Has Bitcoin Failed?

A subjective evaluation of its different aspects

Atis E

Follow

--

Listen

Share

A number of different narratives have been evolving about Bitcoin over the years. There are many wildly optimistic claims about the potential of Bitcoin and other cryptocurrencies — and there are plenty of wildly pessimistic ones, too! Maximalists of various kinds claim that cryptocurrencies and “blockchain” will solve all of the world's problems. On the other hand, their main application so far remains speculation.

If it would be the case that Bitcoin is only good for investment and trading, then Bitcoin would, in my mind, have failed — not completely, but to a large extent. Is it indeed the case? How well Bitcoin and other cryptocurrencies have met the various expectations of these past narratives?

Digital gold

Bitcoin as a long-term investment obviously has succeeded so far, in line with the wildest predictions from the early 2010s. The long-term gains have turned out to be worth the high volatility and risk. On the other hand, many expected not only that the price would go up, but the volatility of Bitcoin would decrease as its market cap got bigger. As recent events show, it has not happened. A case in point is the March 2020 crash, when the price fell by more than 50% in a short time. Furthermore, I’m inclined to believe that Bitcoin is unlikely to ever stabilize, as it lacks the flexible monetary policy of fiat currencies To put it simply, fiat currencies are more stable because central banks work on making them stable. The flexible monetary policy goes against every founding principle of Bitcoin, so volatility will remain a problem.

Current status:

excellent

Potential:

good-to-excellent (subtracted points due to high volatility)

Decentralized cash

Satoshi Nakamoto's famous white paper envisions a "peer-to-peer version of electronic cash". It is fair to say that it has not happened. Bitcoin is not good for small payments. Other cryptocurrencies have made some improvements in this aspect, but they either provide insufficient scalability improvements to be real game-changers, make fraudulent claims, rely on unproven technology — or do all three at the same time.

Layer-2 solutions promise to facilitate small-scale payments, but despite years of work they essentially do not exist in a scalable, real-world usable fashion. The amount of bitcoins locked by the Lightning Network is negligible and is not growing since early 2019. Other Layer-2 approaches are even further away from reality. A fundamentally new approach may be needed. For that, a new scientific breakthrough may be necessary, similar in scale to the invention of the Nakamoto consensus. While such progress is not against any fundamental limits of physics or computer science, expecting it to happen just because “there is a demand for this” is as naive as expecting cancer to be cured in the near term-future just because a lot of people are working on it.

Furthermore, even assuming that the Lightning Network does an excellent job at what it's designed for, the scalability limits in Bitcoin itself are so bad that it's not even possible to “onboard” most people on the Lightning Network in a reasonable time. Let’s assume that each person only wants to record one transaction on the chain, the rest may take place in the Lightning Network. Given that there are 7 billion people on the planet, and that Bitcoin has throughput limits of a few transactions per second (“7 transactions per second” is often mentioned, though it may not be accurate), it would take on the order to billion seconds to onboard everyone on the Lightning Network. In other words, tens of years. Not to mention any other ongoing transactions.

Current status:

poor for Bitcoin, poor-to-average for other cryptocurrencies

Potential:

unclear

A hedge against bad governments

Bitcoin cannot be fully banned due to its decentralized nature. Its use may be made difficult; however, bad governments in the real world are often disorganized to the point that enforcing effective bans simply may be out of their reach. It seems that Bitcoin really has some promise here: both as a hedge against bad policies enacted by the governments and a way how to fight downright persecution.

There is evidence that Bitcoin has already helped the people ofVenezuela and dissidents in many countries, including Navalny's supporters in Russia.

Current status:

fledgling

Potential:

unclear-to-good

A hedge against market instability

If cryptocurrencies belong to a new asset class, they may create a new way how to hedge investments — plainly speaking, a way how to reduce the risk to suffer from market crashes. However, at the moment is seems that cryptocurrencies are in fact correlated with the stock market.

It is difficult to draw any strong conclusions here, as there is no clear evidence either way. Since Bitcoin emerged in 2009, there hasn't been another big global financial crisis. However, we have some tentative evidence since March 2020, when the world comes closest to a big financial crisis due to the COVID-19 pandemic. Bitcoin did not handle it well: its price crashed more than 50% in a few days.

Current status:

poor-to-unclear

Potential:

unclear

Open, decentralized, trustless

Bitcoin certainly is open, in the sense that everyone is permitted to use it and to participate in its mining.

Bitcoin is to large decentralized or distributed, though the details depend on the precise definitions of these worlds. Many cryptocurrencies are inherently less so: there is no such thing as the "Bitcoin Foundation" that attempts to control the policies of the Bitcoin network, but many altcoins have them.

