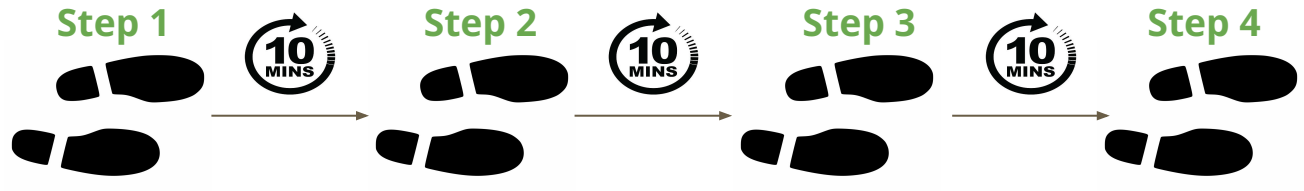
Nakamoto consensus

What, how and why

Blockchain

One-way step function



Id: 00A3D1
From: Genesis

Id: 008F2C
From: 00A3D1

Id: 006B8B
From: 008F2C

Id: 00F1BA
From: 006B8B

Rules?

... ... how do we agree on the next step?

Consensus

Who decides on the step? How do we vote?

VS

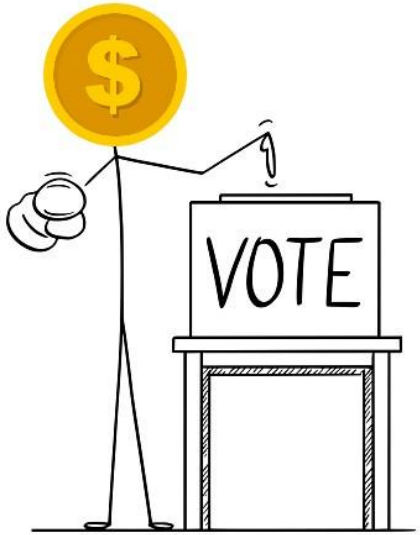
- Individual with too much power
- Easy to stop/DOS
- Concentrated which can lead to manipulation

- Can’t have real life voting - too slow & “too political” i.e. easily manipulated
- … how do we do it?

Traditional consensus

10 Million people (coins)

Assigned voting day



Traditional consensus - implementation

Making a step:

- Pick randomly someone from the set to define what the step looks like
- Choose a random subset of citizens to vote on a step & require majority of votes

Verifying a step:

- Validate random selection of subset
- Validate the description of the step

In ideal conditions, this is not a bad design of a one-way step function

Traditional consensus - problems

Voting properties:

- Voting citizens are public because they're coins
- Voting results are public (public voting)

What if ...

- I duct tape voters to a tree?
- Voters produce two different steps both of which seems valid (weak subjectivity)
- Circularity - Voters vote on who will be in the set of all voters

Traditional consensus - summary

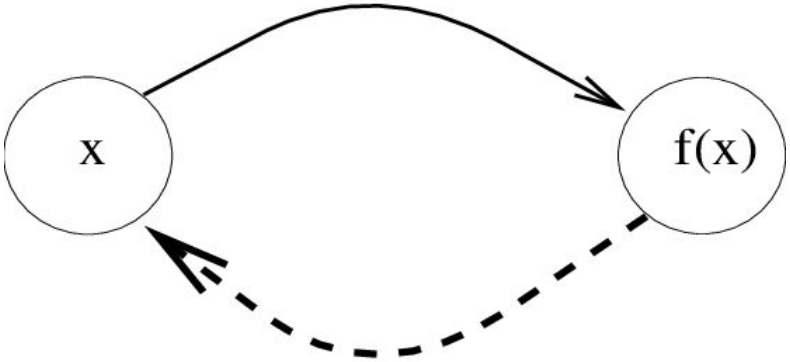
Ugh, ogh: 

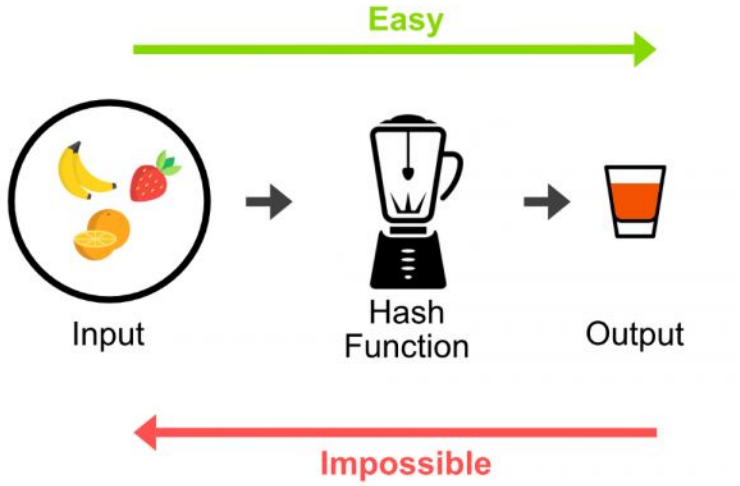
1. Public voting
2. Closed set of citizens (permissioned)
3. Can be stopped (at least theoretically)
4. Requires trust in case of forks (weak subjectivity)
5. Circularity of voter set definition

