

Bitcoin: Should the Functions of Money be Separate, or All-in-One?

Money is a lot of things. Predominantly a unit of account, a store of value, and a medium of exchange. We're quite used to these functions being split up and handled by different tools.

Dollars are a medium of exchange in some countries. They are a unit of account in some countries. Sometimes they are one without the other, sometimes they are both at once.

Dollars aren't really a store of value in the U.S. If you have wealth, you put it into stocks, bonds, real estate, gold, antiques, or other assets or financial instruments, since the relative value of your cash in the bank is likely to decline.

In countries whose governments inflate faster than the U.S., dollars are sometimes used as a store of value, as are gold and a number of other things. The problem of storing value is much more difficult in poorer countries and places with very onerous financial regulations and where most people are unbanked and lack access to financial services. Wealth is literally inflated out of people's pockets before they can do anything about it.

Bitcoin emerged as the ultimate money. It satisfied the key criteria of money better than anything humans have used to date (Hard to counterfeit, uniform, divisible, scarce, durable, easy to store, portable).

The early coders who discussed and tested it had a grand vision. They saw Bitcoin supplanting government controlled money and financial systems. They believed it would unite the three main functions of money in one. It would be a store of value, since it's capped at 21,000,000 BTC, and even unbanked people can use it. It would be a global unit of account, since borders and central banks couldn't regulate it away like national currencies. Soon other currencies and commodities would be denominated in BTC. And it would be a medium of exchange, since no trusted third party is required to verify purchases, and it's more divisible and portable than any currency to date.

The mind-blowing implications of uniting these three functions of money are fun to consider. Can you imagine a world in which Keynesian schemes to stimulate spending and sap savings fail, because people see the real value of holding BTC vs. spending it? The capital accumulation available to all would be immense, and consumption would be weighed against the real cost, not obscured by artificially cheap credit and devaluing currency. The simplicity of accounting and global trade would be nuts.

But this might not be possible.

As Bitcoin grew, it seemed harder to imagine it uniting all three key functions of money. Many people saw a choice. Whether or not it's adopted as a unit of account, it had to choose one of the other two attributes. It could be a store of value or a global medium of exchange.

Why the choice? Bitcoin requires a lot of computing power to verify transactions. This is one of the things that makes it hard to counterfeit and free from trusted third parties. To be used as a global medium of exchange, Bitcoin would have to process thousands of transactions every second. This means larger "blocks" of data to be handled by miners, which would lead to larger server farms or mining pools handling most of the network.

Many fear this kind of agglomeration would threaten the security and freedom of Bitcoin, as bad actors or governments would have fewer parties to bribe or coerce. To remain as distributed as possible, the blockchain must maintain small blocks and therefore can never process more than a few transactions a second, with higher fees and confirmation times too slow for daily commercial exchange. The same procedures are followed when implementing blockchain for the automotive industry.

This is the tech objection to Bitcoin as a global medium of exchange.

There is an economic objection as well; a belief that the increasing value of BTC means no one will ever want to spend any so it can't be used for small exchanges. This objection falls apart rather easily, as there is a positive time value to money, and people won't starve to death with a wallet full of BTC. Spending may not be as profligate as it is under rapidly devaluing currencies today (this is not a bad thing), but spending would still occur and market rates for spending vs. holding would emerge, as well as ways to borrow against your BTC so you could spend now while not losing future value tomorrow. Also, just as people spend, they would also be earning. It's not as if people today only ever lose cash holdings. They add to and detract from them regularly.

Is the tech objection a deal-breaker for the bold dream of an all-in-one money? Probably not.

There are two main solutions currently being debated by people in the Bitcoin community. (I don't recommend weighing in unless you are prepared for comical levels of invective and *ad hominem*. It turns out, people are very emotional about which of these two solutions might work better).

The first approach is to accept that Bitcoin itself will always only be a store of value, or sort of reserve currency for the world in ways similar to gold, but more portable. It will be a "settlement layer" undergirding the global financial system, replacing clearing houses and other mechanisms used by banks to make large transfers. The high fees and slow confirmation times mean transactions more numerous or smaller than these massive

settlements don't make sense. Some businesses are using Bitcoin in this way already today.

Under this approach, while Bitcoin itself wouldn't be used as a global medium of exchange for daily purchases, it would provide a backbone upon which additional layers of fast, low cost, efficient payment processing could be built "off-chain" and only occasionally settled on the big blockchain. Any number of Altcoins or Bitcoin apps could be used as payment processors, just as today we use myriad forms of payment processing for dollars (credit cards, PayPal, gift cards, store credits, etc.).

The second approach is to increase the size of blocks mined on the network so that Bitcoin can handle thousands of transactions per second. This seems to be the idea that the original inventors of Bitcoin had in mind, as they assumed that computing power would continue to increase and that large agglomerations of miners would not be a major threat, as their economic incentive was to keep Bitcoin valuable, and allowing any kind of take-over would destroy it and their own ability to profit.

The two approaches above are, from my understanding, what led to the 'hard fork', when a new currency called Bitcoin Cash split from the main chain to continue down the path of larger and larger blocks to keep transactions fast and cheap with the vision of becoming both a store of value and a global medium of exchange. The other chain, sometimes called the legacy chain, instead added something called SegWit that helps improve speed and lower fees, but doesn't increase the block size...at least for now (there is a debate raging about whether to double the block size on the legacy chain, or hold it constant at 1MB. Bitcoin Cash has an 8MB size and, from my understanding, it will continue to increase as needed).

I have no idea which approach is better. Luckily, I don't need to know. We have both experiments, and probably more to come, so the individuals in the market can try them out and different solutions will emerge for different problems.

One interesting note is that both approaches want a money free from government control. Both claim (for good reason) to be continuing the original vision for Bitcoin. They both also want decentralization, but I think they define it differently, or worry about centralization in different ways.

Those who favor small blocks, where Bitcoin is a settlement layer, fear the centralization of Bitcoin miners they expect if blocks grow. To them, the best way to avoid central control is to have as many people as possible running the software.

Those who favor large blocks, where Bitcoin is not only a store of value but also the global medium of exchange, fear the centralization of off-chain layers which often require trusted third parties and may be easier for governments to control and shut down. They also fear

lower adoption rates if Bitcoin is only useful by large institutions for massive settlements. To them, the best way to avoid central control is to have as many people as possible using the currency.

I'm not a tech guy, and I'm sure I've used incorrect verbiage and possibly badly mischaracterized the tech. I tried to be honest and charitable about the two approaches, and I think I get the basic economics underlying both. I wrote this as much to sort through my own thoughts and come to grips with my own understanding as anything else.