Twitter Thread by Dan Held



Dan Held
@danheld

1/ Satoshi’s Vision™ is a silly endeavor, as it doesn’t matter what it was, we are where we are now. However, those pushing the “Bitcoin was first made for payments” narrative insist on cherry-picking sentences from the white paper and forum posts to champion their perspective.

2/ The following tweetstorm is a categorical repudiation of this tired narrative. Bitcoin was purpose-built to first be a Store of Value (SoV), a thread:

3/ How do we determine Satoshi’s intention? We need to look at his ideology, description of functionality/architecture, timing, and audience. Let's start with how Satoshi describes the problem Bitcoin solves. In his first public comms after the whitepaper, in the first paragraph:

4/ “The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.” - Satoshi

5/ He later expands on that Libertarian thought in his other writings:

“[with Bitcoin] we can win a major battle in the arms race and gain a new territory of freedom for several years.” — Satoshi Nakamoto

6/ How does Satoshi describe Bitcoin? His forum posts provide insight through his consistent gold/metal analogy:

“Bitcoin [is] more like a collectible or commodity.” - Satoshi

7/ "In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases” - Satoshi

8/ “As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties: [not useful/no utility]. And one special, magical property: can be transported over a communications channel” - Satoshi

9/ “If there were nothing in the world with intrinsic value that could be used as money, only scarce but no intrinsic value, I think people would still take up something. (I'm using the word scarce here to only mean limited potential supply)” - Satoshi

10/ “It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy.” - Satoshi

Satoshi here clearly highlights that Bitcoin’s scarcity gives it value… as a SoV. Limited supply is meaningless for VISA

11/ So we now have an idea of Satoshi’s motivations, and how he describes Bitcoin, but what does his timing tell us?

Bitcoin’s launch during the 08' financial crisis was not coincidental. Satoshi had been coding Bitcoin for the last 2 years. Let’s look at the sequence of events

12/ Jan - July: Fed tries to stop the housing bust: Fed bails out Bear Sterns. Paulson explains the need to bail out Fannie Mae, Freddie Mac the two agencies that held or guarantee 50% of the $12T in US mortgages.

13/ Aug 18: Satoshi registers https://t.co/rMWwiEwtxT

Sept 15: Lehman Brothers files for bankruptcy, the largest in U.S. history ($600B)

Sept 17: Investors withdrew a record $144B from their money market accounts. During a typical week, only about $7B is withdrawn

14/ Oct 3: Bitcoin whitepaper PDF likely created

Oct 13: Treasury Secretary Paulson talks with 9 major bank CEOs. The total bailout package ~$2.25T

Oct 21: Fed lends $540B to bail out money market funds

Oct 31: Satoshi publishes the Bitcoin whitepaper

https://t.co/Bf8X1VI7Qo

15/ With the 2008 financial crisis, trust had been lost in a world that ran on trust. Bitcoin was launched in a time of absolute necessity, Satoshi planted the seed at precisely the right moment. The world didn't need a new VISA, they needed an alternative to banks.

16/ So we now have an idea of Satoshi’s motivations, how he describes Bitcoin, and his timing, what about this initial audience for the whitepaper? How did he market his message?

17/ Satoshi crafted the whitepaper as a call to arms for his target audience: the Cypherpunks on the cryptography mailing list. Key components of their ideology are privacy and finality. His message needed to resonate with them as they would have to help him build it.

18/ “Therefore, privacy in an open society requires anonymous transaction systems. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.” - A Cypherpunk's Manifesto

19/ Many point to this in the whitepaper “peer-to-peer version of electronic cash would allow online payments” as proof that Satoshi meant for Bitcoin’s main purpose is to disrupt VISA. However, "cash" represents a pseudonymous push payment in contrast to a credit-based system

20/ Cash is a bearer asset. Let’s look at the whitepaper with that in mind:

“A purely peer-to-peer version of electronic [bearer assets] that would allow online payments to be sent directly from one party to another without going through a financial institution."

21/ Note that the origin of the word “cash” is “caisse” (French) meaning money-box. So cash is by definition store-of-value. Other Cypherpunks had used the word cash in their whitepapers to reflect that functionality, like “HashCASH”, “eCASH”, etc”

22/ In the other part of the whitepaper sentence the phrase “peer-to-peer” has been used as well against the SoV narrative. Charlie Lee has a great tweet storm that addresses this point of contention:

23/ “Bitcoin isn’t “peer-to-peer.” Payments are sent from sender to miners, who record it on a distributed ledger. The recipient receives the payment when it's recorded. BUT, this is facilitated by a p2p network where transactions are broadcasted.” - @SatoshiLite

24/ “Lightning network payments, on the other hand, are p2p payments. They are sometimes direct p2p, sometimes indirect p2p. LN payments have to be sent from p2p to get from the sender to the recipient. Both have to be online, just like other p2p networks like BitTorrent”

25/ “Bitcoin with Lightning Network more closely fits the Bitcoin whitepaper's title: "A Peer-to-Peer Electronic Cash System." This is Satoshi's Vision.” - @SatoshiLite

26/ He wrote the paper to fit his target audience, but the source code implementation were his product specs. “If the Bitcoin Whitepaper is the Declaration of Independence, the Source Code is the Constitution” - @pierre_rochard

27/ “The functional details are not covered in the paper, but the sourcecode is coming soon.” — Satoshi Nakamoto

Aka the whitepaper was marketing, the important details are coming.