Yay: 

1. Can reach a final agreement in good scenario (finality)
2. Low CO2 emission (only a few computations)

One-way functions





1. Given x, it’s easy to compute f(x)
2. Given f(x), it’s *very* hard to get to x

Nakamoto consensus

BITCOIN

A PEER–TO–PEER
ELECTRONIC
CASH SYSTEM

Abstract. *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.*

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

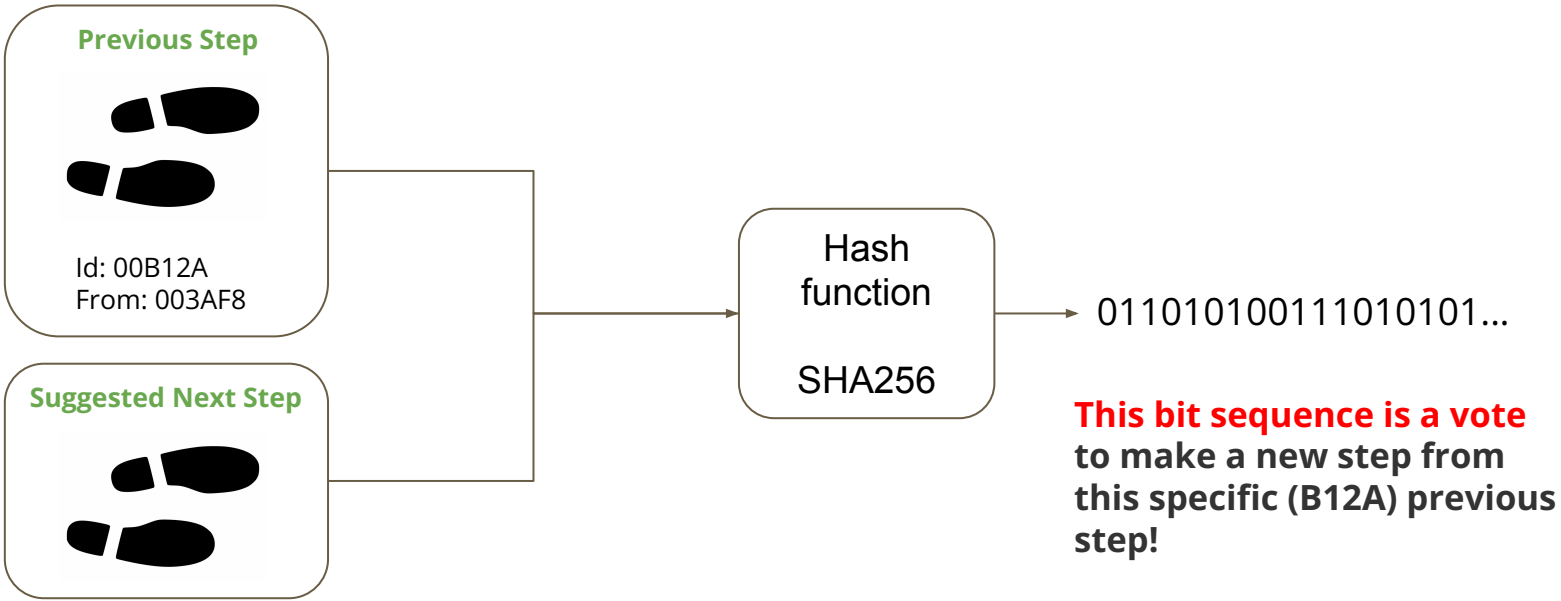
Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

Step = sequence of transactions!

Everyone agrees which transactions happened!

Voting?

PoW vote



This bit sequence is a vote to make a new step from this specific (B12A) previous step!

The vote itself can be used as the next step identifier!

Counting votes

It takes ~4 votes to produce a vote that starts with 2 zero bits, ~16 votes to produce a vote that starts with 4 zero bits etc.

