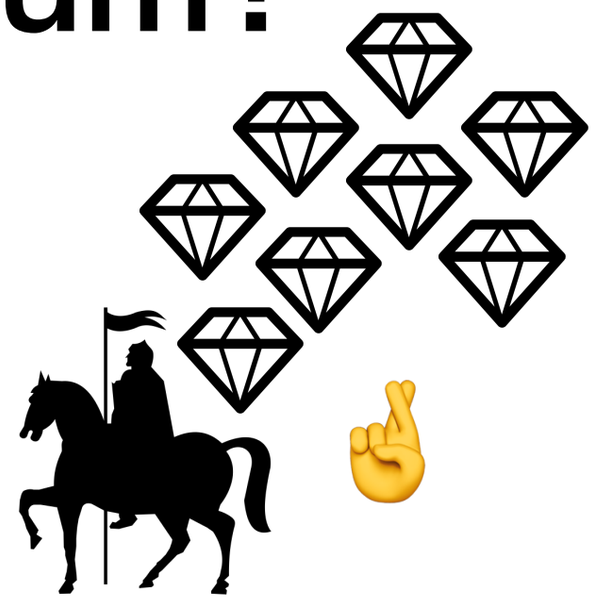
Dominant strategy

$$reward_i = (loot / N) + valueOfStayingAlive_i - (voteCost * votes_i)$$

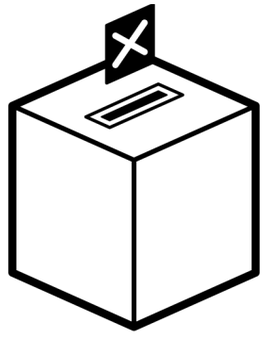
voteCost > ???

Breaking the equilibrium?





???



Bitcoin and the Blockchain

Bitcoin /ˈbɪt.kɔɪn/

A purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution.

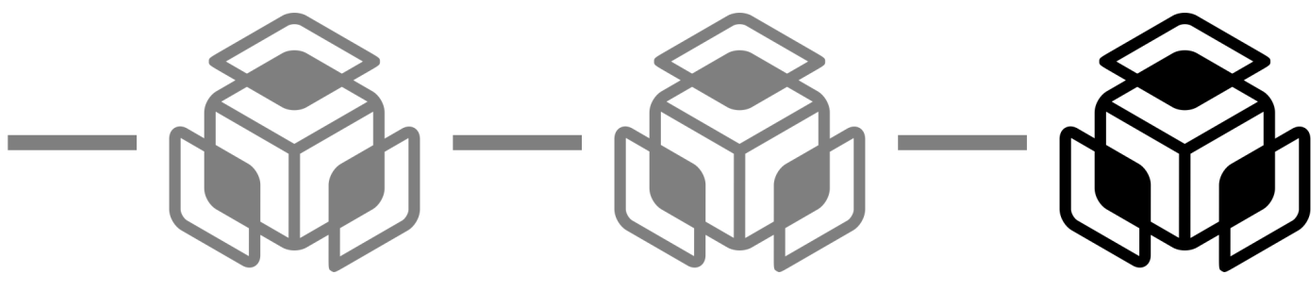
What is Bitcoin, really?

🤔

A database*

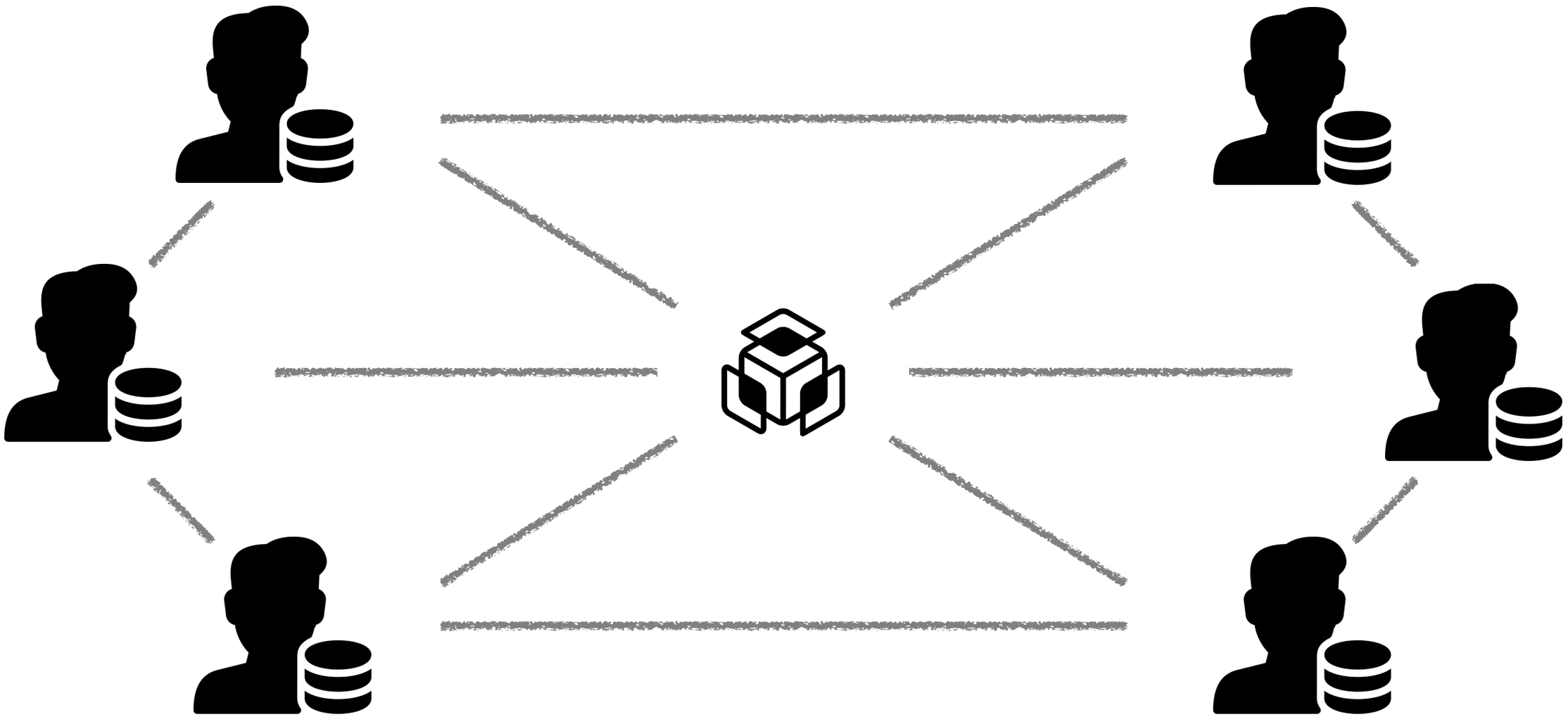
Unrestricted read
Unrestricted write *
Append only