28/ In true Cypherpunk fashion, Satoshi’s whitepaper was quickly followed by code release in January 2009. The notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list.

29/ Just focusing on the whitepaper is a gross misinterpretation, here are the things not described in the whitepaper, but included in the source code or later defined by Satoshi: 21M hard cap, 10 minute blocks, 1 mb block caps.

30/ If Satoshi wanted Bitcoin to first be used as a medium of exchange to purchase goods and services, he would have made it inflationary. People don't spend deflationary currencies when they can make the same purchase in infl. curr. There's even a name for It, Gresham’s Law

31/ Which is entirely intuitive. Why would any average consumer spend their Bitcoin with the perception that it will be worth more in the future when they can spend their fiat that they KNOW will be worth less?

32/ So far that doesn’t sound like he's trying to disrupt VISA now does it? And if that wasn't made perfectly clear, he permanently etched this message into the Genesis Block:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

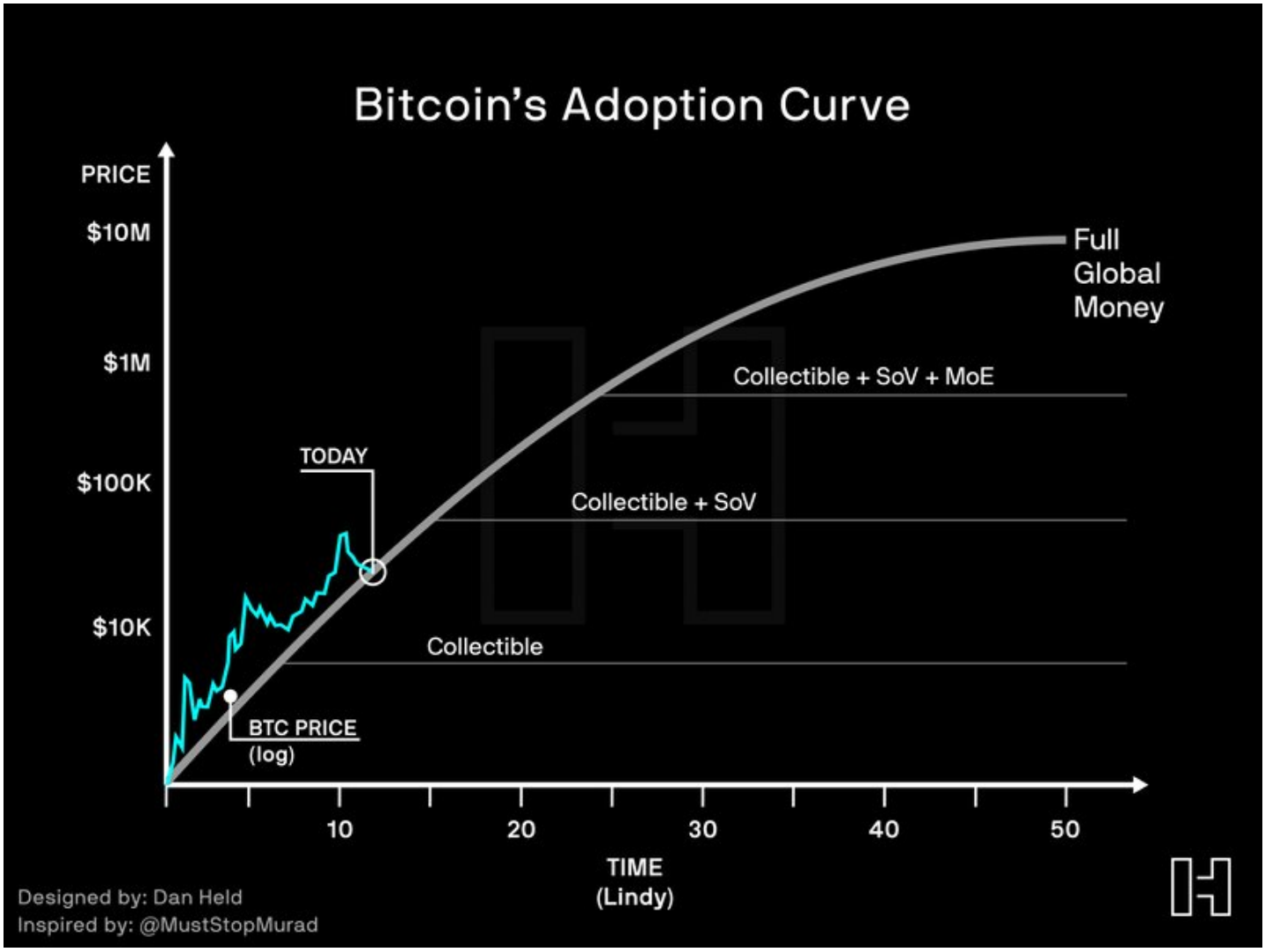
33/ To take it a step further, as a subtle jab to central banks, he chose his birthday as the date the US made gold ownership illegal through EO 6102 April 5th. He chose 1975 as his year of birth which is the year when the US citizens were allowed to own gold again