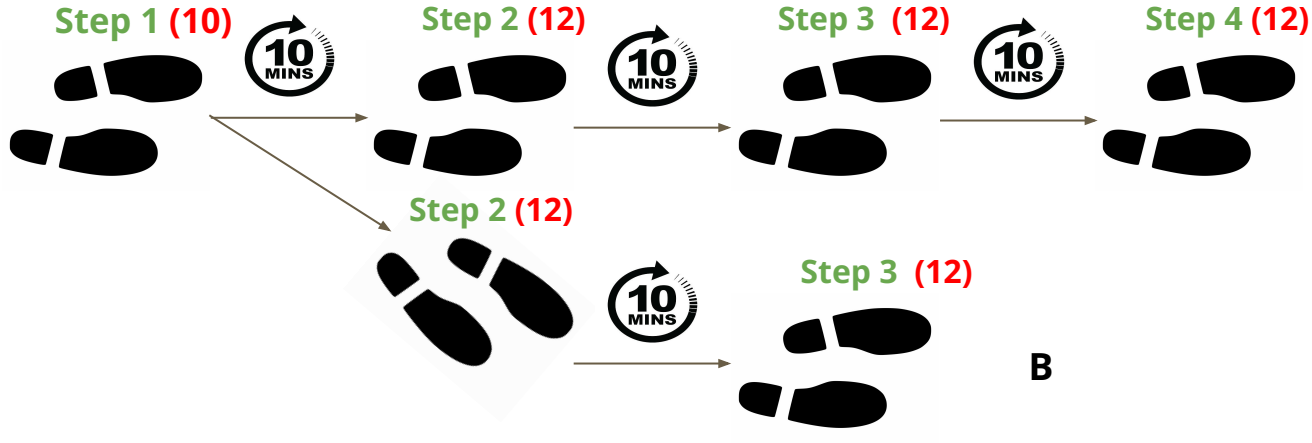
A vote that starts with 10 zero bits is a **proof** we collected ~2^10 votes.

We can now **verify** we collected (roughly) a specific number of votes by showing a single vote!

But wait... what if

- I vote twice?
- What if we collect two valid proofs with a different step?

Convergence to common reality



Two global societies?!
Which one is real?

Solution:
Add a rule: Build on the step whose history has the most collected votes in total. A wins with 46 votes over 34 from B. **No weak subjectivity!**

Consensus through a computational sybil attack?

We created a voting competition where the one with the most total votes wins.

What's an asic miner then?

Anti-reorg Incentives because you're invested!

Get compensated for providing a proof of collected votes!

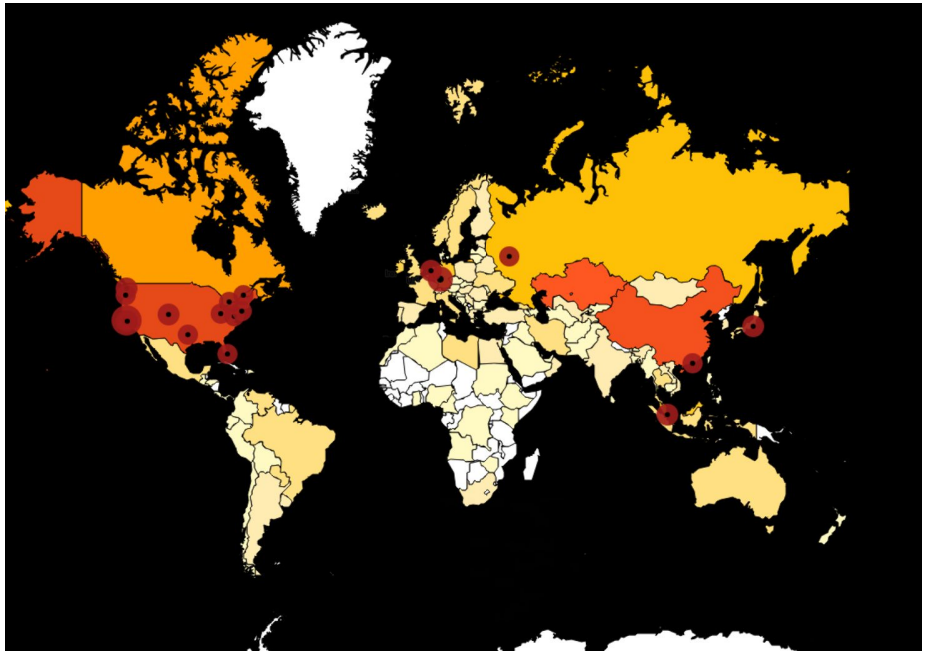
Not money printer, but a vote printer.

Nakamoto consensus properties

- Inclusive (permissionless)
- Blind voting
- Blind vote producers
- Consensus by value
- Asocial
- Trustless

Exa = 10^18 = 1,000,000,000,000,000,000

265 EH/s
= 265 * 10^18 hashes/s
= 265 * 10^18 votes/s



How many votes do we need to collect?