≃



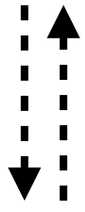
Blockchain:
Linked list of
state updates

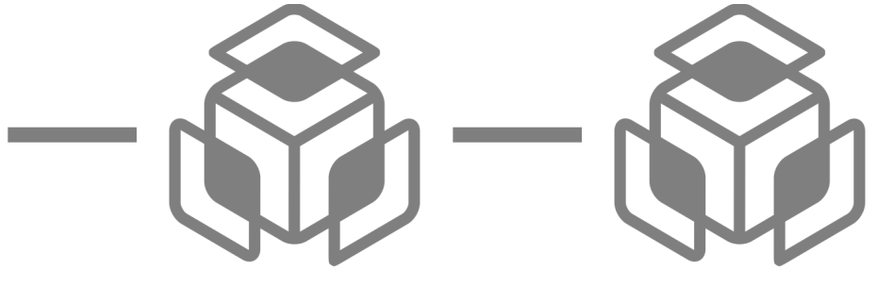
Bitcoin network



Bitcoin protocol

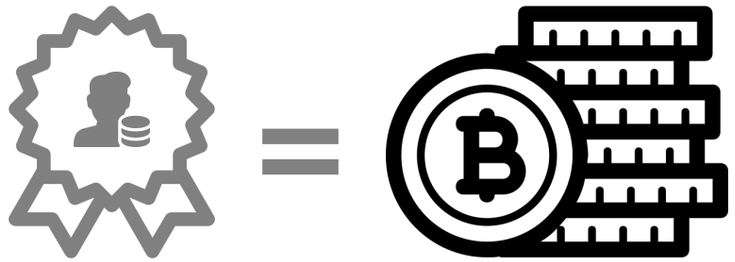
Describes valid blocks



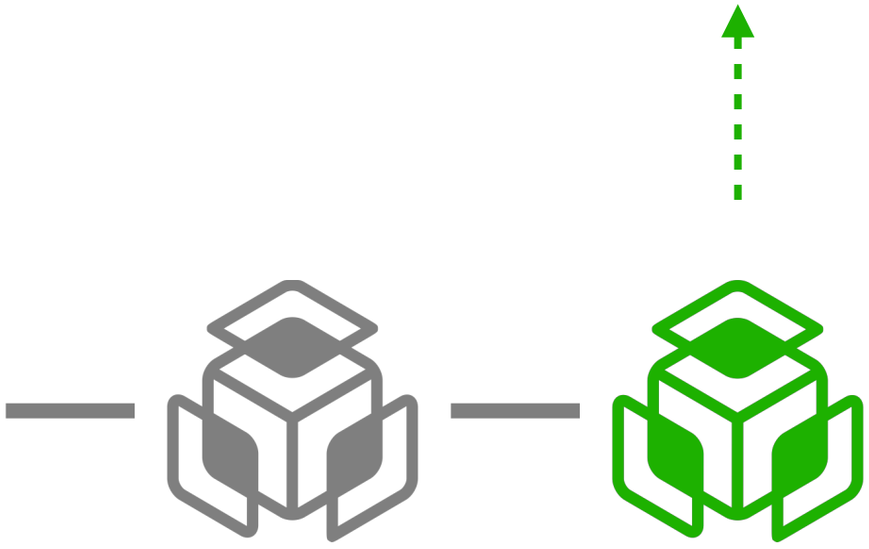


Will others take my block?
Should I take this block?

