Some thoughts on cryptocurrencies from my Quora answers :

### My answer to “Will Bitcoin reach 50k USD?”.

This was answered here : <https://qr.ae/pNQXvY> before it actually did.

With all the countries switching on their note printers post pandemic, a lot of people would like to invest into something that doesn’t lose value by government overprinting money. So I guess Bitcoin will continue going up. {You can think of bitcoin as a hedge against bad monetary policy of a country and some competition for the government to make investing in their country lucrative for retail investor}

I hope it keeps going up and I make money for a new laptop hopefully ;)

### My answer to, “Which one is a better investment choice among Bitcoin, Ethereum, and Ripple in 2021?”

Originally answered here : <https://qr.ae/pNQXva>

Diversify. Don't put your eggs in one basket. Don't invest just in cryptocurrencies, in cryptocurrencies, don't just invest in btc or eth.





I personally think ethereum holds more promise as it being a blockchain ecosystem, can support much more than just a currency. ETH2 with proof of stake rather than proof of work, might be what makes cryptocurrencies useful for microtransactions finally.

Ripple is trash in my personal opinion.

Any crypto bet is very speculative, so only invest what you will not get destroyed on losing fully. Regulations , specially in a time when governments are switching on their note printers, can shock crypto valuations.

### My answer to “Which one is the best cryptocurrency next to bitcoin?”

Originally answered here : <https://qr.ae/pNQXnK>

Cryptocurrency wise Ethereum looks good to me as well.

[Ethereum Posts 450% Gain in 2020, Beats Bitcoin | Finance Magnates](https://www.financemagnates.com/cryptocurrency/news/ethereum-posts-450-gain-in-2020-beats-bitcoin/)



Another crypto I have seen making good returns is Cardano.

[Cardano gains 20% amid a high buying spree | Nairametrics](https://nairametrics.com/2021/02/07/cardano-gains-20-amid-a-high-buying-spree/)



### My answer to “Is it best to buy altcoins with BTC, INR, or dollar?”

originally answered here : <https://qr.ae/pNj85c>

I don’t think it matters a lot.

You could however use Bitcoin’s faster rising value as compared to many other coins as a trick to buy more coins by putting your dollars/rupees into Bitcoin for a few weeks and then later buying altcoins by Bitcoin than you would have in case you bought them directly. But this is speculative and might not work.

### My answer to “Is Dogecoin worth buying in 2021?”

Originally answered here : https://qr.ae/pNEyy9

I have some DOGEcoin which I bought during the #HoldDOGE thing. It rose very fast then {and was the best return you could imagine for a few days} but has been falling since then. Since then, Hold the DOGE movement is kind of dead. I am still holding it though, maybe it rises later, maybe will buy some more when its cheap. :-D

More seriously, unlike bitcoin which is a limited resource somewhat like Gold, DOGEcoin is more like our day to day currency without a central bank. Its a very different type of currency from btc and would serve a very different usecase if it ever becomes mainstream.

### My answer to “Should I invest money in Ethereum ($ETH) in February 2021?”

Originally answered here : https://qr.ae/pN6MjO

As of now, Ethereum is on a boom we have never seen. People have made as much as 40% returns in last 2–3 weeks. So yeah, I guess its not a very bad advice to invest in Ethereum right now. I see it as with more currency getting printed all across the world to push COVID stagnated economies, governments around the world have now scaled their money printers to a limit we have never seen. Its an unknown scenario for everyone {never has happened before}, so people aren’t sure how it all will turn out. They are just using cryptos like ETH and BTC as an alternative. If someday with some probability, regular currencies become valued at the paper they are printed on, they should have some money that is free from money printers.

That said, just like any other investment, there is a fear of correction. If the money printing spike doesn’t trigger a hyperinflation {there are some theories about why it has not yet triggered one} , cryptocurrencies might lose some speculative value or better the returns would get worse. So invest only what you can afford to lose, don’t get too greedy.

