bitcoin's

Sound Money Properties
Series

#3: Distributed & Decentralized

with @SimplestBTCBook and @DJSATOSHI18

- ₿ PORTABLE, DURABLE, DIVISIBLE, FUNGIBLE
- ₿ TRULY SCARCE
- ₿ **DISTRIBUTED & DECENTRALIZED**
- ₿ CENSORSHIP RESISTANT & UNCONFISCATABLE
- ₿ IMMUTABLE & INCORRUPTIBLE
- ₿ EASILY VERIFIABLE & CAN'T BE COUNTERFEITED
- ₿ PERMISSIONLESS, FRICTIONLESS & PEER-TO-PEER
- ₿ NEUTRAL & VOLUNTARY
- ₿ TRANSPARENT, OPEN-SOURCE & AUDITABLE
- ₿ BORDERLESS
- ₿ PROVIDES SETTLEMENT FINALITY
- ₿ PSUEDONYMOUS & TRUSTLESS
- ₿ SECURE & SCALABLE
- ₿ DISINFLATIONARY/DEFLATIONARY

Bitcoin is..
DISTRIBUTED

Definition of Distributed

1 : Dispersed through a space or over an area: spread : scattered

- <u>dictionary.com</u>

Bitcoin is..
DECENTRALIZED

Definition of Decentralized

1 : the dispersion or distribution of functions and powers

2 : the opposite of centralized

- merriam-webster.com

DISTRIBUTED & DECENTRALIZED

₿ Along with true scarcity, enabled by the hard cap supply, decentralization, enabled by distribution, is bitcoin's second most important property.

WHY?

₿ By preventing centralized control of the issuance, the transaction capability and tx verification, bitcoin remains neutral and accessible to anyone anywhere.

₿ No single entity or group of entities can control it or manipulate it, be they individuals, corporations, institutions or governments.

₿ By having the rules of the network maintained and verified by thousands of globally distributed nodes, the rules remain the same for all, and no one gets special favors, ever.

Bitcoin is the
most Distributed computer network
in the world, with over 15,000 visible nodes and
thousands more invisible nodes,
all run by an ad hoc group
of global volunteers
who do not know each other
and
anyone, anywhere can run a node anytime,
without needing permission,
and
that is why
it is the most Decentralized network.

Bitcoin allows

"any two willing parties to transact directly with each other without the need for a trusted third party."

- Satoshi Nakamoto

This is only possible precisely because bitcoin is distributed and decentralized.

₿ When we say bitcoin is distributed and decentralized, we are referring to:

  - bitcoin's issuance (via the miners)
  - the Bitcoin network (the payment rails)
  - bitcoins' transaction validation (via the nodes)
  - bitcoin's transaction verification (via the miners)

₿ Fiat, on the other hand, is not distributed, nor is it decentralized:

  - Fiat issuance is 100% centralized and can be manipulated
  - Fiat payment rails are walled gardens controlled by very few
  - Fiat payment validations/verifications are concentrated and controlled by central authorities.

Fiat is top down: Rulers, who manipulate the rules

Bitcoin is bottom up: Rules, not rulers

Distribution of Reachable Bitcoin Nodes - January 10, 2023

REACHABLE BITCOIN NODES
Updated: Tue Jan 10 11:12:18 2023 PST

15144 NODES

CHARTS

IPv4: -2.5% / IPv6: -0.4% / .onion: +6.4%

Top 10 countries with their respective number of reachable nodes are as follows.

RANK	COUNTRY	NODES
1	n/a	8687 (57.36%)
2	United States	1728 (11.41%)
3	Germany	1347 (8.89%)
4	France	427 (2.82%)
5	Netherlands	371 (2.45%)
6	Canada	289 (1.91%)
7	Finland	230 (1.52%)
8	United Kingdom	211 (1.39%)
9	Russian Federation	180 (1.19%)
10	Switzerland	127 (0.84%)

All (92) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

bitnodes.io

₿ In order to keep bitcoin decentralized, it is critical to keep it distributed.

₿ Maintaining the small block size of 1MB is one of the most important ways we can do so, as this keeps it more accessible for regular people to run their own node/copy of the Bitcoin timechain.

₿ The current size of the whole timechain is just over 500GB, so in order to run an archival full node you will want to get a 1TB external hard drive.

₿ You can also run a pruned node on any computer that has just 6GB of space. This is still considered a full node, as it verifies every single block as it downloads, but then it prunes most of the info to reduce the timechain size, making it easy for anyone to run.

6 Reasons to Run a Node
Adapted from an article by Arman the Parman
@parman_the

PRIVACY

• When you run a node and it is connected to your wallet, you query your own node when checking your balance, instead of some random node that could be run by anyone, including a chain-analysis company, a government etc.

CONFIRM VALIDITY OF A TX

• With your own node, you can confirm that you are 100% receiving real bitcoin, and that no hacker has performed an attack by connecting your wallet to a malicious node and thereby tricked your wallet into accepting counterfeit bitcoin.
• While highly unlikely at this time, we need to remember that hackers are and will become more prevalent, and we need to do all we can so secure our stack.

DEFEND THE BITCOIN NETWORK

• By running your own node, you can help defend the network from attack by refusing an upgrade that changes the rules in a way that is dangerous for the security and sustainability of the network.
• The block size wars is an example where, if you were not running your own node, you could not defend the network from a block size increase.

NETWORK SPEED

- The more nodes that are running, the faster transactions can propagate throughout the network and the harder it is to kill bitcoin.

NETWORK SECURITY

- In order to do stop bitcoin, every single copy of the blockchain would need to be destroyed, so the more there are, the harder it becomes to do this.

BECOME AN 'UNCLE JIM'

- While the ideal would be for everyone to run their own node, it might remain 'too technical' for some people, especially elders.
- If you run anode and are familiar with how it works, you can become an 'Uncle Jim' for your family or local community.
- While this does introduce some trust into the system, it is far safer for the people who know you to trust your node, than some other random node 'out there', especially as the network grows.

Thanks for listening!

Feel free to offer feedback, corrections or additional important points, and I will update this presentation.

Next week we will discuss the properties of:

Censorship Resistance and Unconfiscatability