Bitcoin

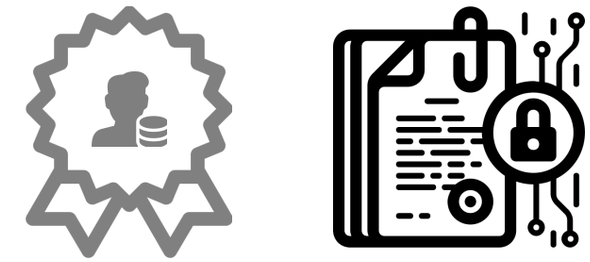


Measure of reward
Granted to block issuer
Described in the protocol

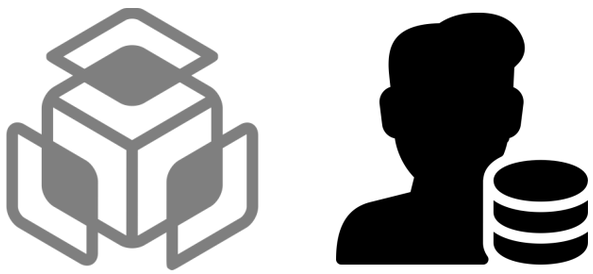


New valid block arrives

Bitcoin transactions



Transmission of ownership
Described in the protocol



Broadcasted
Validated by peers
Inserted in blocks

A few problems

Not a cost-free service

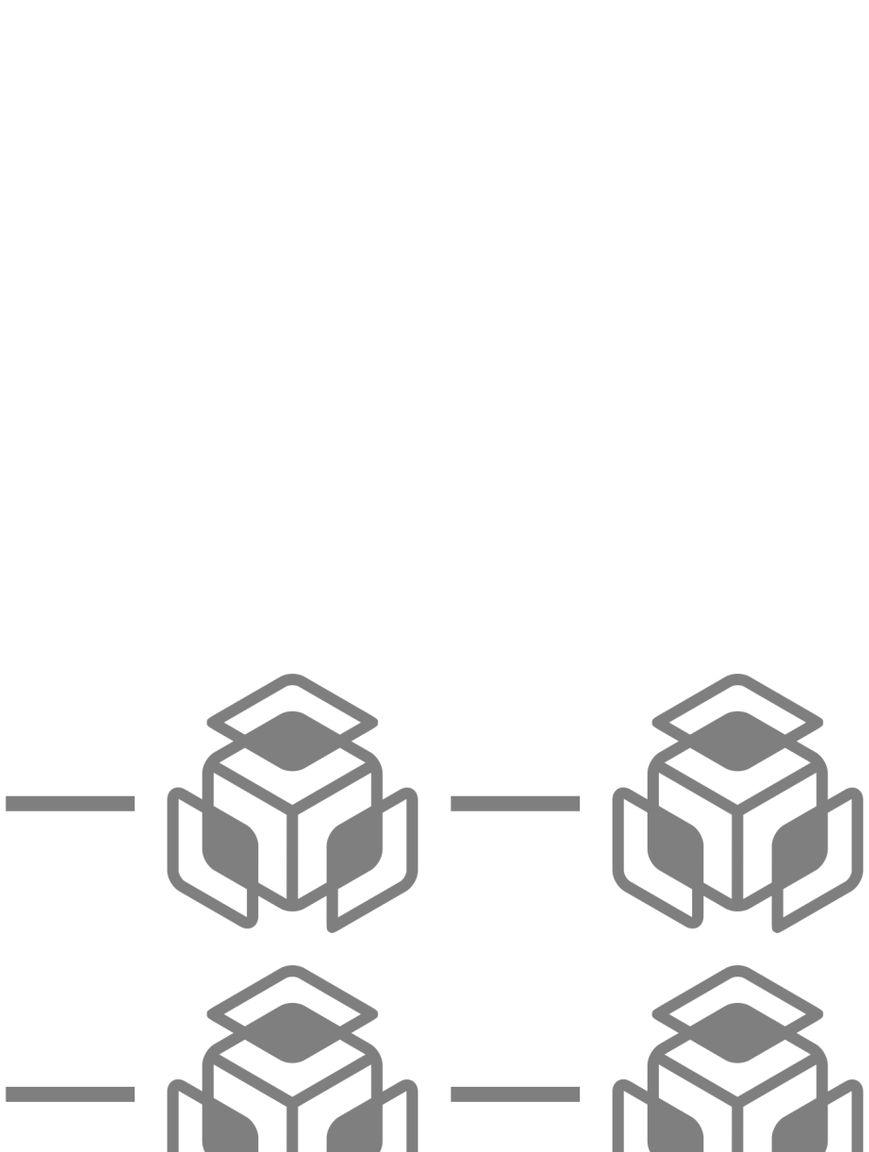
Not everybody is trustworthy

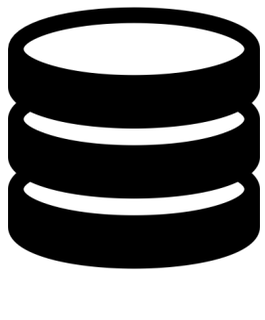
Reward's worth is subjective

So...

WHY does this work, really?