### My answer to “Does Elon Musk own Dogecoin?”

Originally answered here : https://qr.ae/pNcquh

That is like asking “Does Mukesh Ambani own Rupee ?”

Rupee is a currency and is owned by no one. Mukesh Ambani has rupees and Elon Musk may have Dogecoin, but no one owns anything. You can maybe say that Indian government owns rupee {and US government owns the US$}, but even that is not true for cryptocurrencies like Bitcoin and Dogecoin. In fact the entire point of bitcoin’s invention was to make sure no one is a central authority in the currency {and from what I know, dogecoin is a copy of bitcoin in that regard} .

### My answer to “What are your thoughts on Bitcoin crashing 10k USD on the 23rd of February 2021?”

Originally answered here : https://qr.ae/pNQXnX

Any commodity has fluctuations in its price. Bitcoin fell on 23rd Feb, is rising back again (24th Feb). No big deal.

Unless there is a big shocker event hampering bitcoin or people’s interest slowly dies off, these noises in price will stay and Bitcoin will continue to rise to get its eventual stable value. [Muktabh Mayank's answer to Who would be responsible if the Bitcoin price just crashed to pennies?](https://www.quora.com/Who-would-be-responsible-if-the-Bitcoin-price-just-crashed-to-pennies/answer/Muktabh-Mayank?ch=10&share=42fc97ea&srid=qie)

### My answer to “What technology is used to record cryptocurrency transactions?”

Originally answered here : https://qr.ae/pNMaeT

Let’s understand in very basic terms what a cryptocurrency is :

1. Whether one paid to another person or not is verified using the concepts of public and private keys. This is the same public key cryptography that we use to login into our Google or Quora account. Every transaction is signed using private key of the payer and can be verified by their public key. Its somewhat like you signing into your email account and sending an email to whole world that you are transferring X $ to ABC. The proof of this email was sent by you to make the transaction is stored till eternity.
2. However, just verifying a transaction is not enough to make a currency functional, the currency should also take care that the sequence of the transactions is mapped correctly too and can be verified quickly. It you are reading about these for the first time, you can basically think that the entire process of cryptocurrencies depend upon maintaining this order. One way to quickly intuit this is to think while a signed transaction of 10 cryptos from user 1 to user 2 is signed, if order is not maintained, the same signed transaction can be inserted again and again into the ledger to create fraud and extract out money from user 1. The data structure used to verify order is [Merkle tree - Wikipedia](https://en.wikipedia.org/wiki/Merkle_tree)
3. . This makes sure that the order of all the previous transactions and the new transaction is mapped so that every transaction has a place in the history. As you can imagine current transaction cons’ed to all previous transaction would make a “chain” if done after every transaction. Instead of ordering each transaction , a group of transactions (block) is sequenced with respect to all previous ones to reduce computations. This Merkle Tree data structure is called a “Blockchain”.
4. Now the third most important point is who gets to verify the order. Everyone can verify individual transactions using Public Key, but who gets to verify what is the right order in which these transactions were committed. The answer is “any miner on the network randomly”. Bitcoin Miners basically play roulette with each other trying to come up with some number combinations of Hash Values by adding random string to the latest block. If they win the roulette, they get a few cryptocurrency units and as long as these random miners keep competing to verify the transaction , a mathematical guarantee exists that the transaction data order is being verified correctly. If one of the miners tries to copy a few transaction in middle to make double payments to benefit them or friend, they will have to invent a mathematical system that helps them win the roulette of Cryptology Hash Functions again and again, which is impossible mathematically ! So someone who inserts a fraudulent duplicate transaction might be correct for one shot, but then the system will self correct when the next block is verified and the fraud will self remove.

