

## Twitter Thread by [Kirtan A Shah](#)



**Kirtan A Shah**

[@KirtanShahCFP](#)



■ ■■■■■■■■ ■■ ■■■■■■■■■■■■ & ■■■■■■■■ ■■

**I still everyday meet investors who think Bitcoin & Blockchain are the same & this thread is specifically for them**

**Do re-tweet & help us educate more investors ■**

### **#Investing #Cryptos #Bitcoin (1/n)**

(Q1) Lets start with what was historically used as a method of payment?

- Barter system, you give me a cow and I give you 100 kgs of rice (2/n)

(Q2) So why dint we continue with the barter system?

- It was difficult to transact in fractions
- What if I want only 50 kgs of rice? I cant give you half a cow right?
- This is the prime reason for the introduction of smaller units of payment method we now call as coins (3/n)

(Q3) How did Gold coins get shortlisted for the job?

- It was malleable & portable
- It was non corrosive, could be stored for a long time
- It was a perfect combination of abundance & rare
- Plus it was eye catching & visually appealing (4/n)

(Q4) What about paper currencies?

a) When paper currencies were introduced, it was decided that a country could only print as much currency as the gold reserves they have but this was withdrawn in 1971 bcoz of which the central banks could then print as much money as they wanted

- (b) Infusing so much liquidity leads to 'higher inflation' & it is completely 'controlled by the central banks' (This is the problem, remember this through out the thread)
- (c) To solve the above problem, Bitcoin was invented. (6/n)

(Q5) What is a Bitcoin?

- (a) It claims to be a Store of value (like Gold is) & a payment method (Like \$ is) (7/n)
- (b) Because only a limited supply of Bitcoin is available, it is expected to be deflationary (problem 1 addressed) as per modern economics & because it uses blockchain, it is more transparent & no 1 single entity controls it (Problem 2 addressed). (8/n)

(Q6) Before we understand Bitcoin, lets understand Blockchain

- (a) Assume split wise. Friends go out, sometimes someone pays and sometime someone else. At the end of the year, there is a ledger mentioning how much does who owes whom. (9/n)
- (b) The challenge with this ledger is what if I add any entry in it during the year, who verifies if it's correct?
- (c) Currently, banks do this verification when you transact through the bank. Banks maintain transaction record of credits & debits (10/n)
- (d) NSE/BSE /NSDL/CDSL does the same thing in the stock markets
- (e) But what can you do to decentralize? No banks, no NSE/BSE/CDSL/NSDL? To verify the transactions, you use computational work (replacing intermediaries (Banks) with computational work), let me explain (11/n)

(Q7) How does the blockchain work?

- (a) There are multiple computers also called as miners or NODEs are connected to each other on open source software (12/n)
- (b) For bitcoin, you can download the software Bitcoin client, have the hardware in place and you become the part of the mining community who would verify & maintain all transaction records (13/n)

LATEST TRANSACTIONS			
Sender	Receiver	Amount	
1Xsk89KSI3kE	→ Ijs72Hgs8i6	3 ETH	✓
28ShkwUY22jK	→ 2jHsk8Gshn76	92 ETH	✓
kkK2so2992mS	→ IKjs87SvX78H	40 ETH	✓
pOss02fT2Nbd	→ Ns875fSSg527	20 ETH	✓
kJs772oMbY92	→ mFd4jkGsbny6	12 ETH	✓
mkJ742Ghsb6g	→ 97JbsSgs7dhY	0.8 ETH	✓

- (c) Lets say someone buys & sells the bitcoin and that transaction needs to be verified. What happens is, multiple transactions (maximum of 2400) are bundled into a block (14/n)
- (d) 2 authorize if the transactions r correct, u have 2 sign it with a unique valid transaction key (HASH or Proof of work), which is generated after solving some very complicated algorithmic problems 2 arrive at the HASH which other computers in the network also validate (15/n)

Hash function

SHA256(“3Blue1Brown”)


Message/file

=

11001010111100010010111000011011  
11000101101010010110001011011110  
11000001110100000110010100111001  
11111110111100000001111100110110  
00110110000011100000101011110010  
00101001100000000011101110011110  
10010001010000011100001001001100  
10001011111011010101010001110000

“Hash” or “Digest”

- (e) Whichever computer in the open network is able 2 solve it 1st, announces it in the network 2 every1 where every1 saves the transaction in their ledger automatically as a part of the network (decentralized) 4 which the miner who solved the problem receives bitcoin as a reward
- (f) Like in the ledger, these blocks keep forming a chain one after the other and hence it’s called the Blockchain (17/n)
- (Q8) How many Bitcoin’s do I get for the mining activity?
- (a) It is called Bitcoin Halving
- (b) It reduces the bitcoin reward for the miners by half every time 2,10,000 blocks are verified (18/n)
- (c) A new block is created every 10 min, it roughly takes 4 years 4 the bitcoin halving (its an automated process of reducing the reward at every 2,10,000 blocks verified)
- (d) This is the bitcoin reward 4 solving the block & no new bitcoins after 2,10,00,000 bitcoin are released



Block rewards

Jan 2009 - Nov 2012: 50 BTC

Nov 2012 - Jul 2016: 25 BTC

Jul 2016 - Feb 2020\*: 12.5 BTC

Feb 2020\* - Sep 2023\*: 6.25 BTC

- (Q9) What are Altcoins, Stable coins & Meme Coins?

(a) Altcoins - Anything other than a Bitcoin is called the Altcoin. Example – Ethereum, Cardano, Polkadot (20/n)

(b) Token or Stable coin - It is pegged against \$ majorly & tries to mirror its movement. Price of the coin moves up & down with the movement in \$. Example – Tether, USDC

(c) Meme-Coins - Made for fun, have no logic. Example – Doge, Shiba (21/n)

(Q10) What are my views on the same?

(a) Blockchain is a brilliant technology & has multiple use cases in various industries

(b) But on Bitcoin, I am not sure if it will be able to replace paper currencies as a medium of transaction or gold as a store of value. (22/n)

(c) It 'may' evolve into use cases in the future that I cant visualise right now.

(d) Altcoins with use cases like De-fi will evolve over time & we will talk about it in the next thread. Will also talk about the fancy around NFT's & Metaverse going forward (23/24)

This is my 49th thread, 'do re-tweet' & follow me

[@KirtanShahCFP](#)

Have earlier written on,

-Sector Analysis

-Macro

-Debt Markets

-Equity

-Gold

-Personal Finance etc. You can find them all in the link below <https://t.co/UrRt87xIJF>..... (END)

Here's a compilation of Personal Finance threads I have written so far. Thank you for motivating me to do it.

Hit the 're-tweet' and help us educate more investors

— Kirtan A Shah (@KirtanShahCFP) [December 13, 2020](#)