Utility and cost

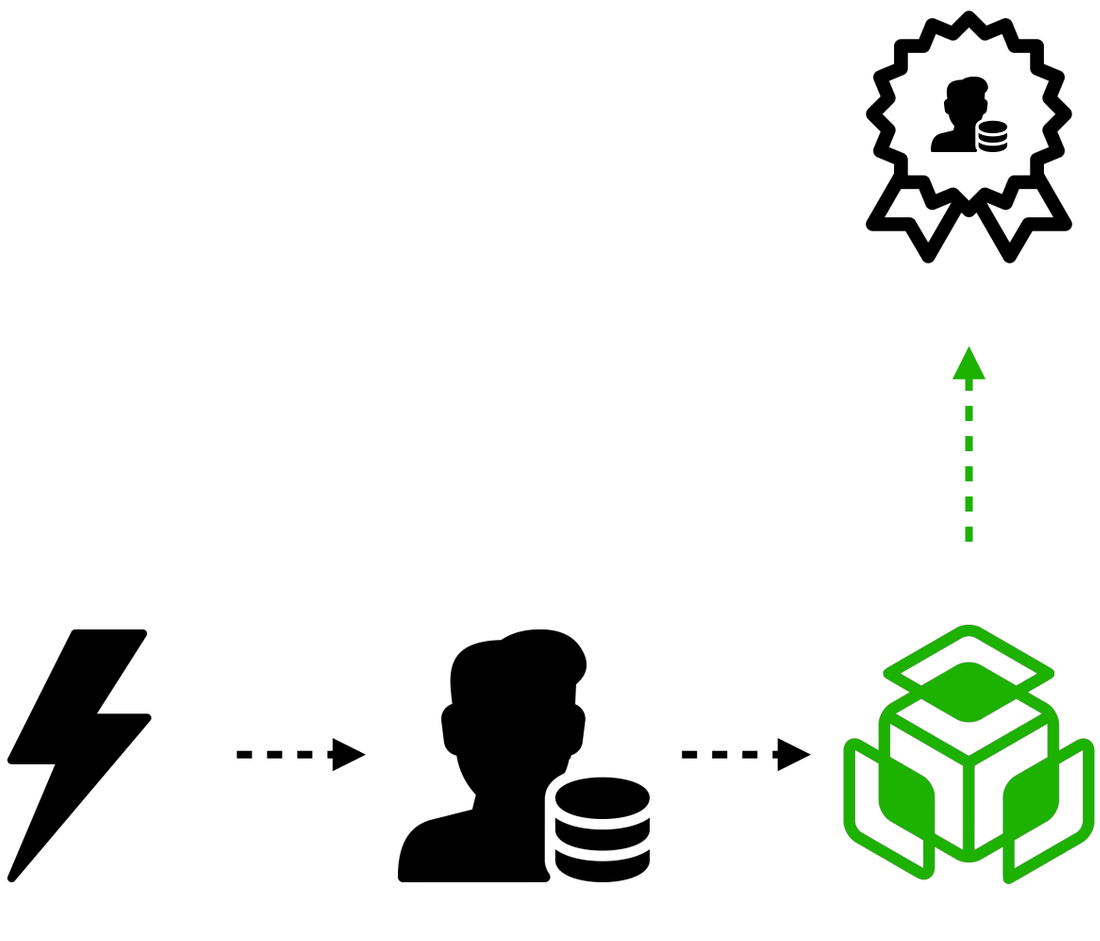




≃

Permission-less
Resilient
Not cost-free

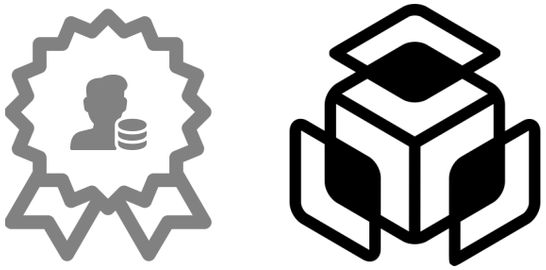
The mining game



