Cryptocurrencies as Cyberstatism

Frank Braun

2020-01-06

Prelude

(Note: Most of this prelude has been put on Twitter[1] before, the impatient reader might want to skip to section Cyberstatism)

I have been wondering for a long time why cryptocurrencies in general and Bitcoin especially became so, for lack of a better word, toxic.

Maybe it's just my personal experience and that experience is totally subjective, but to me it seems that the level of hostility experienced (mostly) online in Bitcoin is way stronger than:

1. It was in the beginning. I have been "around" Bitcoin since the very early days and I didn't experience it like that at all during that time. It seemed to be more of a collaborative effort driven by the excitement of building something new and potentially revolutionary.
2. The level of hostility which can be witnessed in other tech oriented online communities. Nerds are kind of famous for strongly voiced opinions, especially regarding their favorite tech, may it be an editor, operating system, or programming language.

However, the toxicity level in cryptocurrencies in general and Bitcoin especially seems to be off the charts compared to other tech projects. It seems to be have become almost impossible to have rational discussions about technical details that do not devolve into flame wars.

My first hypothesis for why that is the case was:

Toxicity is the consensus mechanism in Bitcoin.

The reasoning being that while proof-of-work is a great mechanism to reach consensus in the distributed ledger for **already agreed** upon rules, it is terrible to reach consensus for **rule changes**.

If not most of all miners and users agree on a rule change it will lead to a fork.

[1] https://twitter.com/thefrankbraun/status/1213190589149265922

Forks lead to a fracturing of the user base **without** solving future conflicts. The BTC/BCH fork was such a case. The BCH/BSV gives empirical evidence that a fork doesn't solve that problem permanently.

Forks are economically bad, because they lead to a fracturing of the user base and developers, bring uncertainty for new and existing users, etc.

So basically the only good rule change mechanism Bitcoin has is to reach nearly 100% consensus between miners and users **upfront**, which makes it extremely hard to make even very desirable upgrades.

This solidifies the Bitcoin protocol and makes it attackable by altcoins (in terms of additional features).

It has been argued that a solidification of the Bitcoin protocol is not necessarily a bad thing, especially given the "digital gold" and Bitcoin as a store-of-value narrative.

So an economically sound consensus mechanism (for rule upgrades / governance) seems to be toxicity.

Toxicity keeps the community together and bashes all outsiders (for example, this leads to terms like "Bcash" and "shitcoins").

However, toxicity alienates outsiders and prevents upgrades, making Bitcoin effectively the orthodoxy of cryptocurrencies.

So either the Bitcoin protocol is good enough as it is to build innovation on top of it (there will likely not be any major changes to the protocol) or it will be out-competed in terms of features.

Granted, given Bitcoin's first mover advantage, brand recognition, and its position as the major cryptocurrency and default trading pair on most exchanges might give Bitcoin a position which is uncatchable far into the future.

Newer cryptocurrencies like Decred[2] put a consensus mechanism in place which is extremely fork resistant (see Detailed analysis of Decred fork resistance[3]), which might be the reason why the discussions over there seem to be much more civil, they actually can resolve disagreements without a fork.

But it might also be that it's just because their community and position in the market is much smaller.

Cyberstatism

The argument above might explain parts of the picture, but further discussing and thinking about the problem let me come to the following, for a libertarian rather uncomfortable, conclusion:

[2] https://decred.org/

[3] https://medium.com/decred/detailed-analysis-of-decred-fork-resistance-93022e0bcde7

Cryptocurrencies are a form of Cyberstatism.

Let me try to explain what I mean by that phrase.

Cryptocurrencies like Bitcoin are a form of Fiat money[4] in the sense that they create money "out of thin air" which doesn't have intrinsic value to begin with. Granted, most cryptocurrencies do not suffer from the inflation problem of government fiat money (cryptocurrencies usually have a fixed monetary supply) and energy has to be expended in order to "print" them (through mining).

However, cryptocurrencies like Bitcoin lack intrinsic value when they are started. The famous Bitcoin pizza purchase[5] is often viewed as the point in time where Bitcoin switched from being a curiosity to becoming useful and valuable as a medium of exchange.

If you look at cryptocurrencies from the lens of fiat money, different cryptocurrencies competing with each other could be viewed as a zero-sum game. They are all competing to become "cybermoney" (a term from The Sovereign Individual[6]), just like states compete over a fixed amount of available *territory*.

If the market for cybermoney is fixed, this is a zero-sum game and competing cryptocurrencies indeed show signs of competing states.

Politics becomes the main mechanism of resolving conflicts, not competition of different products on a free market.

Coins forking off become secession movements and are fought strongly as such (e.g., BTC/BCH and BCH/BSV).

People heavily invested into certain coins (emotionally and/or financially) start to behave like nationalists, fighting for *their* coin and *against* the other coins. Financial investment only makes that a stronger force, because it makes economic sense (if the coins "captures" more territory the value of the investment will go up).

Like with states, the biggest player often becomes the biggest bully...

Conclusion

This is just a theory and I'm sure I will get my fair share of hate for it. If, however, there is some truth to the argument I'm wondering what the conclusion is, given that I find it rather worrisome from a libertarian perspective.

First of all, the competition to become "cybermoney" is **not** a zero-sum game. The real competitor is government-issued fiat money and upcoming state- and corporate-issued cryptocurrencies like Facebook's Libra. That's where the actual war is fought and where it is determined if the world will see an alternative to

[4] https://en.wikipedia.org/wiki/Fiat_money
[5] https://en.bitcoin.it/wiki/Laszlo_Hanyecz
[6] https://www.goodreads.com/book/show/82256.The_Sovereign_Individual

fiat and these centrally controlled coins. Since there is a "war on cash" going on, there seems to be a limited amount of time left to establish one or more decentralized cryptocurrencies as a valid alternative **for payments**.

Furthermore, exchangeability between different cryptocurrencies independent from centralized exchanges is of paramount importance. The Decred DEX[7] and Bisq[8] are very important steps in that direction. What is also needed is a wider availability of over-the-counter exchanges that allow to trade cash for crypto in person.

If all cryptocurrencies can be easily exchanged for one another in a decentralized fashion, they can compete with each other more like different products on a free market and form a "cyberbloc" against the real enemy. There is no need to look at the competition between different cryptocurrencies as a zero-sum game.

Given the two, focus on the real competition and better exchangeability between different cryptocurrencies, it might be possible to make a real dent into the system of government issued fiat money.

[7] https://github.com/decred/dcrdex
[8] https://bisq.network