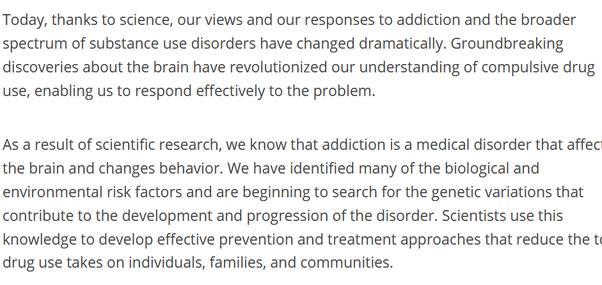
To answer your question specifically, the data is stored in a Merkle Block Chain Tree which is available to every miner on crypto network and anyone who wants to read and see it.

### My answer to “What would be the alternative currencies for a better world towards eradication of poverty? By currencies, I mean just a way of exchanging stuff not necessarily money.”

Originally answered here : https://qr.ae/pNJvbZ

We cannot eliminate poverty, whatever we do. Any currency cannot solve the problem fully. At best, we can make sure that no one is poor because they are born unlucky, that is poor because they are sick or poor because they were born to poor or abusive parents. While majority of poor people are such unlucky men,women and children, there are many who are poor due to making bad decisions. People who are bad spenders {alcoholics, gamblers, drug addicts} seem to have a mental disorder {specifically lack of willpower to say No.} , which like most mental diseases, can be managed, but not cured. You can expect many such people to be poor perennially.

[Preface | National Institute on Drug Abuse](https://www.drugabuse.gov/publications/drugs-brains-behavior-science-addiction/preface)



What we can rather do is have a security network that people can bank on to survive during times of poverty and they have a chance to fight their way out. There are concepts like Universal Basic Income and digital wallets which can get money directly into the hands of the needy in case they need. India, for example, has UPI [Unified Payments Interface - Wikipedia](https://en.wikipedia.org/wiki/Unified_Payments_Interface)

and Zero Balance Accounts (banks are mandated to have no minimum balance requirement for poor people) which has made getting money in the hand of the needy really easy. That is the reason you did not see a full scale rebellion in India during the super long lockdown here : India introduced a temporary UBI during the pandemic times.

[Google cites UPI learnings to US Federal Reserve for proposed RTGS system](https://www.thehindubusinessline.com/info-tech/google-cites-upi-learnings-to-us-federal-reserve-for-proposed-rtgs-system/article30305827.ece)



So FinTech with even traditional currencies has reduced the dependence of government on large institutions to aid the poor. If such a thing like UPI + Zero Balance Account were not available in India, Indian government would have to depend upon many layers of public sector hierarchy or private institutions to help the poor. The more hands involved, more corruption and lesser the welfare reaches poor.

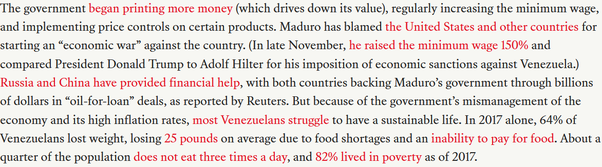
India had to come up with these because upto 85% of the welfare money it was spending earlier was being lost in corruption and inefficiency. So much leakage ! [Rajiv was right: Montek says only 16p of Re reaches poor | India News - Times of India](https://timesofindia.indiatimes.com/india/Rajiv-was-right-Montek-says-only-16p-of-Re-reaches-poor/articleshow/5121893.cms)

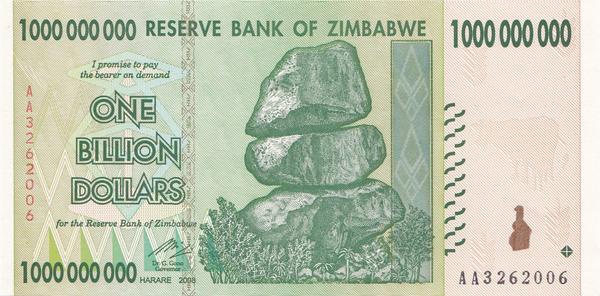


At least in the sense of reducing poverty, the problem is not so much in government welfare numbers <that can be debated well before they are finalized> or the traditional currency system, but rather the bloated bureaucracy and corruption of nation states. The way to solve this is to use more efficient methods like digital wallets or zero balance account. A government which is responsible and committed to its poor needs the traditional currency system to control monetary policy, at least in the time of economic despair to avoid too much poverty.