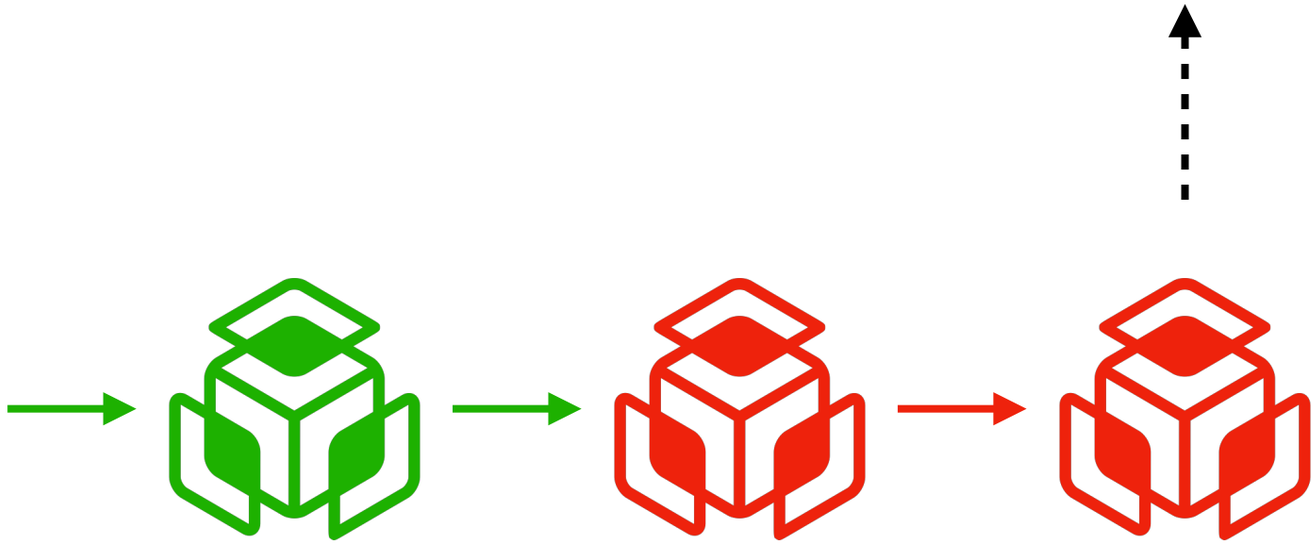
Valid blocks are rewarded

Miners use CPU cycles
They produce valid blocks

Validity chain

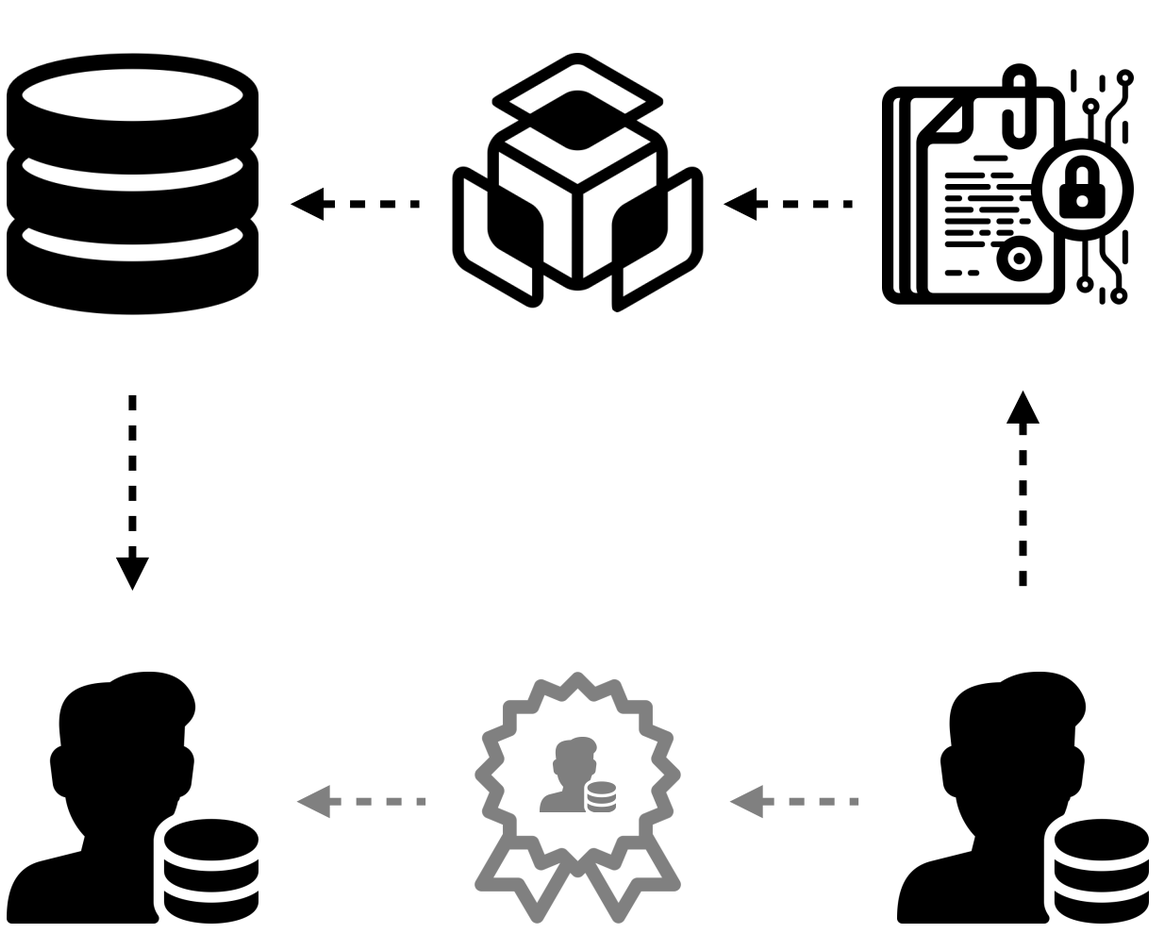


Is this new block valid?