34/ And finally, why did Satoshi choose to be anonymous if he were just disrupting payments?

What he was trying to accomplish was clear, he wanted to build a new backbone for the financial system. Bitcoin isn't merely digital cash, but an alternative to banks.

35/ And how does a new money get created? A new money comes into existence through stages: Collectible, SoV, MoE, and UoA.

SoV and MoE aren’t mutually exclusive. It’s about where in the cycle of appreciation we’re in. At maturity, the payment use case finally makes sense.

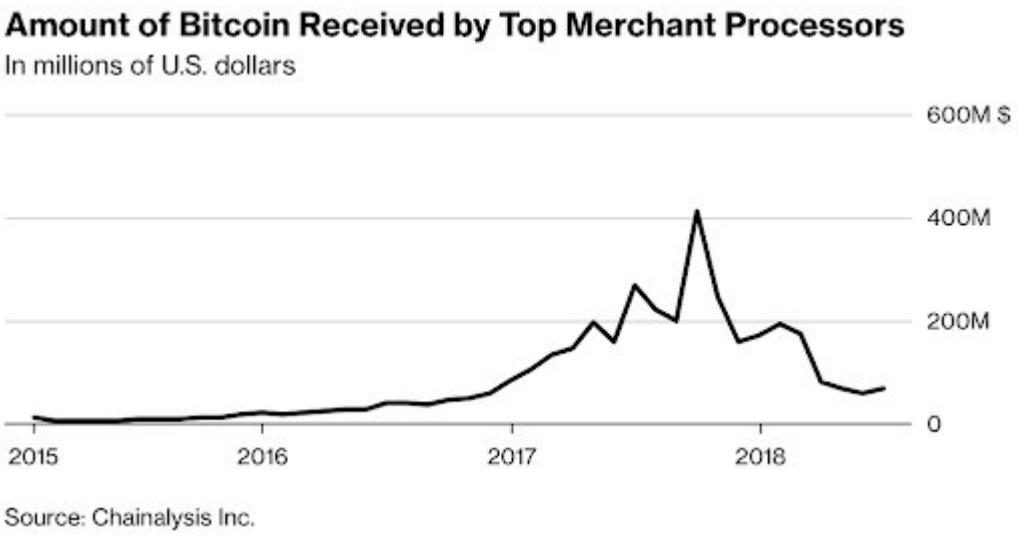


36/ Some may balk at the SoV terminology for Bitcoin since the price fluctuates. However, nothing in this life has a "stable" value, the longest running fiat currency, GBP, has lost 99% of its value since inception. Bitcoin has all the traits of a good SoV
https://t.co/C6kpf8cjKX

37/ Bitcoin is stable. The protocol has a 99.99989% uptime which is higher than USD. The "fluctuation" you see is the volatility of the world flowing into the stability of Bitcoin in ebbs and flows.

39/ This phase, which is characterized by its primordial exploration of the SoV properties of the commodity, can easily take a decades to properly mature. Volatility is part of this maturing process.

40/ People pushing the MoE narrative at this moment in time are counterproductive to adoption. By creating these expectations, which are unattainable at the moment, many people will get burned or disillusioned. This is a big loss for adoption and for the affected individuals



41/ “Only by informing people correctly about the use case Bitcoin has *at this moment* can we maximize it's adoption and prevent a lot of people from making the biggest financial mistake of their life.” - @Willem_VdBergh

42/ So how did the payments narrative become a thing?

A/ Satoshi used it to attract the cypherpunks
B/ HODLing isn’t good for business. In order to command higher valuations, startups latched onto narratives that VCs would fund. And in 2013-2016 that was “merchant processing.”

43/ Background on me: I was the first PM @Blockchain
and @ChangeTip, both attempted to get people to use Bitcoin for payments. Consumers couldn't care less, which is entirely intuitive: right now it’s not faster, cheaper, or easier to use for 99.99% of use cases.

44/ After all of this do you really think Bitcoin was primarily built for payments at this stage in its lifecycle?

45/ If you enjoyed this tweet storm, please sign up for an e-mail newsletter which will include more of my thoughts like these ■

https://t.co/TYJDEruzvc