Bitcoin is more trustless than other payment mechanisms — for example, it is censorship-resistant to a large extent. However, trust is still required in other aspects, for example, in the correctness of the source code, which so has not been formally proved to be free of errors.

Current status:

good

Potential:

good-to-excellent

An alternative to the current financial system

"Hyperbitcoinization" is the hypothetical event when a bitcoin-based financial system replaces the current, fiat-based one. (It is not clear to me whether there is such a thing as a single "current" system.) Ideological considerations aside, it remains unclear how this could ever take place, given the inherent lower efficiency of decentralized systems. In computer science, centralized approaches are pretty much always more efficient than decentralized ones. The weaknesses of centralized systems lie elsewhere: in their limited resilience and lack of censorship-resistance. Due to these different strengths, it seems that the coexistence of multiple approaches is inescapable.

I personally believe that cryptocurrencies will serve as a base of one of these systems.

Current status:

fledgling

Potential:

no potential for replacement, good potential for coexistence

Private and anonymous darknet currency

This apparently was a big narrative back in the early days. Then at some point most users switched to the opposite view, which pictures Bitcoin as an exceptionally transparent currency, with all of its transactions “public, traceable, and permanently stored in the Bitcoin network”. A handful of privacy coins took up the “darknet money” banner from Bitcoin back in the mid-2010s. These coins have not, as a whole, been especially successful.

The truth is that privacy and anonymity are still very many areas where future developments are expected in Bitcoin, and the overall direction is not clear. The vast majority of Bitcoin’s potential users are not interested in having extreme privacy or spending their bitcoins on darknet. They may even see the privacy features as detrimental in case such features make Bitcoin less desirable from the perspective of national governments and law enforcement agencies.

Current status:

poor for Bitcoin, good for a few other cryptocurrencies

Potential:

too early to tell in the case of Bitcoin

A global, open, immutable ledger for storing data

Bitcoin. it has established a lower bound of the value of a bitcoinby looking at Bitcoin’s ledger as a potential replacement for notarial services. It declares “the intrinsic value of around $10,000 per bitcoin”.

While the practicality of this approach is somewhat doubtful at the moment — to my knowledge there is no legislation that would allow replacing notarial services with an electronic database — the idea is fundamentally sound, and the core technology required for it already exists. (Bitcoin has a script opcode called OP_RETURN that allows writing arbitrary data in the ledger.) It just needs to be more widely used.

Current status:

technically sound, but virtually unused so far

Potential:

good

Programmable money for all-purpose services

Ethereum made a key addition to the cryptocurrencies in 2014: it came with a Turing-complete programming language. This allowed the development of smart contracts — pieces of code included in the blockchain and executed by the network's nodes. In theory, such a smart contract functionality can also be added to Bitcoin. (As of now, this is unlikely to happen in practice; in fact, some of the scripting functionality originally present in Bitcoin has been disabled, making it less, rather than more capable.)

There have been a number of narratives behind smart contracts, but one of the main ones has focused on the possibility to automate different kinds of actions, such as paying for services and goods. For a wild example, consider this scenario seriously proposed a few years ago: “a self-driving car may use smart contracts to pay other cars and the road-side infrastructure for sensor data and to pay other cars for the right to overtake them”. For a more down-to-earth example, consider smart contracts for database access rights, or smart contracts for supply chain tracking —i.e. tracking goods across multiple suppliers, and recording whether the goods are always traveling at the right environmental conditions.

However, a key problem here is “where does the input data come from, and how to ensure that it is reliable?”. This problem is still fundamentally unsolved. The interface between the physical world and the blockchain can never be perfect. For instance, in the supply chain application, one always needs to be prepared to deal with environmental sensor measurement inaccuracies, misplaced sensors, or downright forged sensor readings.

Current status:

large technical problems exist in many potential application areas

Potential:

will fall short of expectations

Programmable money for financial services

It was quickly discovered that automating some services is easier to automate with smart contracts than other services. Trading, for instance, is simpler to automate when compared with supply chain tracking. For one, financial services is simply a more lucrative field. More importantly, the inputs and outputs are often digital, and as such more easily verifiable. It is therefore more feasible to construct “oracles” that provide trustworthy input data for such applications. The (qualified) success of ICOs in the previous market cycle and the rise of DeFi (Decentralized Finance) in the recently marked cycle show that this new narrative is catching on. However, this is unlikely to become a big application area for Bitcoin in particular.

Current status:

fledgling

Potential:

good (for altcoins)

Digital collectibles and tokens

Sure, cryptocurrencies may be a very good medium for creating digital tokens and collectibles — but how much value really is in these things, in the first place?

And yet, here we are again — the latest rise of Dogecoin is a slap in the face of all “rational” analyses.