Validators require past blocks

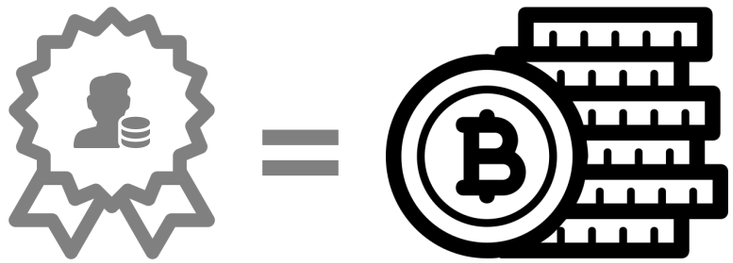
Reward ledger



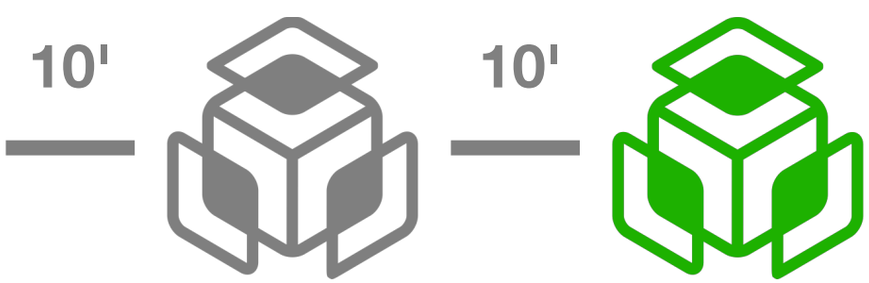
A database of transactions

Anybody can broadcast
Nobody can censor *
Everybody can read

Bitcoin as currency

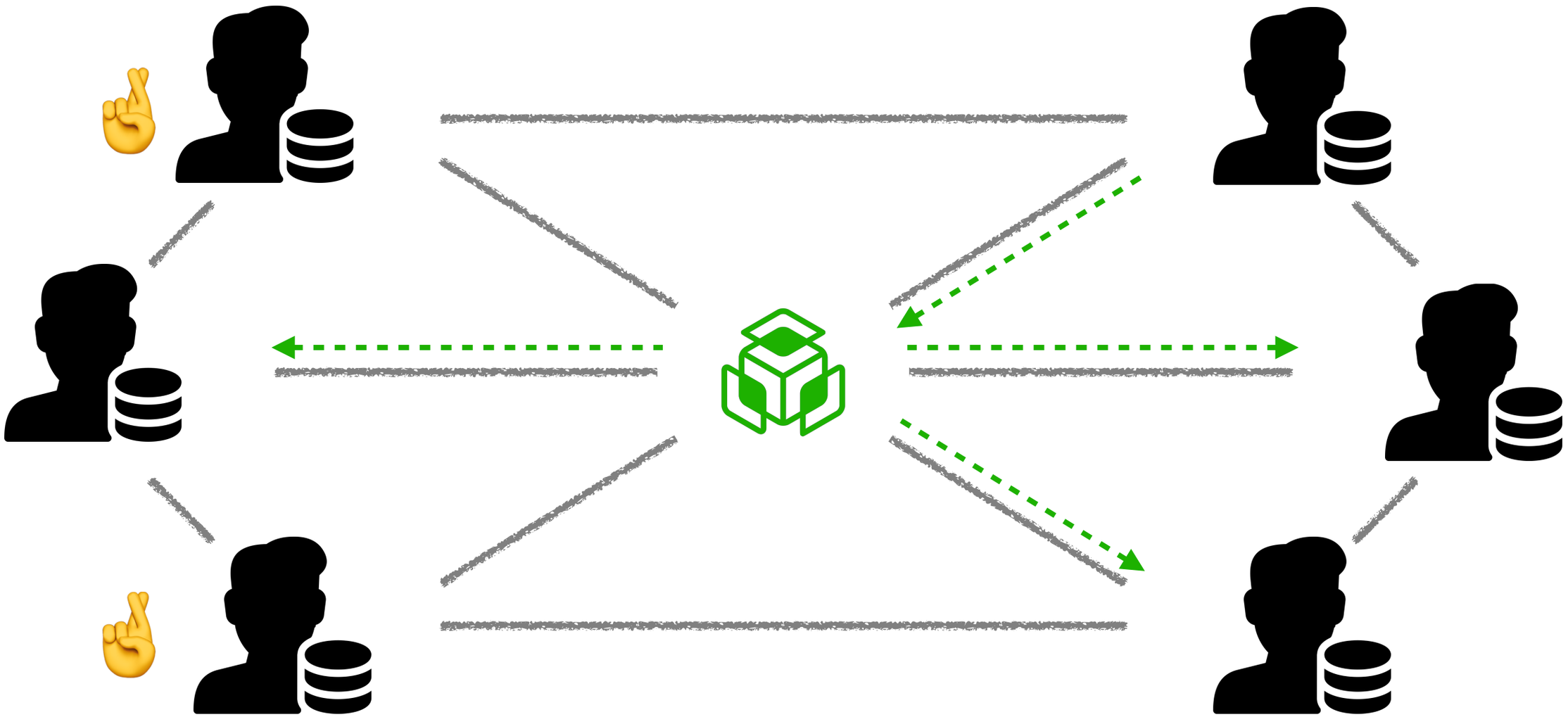


Portable
Scarce



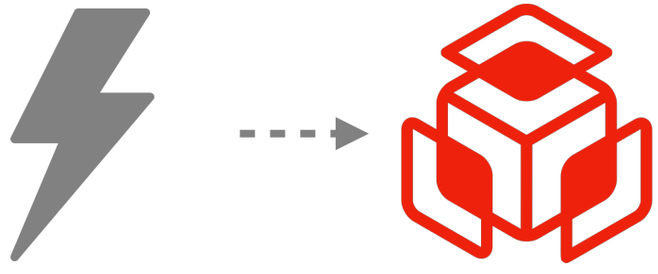
Block creation is rate-limited
Reward is not infinite

Censorship resistance



Sybil attack resistance

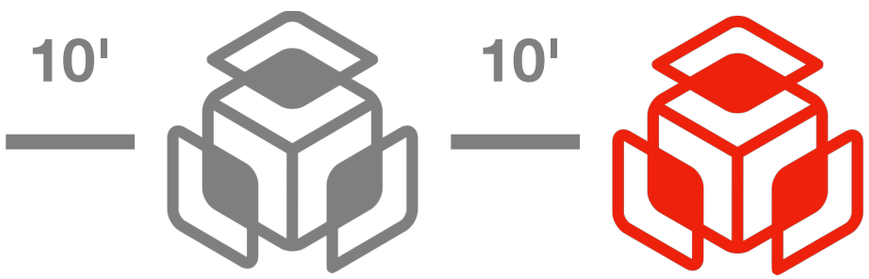
Power into valid blocks
Honest nodes make profit