However, there are even worse case scenarios possible, where because the governance is so bad, the financial system of a country breaks down and they need to print more and more money to distribute amongst people who help them run their regime. Say Venezuela or Zimbabwe like scenario.

[Venezuelans Are Starving as the Nation's Economic Crisis Continues](https://www.teenvogue.com/story/the-economic-crisis-in-venezuela-explained)





In such scenarios, leave alone making poor people better, the governments are making well to do people poor ! This is the type of scenario where alternative new currencies like bitcoin can kick in. By investing their wealth into cryptocurrencies, people can make sure that government’s poor monetary policies don’t ruin them altogether. In fact, cruptocurrencies make sure that no monetary policies are applicable to them, so your existing wealth is never getting devalued.

### My answer to “If India bans all private cryptocurrencies and introduces a single official digital currency issued by the RBI, how will it affect the economy of India?”

Originally answered here : https://qr.ae/pNzj8e

There is some misplaced sense of bureaucratic logic that is driving this initiative. RBI tried to ban other cryptocurrencies while launching its own crypto and when that was struck down this has been sent to the parliament. I hope our government and members of parliament understand that CBDCs [Central Bank Digital Cryptocurrencies] and decentralized cryptocurrencies have two very different applications and banning the later is not required to get a market for the former. The competitors for CBDCs are international centralized coins like Libra {Now called [The Diem Association](https://www.diem.com/en-us/)

}, other upcoming CBDCs like China’s and EU’s and not Bitcoin/Ethereum and its brothers. We are fighting the wrong monster here.

**CBDCs usecases :**

The top benefits of a CBDC are :

1. Quicker disbursement of government financial aid/UBI. While right now RBI prints currencies, sends to government/banks and banks then disburse the money, A CBDC can be minted and disbursed almost immediately after decision is made. A few years back, when this disbursal was done through cash, there was a lot of corruption and even more delay which fintech has already solved, now CBDC when combined with fintech would make the process instantaneous .
2. Tracking flow of money is another cool thing about CBDCs. While for most citizens the CBDC ledger is anonymous, the government accounts will be public and people can see where there tax money have been spent down to one rupee. This ensures certain types of corrupt practices will be much easier to detect and highlight. In a way good step to check public sector corruption.
3. Indians are already accustomed to digital currency [You have amazon wallet cash, paytm wallet cash] and so on. While right now, this cash is guaranteed by the companies, CBDC as a digital cash will be guaranteed by the government. These are two very different type of guarantees. Sudden nationalization of AliPay for example makes a lot of AliPay guaranteed digital money of SouthEast Asian and African businesses using AliPay, Chinese government guaranteed money. Not sure how comfortable people would be wit that, but private companies are under umbrella of the countries they have their effective center of control in.

**This is in total contrast with how decentralized cryptocurrencies [like Bitcoin] are being used in today’s day and age:**

A. Decentralized Cryptocurrencies are emerging as a hedge against poor monetary practices of a government. When a government is printing money like newspaper, people need ways to preserve their wealth and not need to depend upon other governments for their currencies and CBDCs. That is what main usage of Bitcoin is in current day. Bitcoin/Ethereum is not really useful for transactions because of the slow nature of transactions.

B. The other prominent usage of decentralized cryptocurrency is as a vehicle currency, that is way to send money abroad without all the charges involved today. This is possibly the use that government officers might be worried about and rightly so due to security concerns. There should be strict ways to regulate the improper money transfers but in my view banning decentralized cryptocurrencies over this is a bit over the top.

One more concern over decentralized cryptocurrencies is that people can be conned and can lose their savings over bad explanations of the new concept of currency in software.

