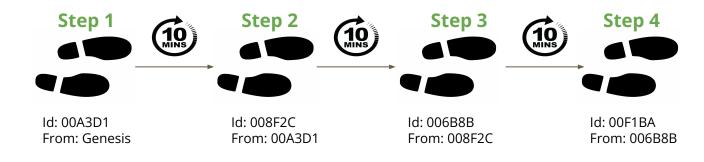
Nakamoto consensus

What, how and why

Blockchain

One-way step function



Rules?



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



Who decides on the step? How do we vote?



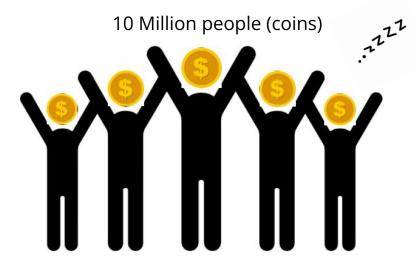
VS

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

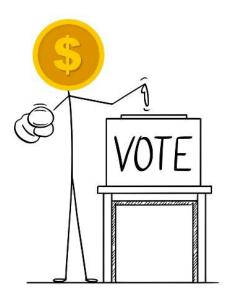


- Can't have real life voting too slow & "too political" i.e. easily manipulated
- ... how do we do it?

Traditional consensus



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:

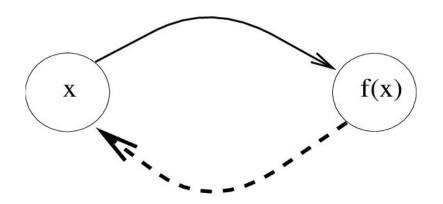


- Public voting 1.
- 2. Closed set of citizens (permissioned)
- Can be stopped (at least theoretically) 3.
- Requires trust in case of forks (weak subjectivity) 4.
- Circularity of voter set definition 5.

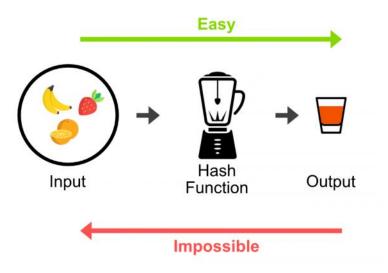


- Can reach a final agreement in good scenario (finality) 1.
- Low CO2 emission (only a few computations) 2.

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 cannee from the largest pool of CPU power. As tongest enamination and years as provided in a sequence of versus writesseed, but provided it and it came from the strengest poor of CPD power. As long as a majority of CPD 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 possest proof-of-work chains as proof of what happened while they were gone.



Free State	Merkle branch linking the transaction to the block it's timestan in. He can't sheck the transaction for himself, but by linking it place in the chain, he can see that a network node has accept			
Te Te	and blocks added after it further confirm the network has acc			
es the problem of determining	E. Longer Post of the Own			
ision making, if the majority were	and here	mus have	Burlinger.	
	- techar tena	· Pachat heat	· Paciet.	-
	Table Run	and has	dama kas	
represented by the longest shain,				
ef-work effert invested in it. If a		(matrix) (matrix)		
ulled by howest nades, the honest outpack any competing chains. To			Nata Stand for 5.0	
r would have to reduithe proof of-		(100) 10		
after it and then catch up with and				
nodes. We will show later that the macker catching up diminishes	the network, but is m			
ichs are added. To compensate far				
sarying interest in running nodes	themselves, the simp			
	fabricated transactions for as long as the attacker can continu			
	everyower the network. One sinalings to protect against this w be to accept alerts from network nodes when they detect an in			
Inoneases.				
	block, prampting the			
e an Sofewa:	alorted transactions receive frequent pay			
nit to all nodes.	nodes for more indep			
actions into a block.				
	9. Combining and Splitting Value			
Fwork, it broadcasts the block to all	Although it would be pencilite to handle coirs individually, it s			
	be unwieldy to mak			
If all transactions in it are valid and	transfer. To allow w			
	centain multiple input			
since of the black by working on	single input from a 1			
tain, using the hash of the accepted	containing ancator an			
	payment, and one rat			
est chain to be the convext one and				
it, if two nodes broadcast different tanenusly, some nodes may receive		• B 04		
use, they work on the first one they		• N []		
anch is case it becomes larger. The ext proof of work is found and one				
des that were working on the other	it should be noted to			
the longer one. New transaction receil to reach all nodes. As long as	several transactions.			
il gat into a block before long, Block	is not a problem here			
it gat with a block before long. Block dropped messages. If a node does	standatone copy of a			
at it when it receives the next block	10. Privacy			
	The traditional bankie			
	access to information			
ion in a block is a special transaction of the creator of the block. This adds				
of the network, and provides a way	fow af information			
circulation, since there is no central	anonymous. The public			
ready addition of a candidet, of	to someone elos, but			
logeus to gold minen expending	anyone. This is similar			
don. In pur case, it is CPU time and	exchanges, where the			
a incentive can also be funded with	is made public, but m			
transaction fee that is added to the		ne · here		
	in here and			
why to transaction free and the				
centive may help encourage nodes	motion Taria			
cker is able to assenble more CPU	As an additional fine			
, he would have to choose between	transaction to keep it			
rating back his payments, or using it				
te to find it more profitable to play	which necessarily reveal that their inputs were owned by the t			
our him with more new coles than				
to undowine the system and the	could reveal other tra			
	11. Calculation			
ace	We consider the sc			
coin is buried under enough blocks, can be discarded to save drA seace.	altamote chain fact			
	accomplished, it do	es not throw the ta	sizer same bi	i.
ng the block's heah, transactions are				
I, with only the rest included in the	never beiunged to D	e affasher, Bodes an	not mine to	10.00
r hadres de not need te be stored.	a block containing th	en. An allacher can o	ely by la chas	-
disk Boot Basic Boot care	his own transactions	to take back money	he recently a	õere
(Auction) Name				
	characteriood as a Bi-	namial Fandom Walk.	The success of	ent i
Red Hart	honed chain being ex			
	and the failure event	is the attacker's chail	being extend	ed by
Reality Reality	block, reducing the	gap by -1. The pri	statily of a	1.40