Power into invalid blocks
Malicious nodes gain nothing

Race condition resistance

The longest chain rule
Most work invested



Adjustable difficulty
Rate-limits updates

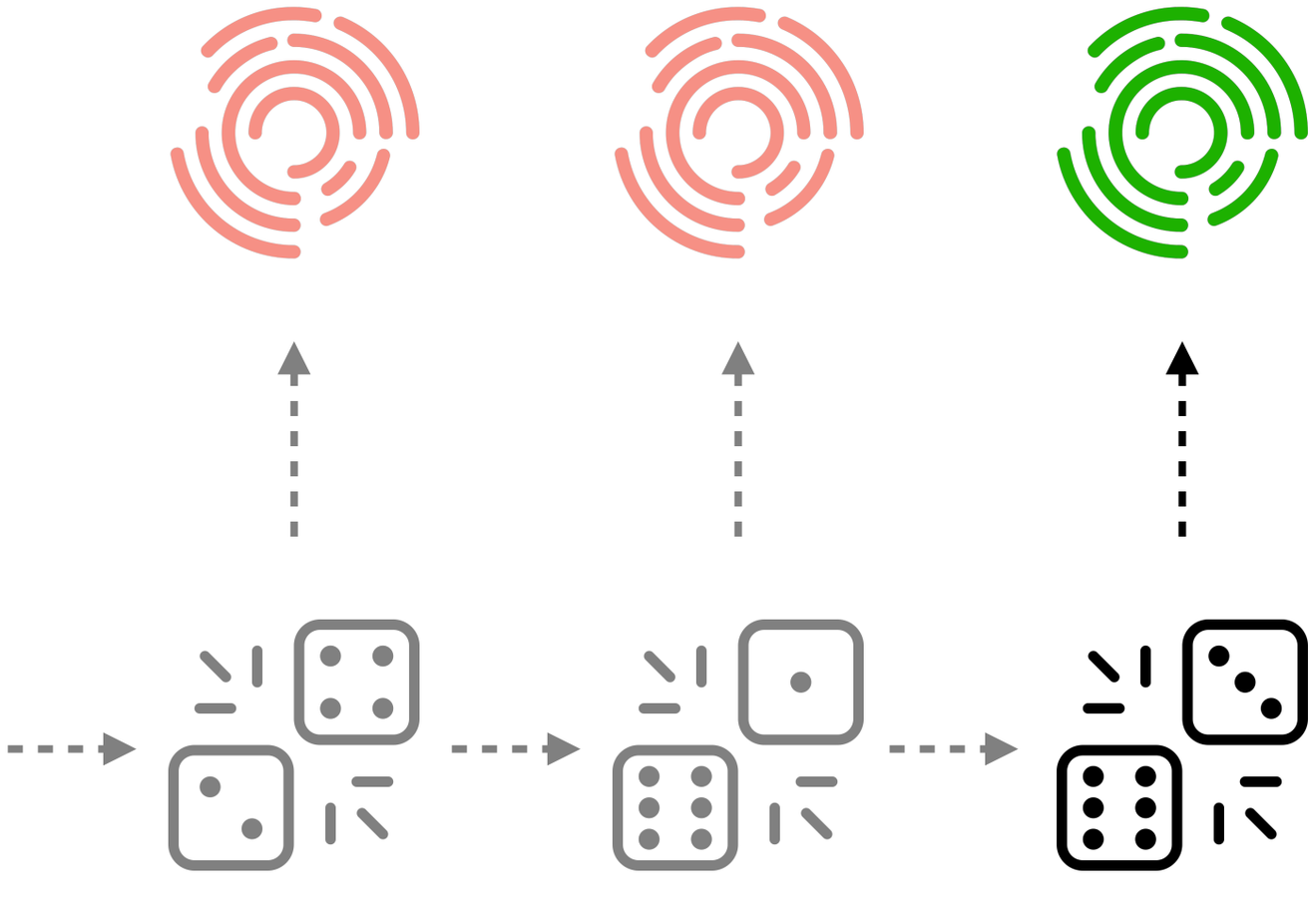
Proof of Work in Bitcoin

Block hashes

Double SHA-256

Hash of the previous valid block
Valid bitcoin transactions
Nonce

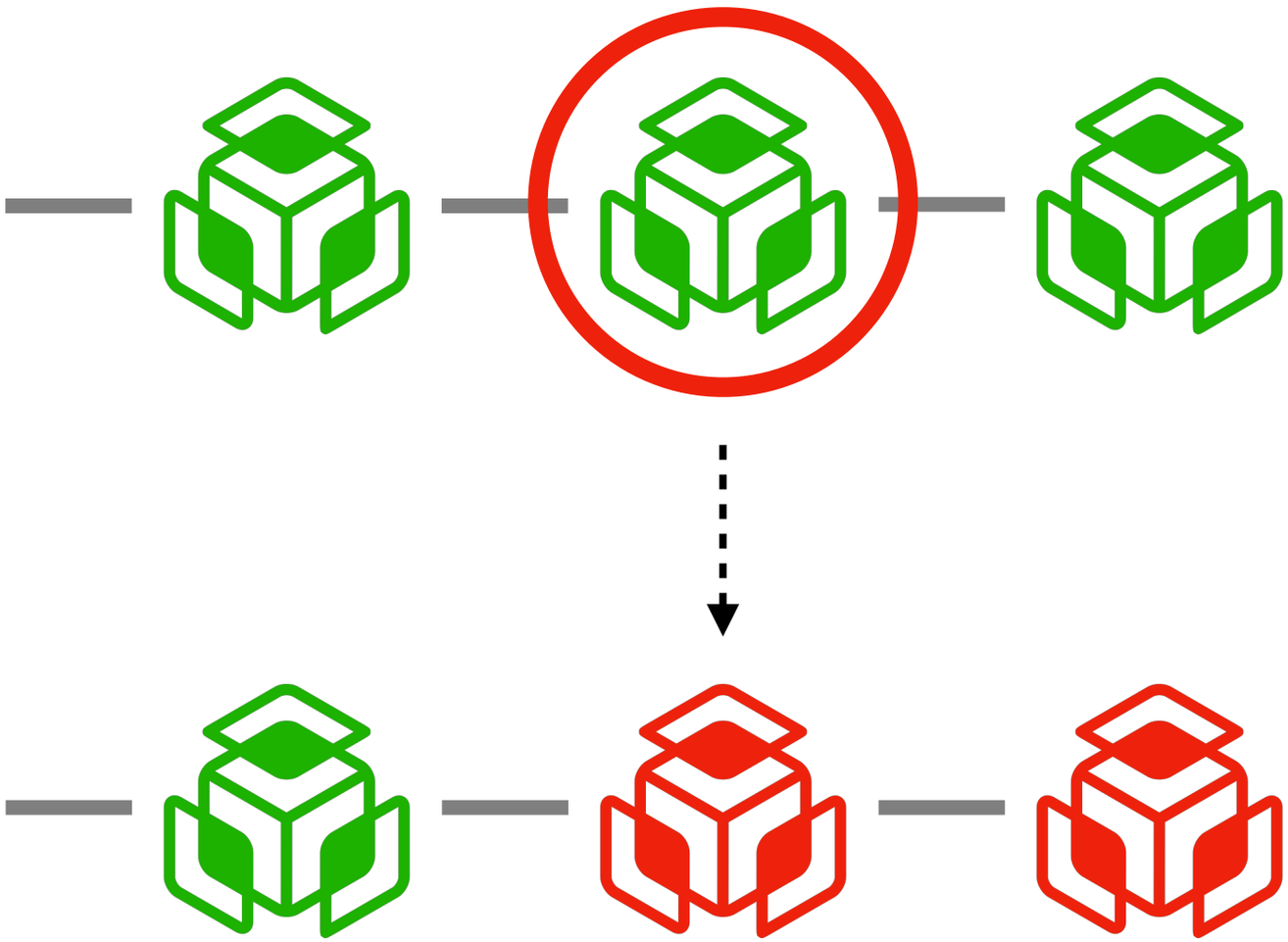
Block mining



Valid hash:
0000000000000000001b13...