All in all, I see CBDCs and Decentralized cryptocurrencies operating in parallel without disrupting each other.

### My answer to “Is it true that the Indian government is banning deep learning and blockchain technologies?”

Originally answered here : <https://qr.ae/pNQXAI> . Note this was much before Feb 2021.

No. Nothing like that is happening. Pure misinformation.

Infact, government organization Startup India ( [Homepage](https://www.startupindia.gov.in/)

) collaborated with Softbank ( [SoftBank Group - Wikipedia](https://en.wikipedia.org/wiki/SoftBank_Group) ) to give Tech4Future award which my Deep Learning startup [ParallelDots](https://www.quora.com/topic/ParallelDots) won. Details here: [ParallelDots Wins the Tech4Future Grand Challenge Powered by Invest India and SoftBank Group](https://www.business-standard.com/article/pti-stories/paralleldots-wins-the-tech4future-grand-challenge-powered-by-invest-india-and-softbank-group-119061400236_1.html) . There have been other similar approaches where government is encouraging Deep Learning startups, like the latest BSF startup challenge where BSF is awarding a good autonomous UAV startup [Challenge](https://www.startupindia.gov.in/content/sih/en/ams-application/challenge.html?applicationId=5d07381fe4b08f8b1a9c75da)

. So AI will be soon guarding Indian borders agains terrorists.

Similarly with blockchain. Almost all forums for government startups list fintech, AI, blockchain and robotics as the next area to target. Government plans to build blockchain itself for multiple uses: [India's National Payments Corporation Wants to Build a Blockchain Solution - CoinDesk](https://www.coindesk.com/indias-national-payments-corporation-wants-to-build-a-blockchain-solution)

There is one place where the government is very hesitant to allow companies: cryptocurrencies. Cryptocurrency is one of multiple ways where blockchain technology can be used. It is **controversial** and **has been used to take advantage of poor and less informed people** in other countries. Indian government is right IMO to have reservations about usage of such a technology. Its a systemic risk and needs to be regulated (regulated is not banned BTW).



https://youtu.be/-Jn41vwZd94

India has not banned even cryptocurrency completely as of yet btw :

I am tired of writing a [@coincrunchin](https://twitter.com/coincrunchin?ref_src=twsrc^tfw) article after reading shitty articles by Mainstream media. So lets do a thread.  
  
The report: India is bringing a law to ban crypto trading is written by [@archchaudhary](https://twitter.com/archchaudhary?ref_src=twsrc^tfw) & Siddhartha Singh.   
  
It has been syndicated to many other news portals.

— Naimish Sanghvi (@ThatNaimish) [September 15, 2020](https://twitter.com/ThatNaimish/status/1305958392985350145?ref_src=twsrc^tfw)

IMO, we should have restrictions on bitcoin businesses just like we have SEBI for public companies.

In case involuntary public facial recognition using Deep Learning starts, people will want government to put limitations on Facial Recognition Deep Learning startups too. That will not mean banning all Deep Learning startups.

### My answer to “How will rising inflation affect the global economy?”

Originally answered here : <https://qr.ae/pNQXtl> [in context of a possible inflation post COVID19 disruption]

We have not seen retail inflation rise yet despite of governments running their money printers due to pandemic disruption. Some people think that maybe economies {at least the US economy} has become resistant to inflation forever because the supply of money printed into retail economy is not that huge. The money being printed is mostly buying assets from banks which can be further lent out/invested.

[https://youtu.be/3-dvi1f\_2vA](https://youtu.be/3-dvi1f_2vA)

We have no other alternative to money printing during a pandemic. The direct handouts to people was not really enough for them to go splurging after goods, but just to keep the economic motor running. We needed that to avoid a depression. If the money supply in economy would have reduced due to people saving instead of spending, the economy would go into deflation mode. Retail inflation is thus controlled as money supply has been restricted to look like normal circumstances and not excess of cash. The most responsible economies are the ones who have just printed this much money or not much more than this money to keep economy afloat. Responsible is safe, but might not be the best.