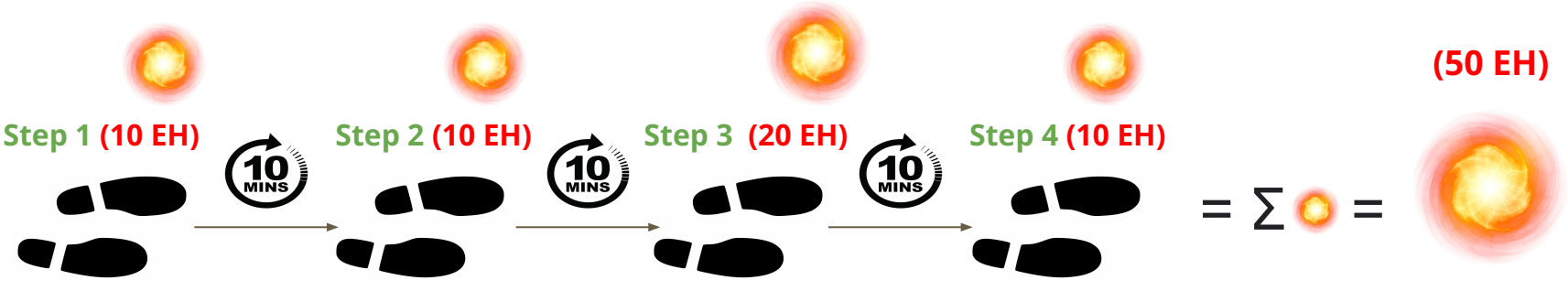
Walking too fast or too slow?

Make a step every 10 minutes

DAA

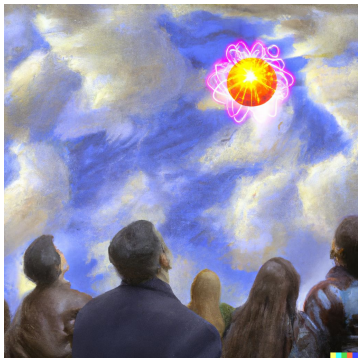
Slow? Still MUCH faster to move than gold.

Voting -> Energy



Steps build on one another. Each subsequent step hardens **all** the previous steps. And it hardens them with **physical** energy commitment proof. **No exploits!**

We simply follow the mass of energy.



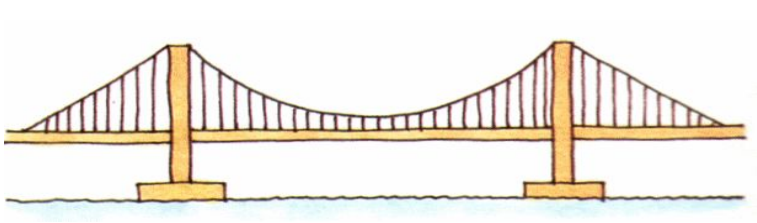
Differences traditional/nakamoto

- “Type” of democracy (permissioned vs permissionless)
- Nakamoto consensus is unstoppable and trustless
- Permissioned set of voters has some advantages:
  - strong consistency of steps (fast finality)
  - no/low CO2 emission
- And...

Biggest difference - The voting asset

Digital world (cyberspace)

Nakamoto consensus
A mental construct with a **physical vote function (energy)**



Proof of Stake consensus
System is **100% mental construct**

Real world (physics constraints)

Why physics?

Who are we defending from?

Which system we have absolutely no idea how to exploit?

We inherit the security from physics!

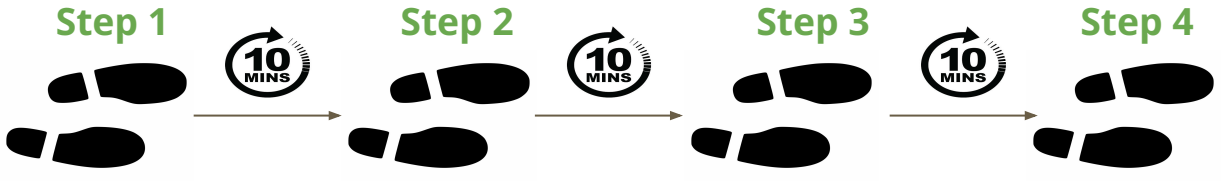
Bonus: What else can we do with steps?

They have an order so timestamping!

1. If each step has a “time” (Bitcoin does), we can prove a document existed at certain time
2. Can prove an event happened after time T i.e. video of Putin telling a block hash that was mined 30 minutes ago can’t be more than 30 minutes old

People will figure out more things.

Blockchain TLDR



Id: 00A3D1
From: Genesis

Id: 008F2C
From: 00A3D1

Id: 006B8B
From: 008F2C

Id: 00F1BA
From: 006B8B

=

Id: 00A3D1
From: Genesis

Id: 008F2C
From: 00A3D1

Id: 006B8B
From: 008F2C

Id: 00F1BA
From: 006B8B

Questions?