Setashi Nakamata satashin@emx.com.www.hiteoin.ore

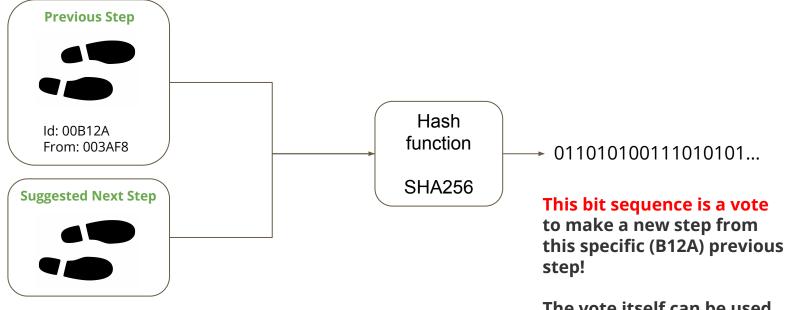
Step = sequence of transactions!

Everyone agrees which transactions happened!



Voting?

PoW vote



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



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.

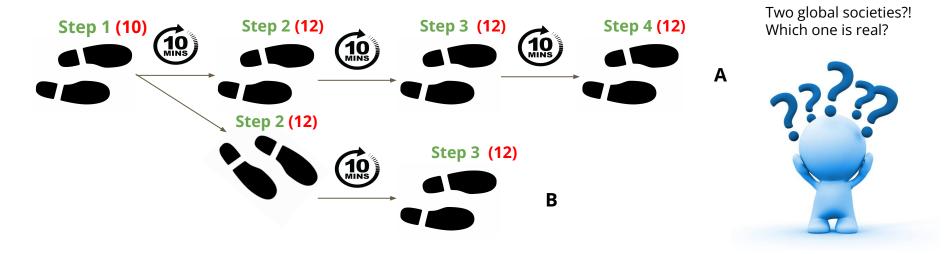
We can now **verify** we collected (roughly) a specific number of votes by showing a single vote!

But wait... what if

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



Convergence to common reality



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.

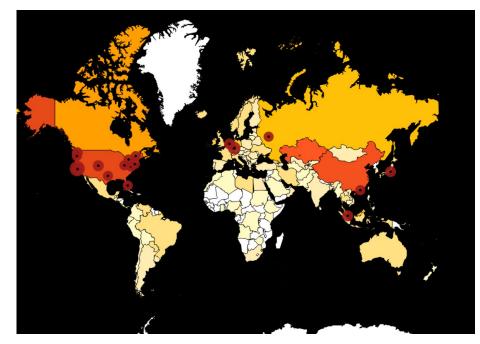
Nakamoto consensus properties

- 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?

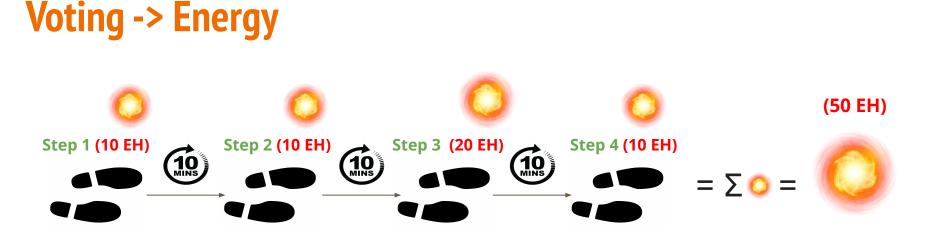


Make a step every 10 minutes



DAA

Slow? Still MUCH faster to move than gold.



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.

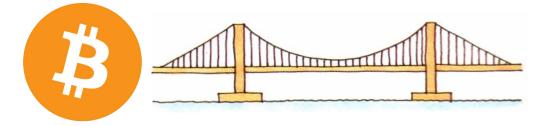
Differences traditional/nakamoto

- "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)**



Real world (physics constraints)



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





Who are we defending from?





Which system we have absolutely no idea how to exploit?



We inherit the security from physics!

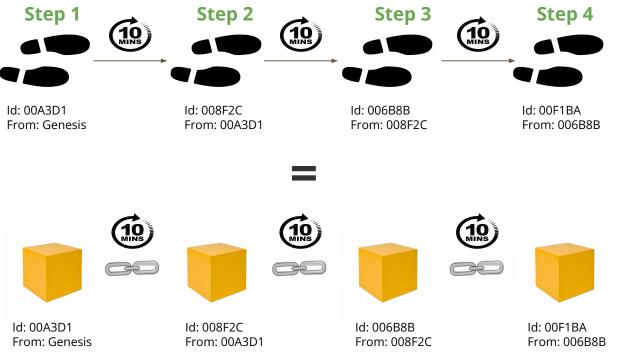
Bonus: What else can we do with steps?

They have an order so timestamping!

- 1. If each step has a "time" (Bitcoin does), we can prove a document existed at certain time
- 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



om: 006B8B

Questions?