Current status:

average-to-good (for altcoins)

Potential:

good technical potential to deliver (for altcoins), unclear potential to create a long-term value

Fixed cap money

It is a fact that the yearly issuance of new bitcoins is limited and will eventually cease altogether. While this can be changed by tweaking the Bitcoin source code and running the changed code on majority of the nodes in the Bitcoin network, such a change would destroy most of its value, and as such is very unlikely to happen. (If it would happen, then almost certainly as a hack aiming to do precisely this; however, such a successful attack is unlikely, as Bitcoin has demonstrated to be hack-resistant for 10+ years, both in practice and in theory, largely due to its decentralized nature.)

In theory, this fixed cap property creates a strict upper limit on the amount of assets available in this class. In reality, it is not as clear cut as maximalists would like it to be:

- The increasing number of Bitcoin forks shows that it is possible to create new value simply by forking the chain.
- Altcoins provide additional competition to Bitcoin, with a practically unlimited supply of chains and coins.
- It is not clear whether Bitcoin can actually remain fully functional at the point when the block reward is eliminated. We will have to wait until around 2140 for empirical proof.

These all have proven to be minor problems so far — Bitcoin forks and altcoins are not especially valuable, but they do create potential future risks.

Current status:

good

Potential:

unclear-to-good

A way how to do free and almost instant transactions

This used to be a selling point of Bitcoin in the early 2010s. Free Bitcoin transactions were actually possible at that time. Most of Bitcoin's transactions were free before 2013, and a few % remained free as recently as 2014. It is fair to say that this will not repeat in foreseeable future.

Regarding the transaction speed, it was favorably compared with Western Union and other money transfer services. However, as the traditional banking system is evolving, any advantage Bitcoin may retain here is short-lived.

Current status:

the narrative has been replaced and almost forgotten

Potential:

low, as depends on solving the scalability problem

A solution for remittances

Remittances are cash transfers, typically made by people working abroad. Bitcoin was promised to transform this field, apparently currently relying on slow and expensive services.

However, remittances would need "free and almost instant transactions" to happen first. See above for the reasons why they have not happened.

A functioning remittance system would additionally

require either:

- currency conversion before and after the transfer;
- Bitcoin being accepted as a digital cash in the home country.

In both cases, the volatility of Bitcoin creates a significant margin risk. This risk almost certainly dwarfs the 10–20 USD fees of the traditional postal services.

Current status:

narrative has been replaced and almost forgotten

Potential:

low, depends on solving several problems

A solution for "banking the unbanked"

Apparently, there are billions of people around the world who are somehow excluded by the current financial system. The promise here is that Bitcoin may give them full financial services — not just a bank account, but a whole "bank in their pocket".

Of course, this use case requires Bitcoin or another cryptocurrency is suitable for use as digital cash, which is not currently possible due to the scalability problem.

Current status:

narrative is not especially active

Potential:

low, depends on solving at least the scalability problem

Space coin

The science-fiction writer Arthur C. Clarke was one of the first to consider the problem of universal currency. He proposed a realistic solution: namely, that energy could serve as a universal exchange unit. Energy can be harvested, traded, and spent. Energy expenditure roughly correlates with living standards.

However, exchanging energy is cumbersome, slow, and requires either physical proximity or expensive dedicated infrastructure. When looking into the far future, such an exchange of energy is not feasible on the Solar system scale. Bitcoin or similar proof-of-work coins could serve as a proxy for the ability to generate energy. One drawback here is that due to the limited speed of light, space coins must have very large block times. Another problem is that a spatially localized mining operation (e.g. a single planet) with a sufficient hash power can effectively censor the transactions submitted from

elsewhere and blocks mined elsewhere. However, assuming that we do expand in space, there may be some opportunities for system-wide cryptocurrencies.

Current status:

highly speculative theories only

Potential:

too early to tell, but speed-of-light limits could be a major problem

What's next?

As the year 2021 goes on, we are very likely to see not just new highs in price, but also the end of the current market cycle, and the start of a new multi-year bear market. Reflection can be beneficial as this happens. Bitcoin is designed to be ultra-resilient. This has allowed it to survive and thrive so far, despite failing to live up to some of its narratives, including the major failure to become a democratic peer-to-peer digital cash.

To me personally, the main lesson from the current market cycle was that achieving scalability is harder than was initially expected. Multiple potential solutions seemed to be just around the cornerback in 2017. At the start of 2021, these solutions either remain just around a corner or have been tested in practice and fallen short of the ideal in many ways. So far, there is no universally accepted Layer-2 solution for Bitcoin, and there are no altcoins that would be simultaneously secure, scalable, and decentralized. 2021 is an exciting year because we can expect several new approaches to testing the waters.

References / further reading

The Internet of Money series

Every Reason Bitcoin Will Not Fail

Welcome to the r/Bitcoin FAQ

Common Bitcoin misconceptions