But all the stimulus given out in US was not to individuals, a lot of it goes to financial institutions too. Whether pumping much more money into banks and financial institutions has actually increased economic risk is yet to be seen. However, it does feel that there would be two long term effects :

1. People are seeing wealth rise in stocks. Stock markets have been on a rally. While investors are being clever and investing in long term stocks like tech and alternative energy, its not like their wealth is not going up and all they are looking for is delayed gratification. When all this wealth increases, some day it might come back to retail markets when people want to cash out. Whether that changes the inflation/affordability in long term is to be seen. Maybe the hyperinflation that would happen today if all money was dispersed into the economy will slowly balance out as increase in purchasing power over years as these investments yield opportunities ? There is no historical lesson for such a thing so we still need to wait and watch.
2. Another topic is while there are people who are using the government handouts to just sustain themselves, there will be people whom these stimulus would make extremely rich and in control and knowledge of resources of future. So there is going to be increase in inequality and gatekeeping. This might lead to a feudalistic society with happy serfs living on handouts but being so far behind the elite (and their clergy) that their is no way they could bridge the gap [and maybe they don’t even want to if handouts are decent enough]. Think of it, there are people who got 1200 dollars to handle their life’s complexity while others, unknowingly to them (as it did not cause any inflation/inconvenience), just gained immense power over them by becoming future rich through the technologies which are supposed to run the world in future. This is not just a 1%-er discussion by the way. Someone who bought two iPhones and airpods last year lost out considerably to someone who could manage with a cheap Android and invested the rest in Tesla. We don’t really know if a society of happy serfs exists [because their hasn’t been one], serfdom used to become unsustainable making sure a deliberate or forced wealth redistribution occurred. Or maybe we actually voluntarily redistribute the wealth as inequality rises and the TV series Brave New World has had too much effect on me :P .



### My answer to “How does a tweet from a high profile person change the market value of crypto, e.g., Elon Musk?”

Originally answered here: https://qr.ae/pNEyrj

Any investment is mostly about trust, and damn people trust Elon Musk. Look at his online fanboys and believers. Whatever new technology he has touched {digital payments in paypal, Electric cars in Tesla and reusable rocktships in Spacex have become mainstream}. Elon Musk endorsing Bitcoin, not just verbally but also Tesla putting over a billion of its money in bitcoin, in a way convinces many people that Bitcoin will be real and not just a toy for nerds.

Crypto’s market value will rise until :

1. Either it fizzles back into oblivion like previous times,
2. Or it becomes mainstream and rises until crypto achieves its actual value after which it would go stable.

The odds of two becoming a reality become much more have suddenly gone up with Tesla putting money into it. That is the reason why people are investing like crazy to take advantage of a possible boom until stability/corrections.

### My answer to “Elon musk stated “bitcoin is arguably deflationary to a fault” what does he mean by that? How can an asset to be “deflationary to a fault”?”

Originally answered here : https://qr.ae/pN6dFE

Elon Musk is not talking about cryptos as currencies and not assets.

Bitcoin is prone to deflation because you cannot print Bitcoin beyond a certain limit. There have been visible problems in the past when supply of day to day currency was limited by some factor {say gold standard in 19th-20th century}. The fear of individuals during bad times can trigger a deflationary spiral like 1930’s great recession.

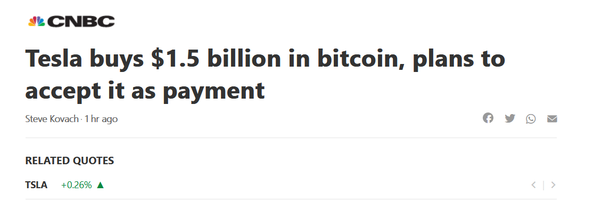
This is exact opposite is what happened in Zimbabwe or current day Venezuela is excess note printing. The currency becomes newspaper in such cases. You cannot just increase currency supply and solve all problems. However, in times like the COVID crisis when people dont want to or cannot spend, government needs to print and spend.

