Twitter Thread by Alan Liang



Alan Liang
@alanhliang



1/ Critics denounce Bitcoin as technology that just isn't that useful. In many respects, they're right. The network doesn't scale. Privacy is fragile. Prices are volatile. Custody is hard.

2/ If we take a step back, however, it might be easier to understand why Bitcoin is such an incredible achievement.

3/ Bitcoin is many things.

It's a network in which anyone with an Internet connection can participate. A network no single entity controls.

4/ It's an economic system. A system in which anyone can opt and transact. A system in which trust is minimized.

5/ It's money. Money that you don't need permission to own or use. Money whose rules are set in stone, not dictated by any government. An Austrian-economic experiment at grand scale.

6/ It's code. Code is hard to censor as it's similar to speech. Now money is hard to censor.

7/ It's the culmination of a series of technological innovations in cryptography and distributed systems.

8/ An append-only log that utilizes cryptographic hash-chaining to make the log tamper-evident. A blockchain.

9/ Proof of work to secure the economic history of the blockchain. A largely meritocratic process for choosing who decides what additions are made to the blockchain.

10/ Nakamoto consensus as a set of rules that help network participants agree on what changes are valid and and how to reconcile conflicts arising from latency or malicious actors

11/ Cultural norms of the Internet are weaved into the fabric of Bitcoin's culture.

12/ Open source code which ensures participants can't be compelled to use a network they don't want to. When you can fork, you can leave.

13/ Open source ethos, from which emerges a loyal mass of ideologically-aligned participants who contribute to the network's security and development.

14/ Cypherpunks, which encourage thinking of nation-states as reducible in scale and scope and the Internet as a champion for freedom.

15/ Permissionless. Everyone has a place in the system.

16/ There's a lot under the hood that makes Bitcoin work, which is why the "Blockchain, not Bitcoin" movement is laughable. The fundamental breakthrough of bitcoin is not the blockchain.

17/ Bitcoin is a fundamental breakthrough in human consensus.

18/ In society, we have institutions such as governments, laws, banks, and social norms. These help society coordinate action at scale. To reach consensus.

19/ Millions of people, spread across the face of the planet. Who've never met each other, who don't trust each other, and who don't speak the same language can come to agreement on one thing. On average every ten minutes. All they need is a computer and an internet connection.

20/ The first application of this consensus is on the state of a digital ledger. Bitcoin.

21/ Consensus is what allowed humans to evolve from their hunter-gatherer days to become the dominant species.

It's exciting to think what other novel, emergent ways of human consensus enabled by the Internet might arise, and how they might be useful for society.

h/t: @aantonop @naval @nic__carter @EdFelten @NickSzabo4 @MustStopMurad @derek_hsue @LaurentMT

Post-script: @nic__carter published a great piece today on the subject. Get your Vitamin C folks, lest you get lost in the semantic wasteland:
https://t.co/VRhF1gxG2e