Post 1 of 3 on Crypto.

How clean is your Bitcoin? Date 2025-8-12

Carlos Alegria

In this age of government surveillance and no privacy, I love the idea of individuals coming together and building new, organic communities for human interaction. I love the possibilities of the blockchain technology to solve many of our challenges in the digital era. Disclosure: I own crypto assets, including bitcoin, so I have skin in the game.

Being a quant and working with the most liquid assets such as the S&P500, US Treasury bonds, major FX currencies, the most liquid commodities such as oil and gold, I was a late comer to the crypto world. I monitored it from a distance, "letting the technology mature".

In 2020, with the start of the COVID-19 pandemic and with too much time locked up at home without the possibility of social interaction, I decided to spend some time delving into "crypto". I did so not with the perspective of trading, but instead to understand the technology, do some experiments, and think about the possible implications for its use in society. After installing some crypto nodes at home, working with different coin API's and creating my own wallet software to understand the processes involved, I felt that I got a clear picture of the basics of the technology. At that point I started talking with enthusiasts in the crypto world and quickly noticed that most people do not understand the pros and cons of the technology. In this post I'll summarise some of my findings, and my concerns.

This post was written a few months ago, in September of 2024. I'm only publishing it now as since then at the bequest of different individuals, I expanded my thoughts into the wider context of crypto regarding their use in a future financial system. These are complicated questions with no definite answers but after some examination lead to more questions instead of less. This post is therefore the first of a series of 3 posts that will be forthcoming.

1. Public versus private.

There are two broad types of crypto assets. Public and private ones.

Public assets are those where the blockchain information is accessible to anyone and there are numerous tools to search each of the blockchains. The information written on the blockchain varies, but in general each transaction information is recorded, which includes the source account, the target account and the transaction amount.

Public crypto assets represent the vast majority of crypto assets and are what most individuals refer to when talking about "crypto". These include Bitcoin, Litecoin, XRP, Ether, etc…

There are a few private crypto assets, of which the oldest and most "well designed" is Monero. Private crypto assets also record the transaction information on the blockchain, but it is encrypted so that only the parties in the transaction can access it.

2. Path dependency. Are public coins/tokens fungible?

Most crypto enthusiasts state that bitcoin is like digital gold. Its quantity is limited by design (such as gold), it is mined (by using computing power to validate transactions on the blockchain), it is divisible and completely fungible (every bitcoin is equivalent to another).

Is it?

When crypto enthusiasts try to gaslight me, I ask them: "How clean is your crypto?". I'll explain why.

In public crypto blockchains, assets cannot be fully fungible. The reason why is that by searching the public blockchain we can track the full historical path that the assets took until they arrived at the owner's wallet. If,

for instance part of the bitcoin in one's wallet originated from a criminal activity such as a payment for a stolen car (say 5 transactions in the past), then theoretically and possibly in practice one would be complicit in a criminal activity and the best-case scenario would be the need to return the asset to the lawful owner.

Consequently, the value of each fraction of a bitcoin in one's crypto wallet is **path dependent**, meaning that some bitcoin fractions might be completely "clean" and others could be "dirty" will all shades of grey in between. To calculate the true value of the bitcoin in the wallet one would need to weight the probabilities (and expected loss) of each fraction of bitcoin in the wallet to be involved in an illicit transaction in the past.

When confronted with this question, most crypto enthusiasts go silent, and the conversation quickly changes direction. I must admit, I also continue owning bitcoin, but I still wonder...

This problem can only be solved with owning private assets.

3. Freedom to transact, without government control.

Crypto enthusiasts, like me, worry that we are in danger of falling into a social credit system where all our social interactions are monitored, and proper behaviour is "incentivised" by using a mixture of carrots and sticks.

Let's assume that Bitcoin is fungible and the "problem" that I mentioned before does not exist. Crypto enthusiasts tell me vehemently that Bitcoin is the solution for trading without government interference; and to avoid falling into a dystopian control trap, we need to avoid CBDCs (Central Bank Digital Currencies) at all costs.

Is this the case?

Yes and no.

Yes, CBDCs would equate to the ultimate control tool and should be avoided for transactions between individuals, if we want to keep our individual freedoms.

No, bitcoin would not be the answer, as, with centralisation of crypto assets and trading in regulated crypto exchanges together with public blockchains, a similar social credit system can be **easily** implemented. Even without the centralisation of bitcoin assets in exchanges, bitcoin could be easily used to impose a system of control, more so than by using the large payment systems such as VISA, Mastercard and Stripe.

For example, by creating an official registry of "flagged" Bitcoin accounts that is associated with a payment system, or exchanges, those bitcoin accounts could be all but frozen. Any account that transacts with a "flagged" account would also be "flagged" so that each individual would have an incentive to only trade with regulated accounts. As the blockchain is public, the system would be inescapable.

Ultimately, this problem can only be solved with using private blockchains.

4. Sound money. Protection against inflation.

Crypto enthusiasts often state that bitcoin, like gold, has limited supply and consequently it is sound money and would be a tool to limit inflation by the government printing of money.

Is it?

Bitcoin is indeed limited in supply to 21million bitcoins. Theoretically, it is true that bitcoins could protect owners from inflation. However, if we think of the broader crypto market, this is clearly not the case. Every single day numerous new crypto coins and tokens are launched and currently thousands of crypto assets are used. Consequently, even though the supply of bitcoin is limited, the supply of crypto is unlimited.

Crypto enthusiasts would retort: But then why would anyone want to own other crypto coins/assets? Bitcoin **is** the store of value. Other assets/coins are used for specific purposes (such as Ether to settle transactions in the Ethereum blockchain).

Well, this is obviously not the case. There are many other crypto assets, such as Litecoin, Bitcoin Cash, and many others, that are alternatives to bitcoin as stores of value.

Why would one want to use other stores of value?

Let's go back to the gold standard that was in place in the early 1900s. In 1930 the great depression was a worldwide economic downturn that was exacerbated by a debt/deflation spiral. In order to escape the depression, countries that decoupled from the gold standard recovered earlier than countries that stubbornly stuck the gold standard[1]. The US abandoned the gold standard in 1933 and only started its economic recovery from then onwards.

The experience from the great depression led to decisions being made by central bankers to embark in quantitative easing (printing money) to during the 2008-2009 great recession (US subprime housing crisis). These examples illustrate why new crypto currencies could be adopted by individuals (even without government intervention) in order to escape a debt trap, if the circumstances warrant such necessity.

Ultimately, a currency being a store of value is based on the confidence individuals place upon it, which applies to crypto assets as well.

5. Summary.

The questions I pose above arise from a simple dispassionate analysis of the technology and its potential pitfalls. This does not invalidate the usage of the technology as experiments for developing alternative financial tools. However, one must also pose deeper questions relating to systemic aspects of financial systems, in terms of the balance between security and privacy; protection of human expression (individual freedoms); protection of individuals' property rights from theft, fraud and mistakes; protection of systemic aspects of human interaction; and other.

The whole question of how to develop alternative means of human collaboration and interaction gives rise to complex questions at different levels. I'll be exploring some of these questions in following posts. Even though I do not pretend to have the answers to these complex questions, it is a worthy enterprise to ask the fundamental questions.

On a humorous note, don't panic just yet, I'm a crypto enthusiast myself. In the following posts I'll explore under which conditions public assets could be the solution for enabling human interaction we all dream of.

[1] https://www.aeaweb.org/research/charts/depressions-gold-standard-recovery