We are seeing both point of views take place in real world crypto. While bitcoin is being bought as a bet against note printing machines as it cannot be diluted by making more currency, Elon’s new favorite DOGE is being thought to be a day-to-day use cryptocurrency. New DOGE coins can be printed with certain rules. With the record breaking currency being printed, people are buying Bitcoin and Ethereum as a hedge. DOGE on the other hand is seeing a surge as people think its going to be a day to day crypto {at least the Reddit WSB community believes so}

I guess the point is that people can have opt in or opt out of currency policy as they wish. [Which is really cool !]

Few hours after I write this answer :

[Tesla buys $1.5 billion in bitcoin, plans to accept it as payment](https://www.msn.com/en-us/money/companies/tesla-buys-2415-billion-in-bitcoin/ar-BB1duGM7)



Elon is not really “anti bitcoin” if it felt like that in anyway :



### My answer to “Does bitcoin price rise and volatility simply a symptom of our lizard brain to want to gamble? What more evidence do you need than seeing that those with least knowledge of the technology and cryptography have punted the most on bitcoin?”

Originally answered here : https://qr.ae/pN6dHH

Unlike what many of us think, you don't necessarily need to understand things in depth completely to make something work. You need to have one correct idea about the situation that is working and scale it more and more.

While understanding things is a full time profession, doctors, engineers, scientists, economists do it all the time, that doesn’t really mean they are the only ones who sell technology or innovate or be an athlete. In simpler words, a doctor who understand how body functions can be an athlete, but an athlete doesn't need to be a doctor. For being an athlete, one has to practice one skill that is running, for being an athlete and a doctor : one has to practice two skills, running and medicine. If anything being an athlete and a doctor is harder than just being an athlete or being a doctor.

So all you need to understand while investing in bitcoin is its behavior as an asset, when to buy and sell. You need to understand some of the technology, but bitcoin was invented to be a normal day-to-day currency and not a “currency for computer science graduates” and requires one to understand day to day economics to use it.

Another thing is that everyone needs to know is that gambling is not bad. In fact, its good and should be encouraged for the amount of risk appetite one has. Goes without saying that mindless gambling is much more than one’s risk appetite and is stupid. If Wright brothers did not gamble, we wouldn’t have the aircraft, if Columbus did not gamble his life {and queen of Spain her money} we would not have Americas. I have no idea why gambling is being called lizard’s brain here !

### My answer to “Who would be responsible if the Bitcoin price just crashed to pennies?”

Originally answered here : https://qr.ae/pNj8W9

Some shock event.

One possibly big roadblock that can hit bitcoin and other cryptocurrencies is regulation by different countries banning their use.

This might be done for variety of pretexts :

1. Fear of investors being taken advantage of
2. Pushing CBDCs issued by central bank
3. Avoiding cryptocurrencies giving competition to local banking system.

In case of regulations by major countries like US, EU, China and India, bitcoin might dive in value.

Apart from this the only problematic event I can think of is fizzling out of the interest in crypto just like it happened in previous volleys. However, in such case, price will not crash but come down more gradually.

### My answer to “Will gold’s value be wiped out like aluminium if Bitcoin becomes the official currency?”

Originally answered here : https://qr.ae/pNJvOw

No way ! Not for a few centuries.

Gold is never “going out of fashion”, unless of course we start mining asteroids for gold and we have so much gold that you have gold like Iron. [That is not impossible by the way, but a distant scenario]

Bitcoin somewhat does many functions of what gold is in today’s world :

A. International Currency

B. Value independent of governments’ monetary policies thus free from Quantitative easing

C. Both are incorruptible in value. Bitcoin due to mathematical guarentee and gold due to its deep cultural connection. [I mean you can mix stuff in Gold I am not speaking of that kind of purity] . You can be sure if you hide Gold underground and take it out 500 years later, 1. Gold is a nobel metal so it will not get corrupted chemically and 2. people would still value it, its not going to become just a piece of metal. Botcoin has property 1 but still needs to stand the test of time on property 2.