Nonce increases
CPU used in SHA-256

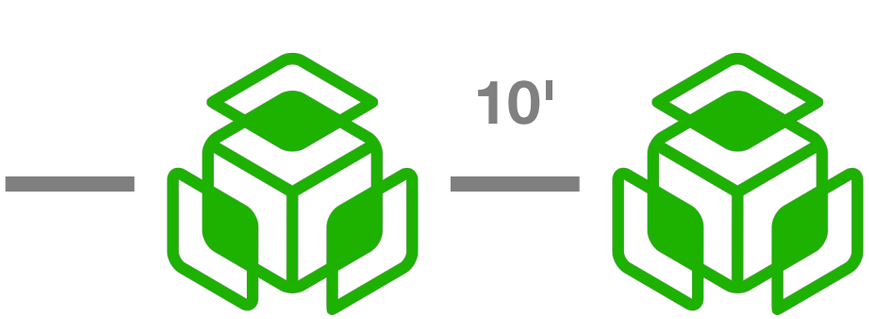
Tampering with the past



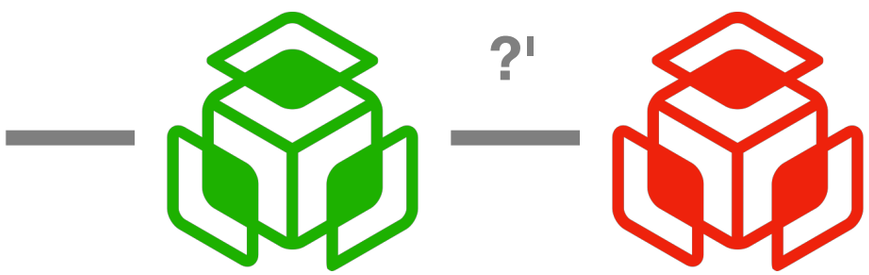
Blocks can be altered locally
Hashes become invalid

Invalid blocks must be re-mined
Attacker must spend CPU

Single version of truth



Honest chain keeps growing



Attacker must outrun network
51% attack would allow this *

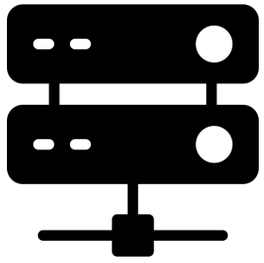
Bitcoin applications beyond cash

Ethereum, Smart Contracts, and Decentralized Applications

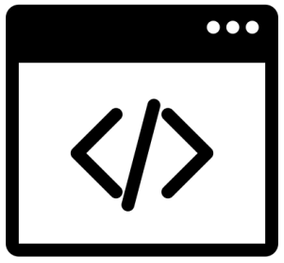
Contract /ˈkɑːn.trækt/

A legal document that states and explains a formal agreement between two different people or groups, or the agreement itself.

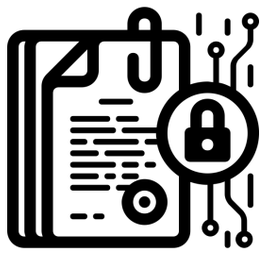
Ethereum



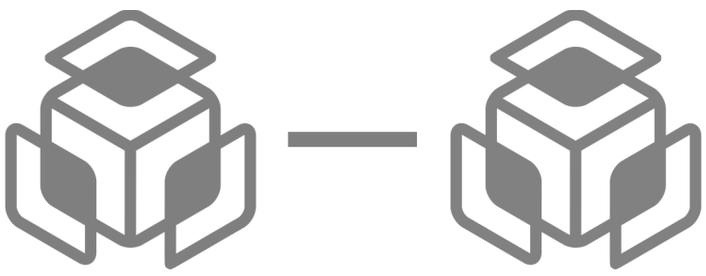
A computer *



Turing-complete language



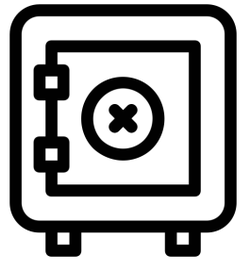
Arbitrarily complex transactions *



Smart Contracts

Agreement between parties

Protocol to perform on promises



Breach is expensive

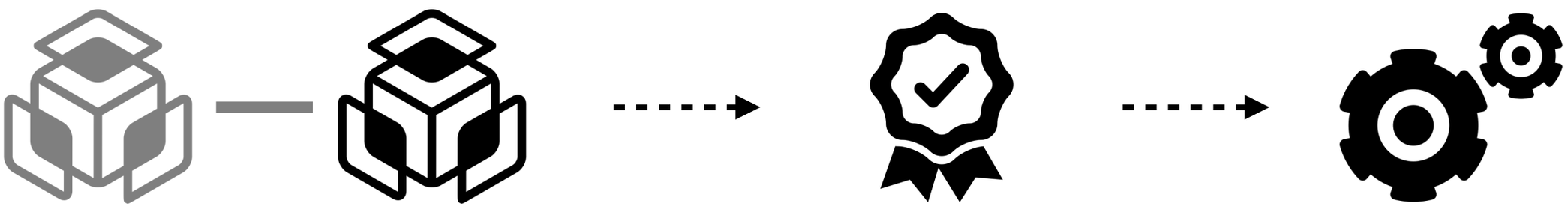
Contract design

Who can resolve disputes?

Reactive enforcement

Proactive enforcement

Decentralizing contracts



Arbiter replaced by the blockchain

Reduced need for trust in humans *

Higher degree of automation

Decentralized apps

Golem

Decentralized computing

Gnosis

Crowdsourced knowledge

Etherisk

Decentralized insurance

Colony

Decentralized business

Aragon

Decentralized court systems

Decentralized digital nations?

The Future of Decentralization