D. Limited. You have scarce new bitcoin with time and you have somewhat scarce gold in the world.

The reason why gold will not go the way of Aluminum is ***D*** . Aluminum is one of the most abundant elements {the most abundant metal infact, more than Iron} in Earth’s crust so its value was high because it was hard to extract, bot because it was rare. [Hall–Héroult process - Wikipedia](https://en.wikipedia.org/wiki/Hall–Héroult_process)

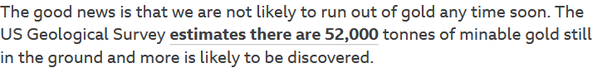
disrupted its value by making extraction of Aluminum cheap. Gold, however, is hard to become easy, because humans have already mined most of easily accessible Gold from Earth.

[How Many Bitcoins Are There?](https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/)



[How much gold is there in the world?](https://www.bbc.com/news/magazine-21969100)





The cost of gold mining is going up [because of the nature of deposits left to extract and high environmental cost] and it might eventually become pointless to mine it due to this factor. {This is less sure of a scenario than final bitcoin however as we mind end up finding new deposits in Earth or mine gold from asteroids}.

Bitcoin [and other cryptocurrencies] are an alternative to Gold, but they are still not complete alternatives, [Look at point C above]. It will take centuries to establish whether they are able to stand the test of time like Gold and thus you can be sure that Gold is not going away for that amount of time. Maybe even after that it lives as one alternative international currency along with cryptos.

### My answer to “What do you think has more value in today's world, data or money?”

Originally answered here: https://qr.ae/pND8bJ

Data is the new money ! I mean all cryptocurrencies are just cryptographically anonymized data about spending.

Power comes from many sources : Data is one source, Money is another, power of state is one source, belief of people is another source, skill is one such more source of power.

I think the answer is situational as data can be used to generate money and money can be used to create infrastructure to accumulate data. Its like answering the question about whether a Lion wins in a fight or Tiger. Case by Case.

### My answer to “Why don't currency notes have digital signatures? That way a note can't be counterfeited unless criminals know the signature as well.”

Originally answered here: https://qr.ae/pNVwK3

Just having digital signatures doesn’t make currency notes robust to counterfeiting. Any digital signature can be forged {because forging is just copying, you can only make copying as hard}, not a big deal.

If you are referring to digital signatures like those used in centralized or decentralized cryptocurrency protocols like [Ecash - Wikipedia](https://en.wikipedia.org/wiki/Ecash)

or [Bitcoin - Wikipedia](https://en.wikipedia.org/wiki/Bitcoin)

who have guarantees of no-counterfeiting , you should understand that its not just digital signature that ensures no duplicate spend. Its a combination of ***A. Digital Signatures, B. Keeping a track of currency flow and C. Ensuring sanctity of data for point B*** which can make sure that there is no counterfeiting.

Unless you keep a track of cash flowing from one person to another, you cannot implement the no counterfeit property of cryptocurrencies in cash. If you want to understand how this process is done technically, please refer to my answer here : [Muktabh Mayank's answer to What technology is used to record cryptocurrency transactions?](https://www.quora.com/What-technology-is-used-to-record-cryptocurrency-transactions/answer/Muktabh-Mayank)

To sum up, in cash you know where the money flow originated from [who took out the bank note from bank], but you don’t know its path. In Crypto, you know about the source of the money [all account names have anonymous signatures], and you know the entire path currency traces in terms of anonymous handles. A digital signature can only guarantee latter type of currency flow to have no counterfeiting . Cryptocurrency has much more information available, just that the information is anonymous.