Why Does Currency Have Value?

There's a general agreement that coins have value–this is a requirement for any currency to work. So how does it? Is it a "mutually-shared delusion"? Is it the "Tinkerbell effect" (i.e., value only exists because we all believe in it)? Is it based on the Greater Fool Fallacy (i.e., "I may be a fool for buying this, but there's a greater fool out there who will pay more")?

Are there any inherent reasons why Bitcoin should have value? Or is it just a "mutually-shared delusion?" There's no shared consensus–hopefully, we'll have a better understanding of it at some point in the future.

The Bitcoin Core Software

The core Bitcoin software ('bitcoind') is open source under the MIT license. What's interesting is that the software actually *encodes* (or even *enforces*) the rules of the system–in that sense, it's more than just source code.

BIPs

There are several Bitcoin Improvement Proposals (BIPs), which are formal proposal for changes to the Bitcoin technical spec and rationale. They're published in a numbered series and each has a champion to evangelize and coordinate on its adoption and implementation.

Core Developers

There are six core developers, including Satoshi Nakamoto and (previously) Gavin Andresen (who's now their Chief Scientist). The most "researchy" of the developers is Gregory Maxwell, while Jeff Garzik was seen as the "second-in-command" to Gavin. The lead developers are more powerful than other members of the Bitcoin network: **their rule changes will be followed by default**.

Rebelling Against Changes

If users don't like a rule change (e.g., a change introduced by the Bitcoin Foundation):

- With a centralized currency, users have the right to exit (i.e., cash out of the currency).
- With Bitcoin, **users have the right to fork the rules**.

This is a whole new way to fork that we haven't discussed in the past. When you fork in this manner, there are two ways to handle the blockchain:

- They could abandon the old blockchain and come up with a new genesis block (i.e., come up with a completely new AltCoin).
- They could inherit the blockchain up until the point that they decide to fork. This preserves those who are rich in the previous system, as their value is preserved after the fork.

The community processes that lead individuals to start AltCoins usually do so under the auspices of being "more democratic", etc. So they typically start from a clean slate, as they don't want to preserve the existing hierarchy.

If a hard fork was meant to start an AltCoin, then the AltCoin can go its separate way and the branches can coexist nicely. However, if a hard fork reflected a fight over the future of Bitcoin, then they'd fight for market share.

Stakeholders

Let's discuss potential stakeholders. In other words, who's in charge of the Bitcoin system?

- Claim: **Bitcoin Core developers**. They write the rulebook and almost everybody uses their code and follows their rules. But if they make an egregious change, everyone could just fork and not enforce it.
- Claim: **Miners**. They write history and thus history will be consistent with the miners' consensus rules.
- Claim: **Investors**. The investors determine whether Bitcoin has any value. In the case of a hard fork, you might claim that the investors decide which branch wins out.
- Claim: **Merchants and customers**. They decide that the currency has value.
- Claim: **Payment services**. They really handle transaction volume and make Bitcoin useable.

If the miners and developers got into a fight and a fork started, who would win out? And what would be the results? Well, there's one argument to be made that this fork would be better for everyone–maybe the differences between the two currencies suit some parties better and thus the granularity makes the crypto currencies more useful in general. Another case might be that the volatility of the system would drive out value as trust deteriorates. Yet another case might be that the value would centralize on one of the AltCoins, as it has on Bitcoin in the real ecosystem.

In summary: there's no simple answer to the question of "Who holds the power?" The Bitcoin Foundation was actually formed to give them a unified voice, i.e., to talk to governments.

However, there's been plenty of controversy. A lot of more Libertarian Bitcoin users hate the idea of a central authority, and the members of the foundation have been accused of conflict-of-interest on multiple occasions as they have stakes in certain Bitcoin companies.

Roots of Bitcoin

The precursors to Bitcoin include:

- The Cypherpunk movement: Proposes using cryptography as the background for instigating social and political change.
- Chaumian e-cash.

Satoshi was the author of the white paper and the original Bitcoin software. "Satoshi" is almost surely a pseudonym: they could be a man, a woman, or even a group of people. The identity is associated with a number of public keys which themselves own tons of Bitcoin from early mining. He/she has barely been heard from since 2010, and their coins have barely been touched (one theory: as soon as Satoshi touches these coins, the system will tank as those will be terrified that Satoshi has come to cash out–hence, Satoshi is waiting until the system is stable enough to withstand that kind of shock).

In Satoshi's original writings, some of these roots are made clear (or at least implied).

Government Involvement

Why would governments want to regulate Bitcoin?

- Typically, they have capital controls on their currencies, e.g., taxing money that comes in and out or pegging the exchange rate. This is helpful for various reasons (that we won't go into). **Bitcoin presents a threat to this model**: for example, you could convert your dollars into Bitcoin, cross the border, and convert your Bitcoin into the new currency you need.
- Untraceable cash also tactilities crime, e.g., tax evasion, extortion, the sale of illegal items, and so forth. There are a huge number of criminals that are eventually caught through some sort of money-based paper trail–Bitcoin could render this type of analysis useless.

The Silk Road was the largest online market for illegal drugs that ran as a Tor hidden service (both the server and client connect at rendezvous points in the Tor network). Payments were made in Bitcoin, with the site holding BTC in escrow while goods shipped.

Anti Money-Laundering

The goal of anti money-laundering (AML) is to stop large amounts of money from crossing borders or moving from the underground to the legitimate economy.

In the US, there's some mandatory reporting (by companies):

- You must report currency transactions over $10,000.

- You must watch for clients "structuring" transactions to avoid reporting (known as "suspicious activity").

Bitcoin businesses have been shut down after failing to follow these policies. As a result, businesspeople (e.g., Charlie Shrem of BitInstant) were arrested. The government takes this stuff very seriously.

Regulation

The argument *against* regulation is common and well understood.

The argument *for* regulation is not as well understood. To understand it, we should first define market failure: *a market is said to be failing when there's a different allocation of resources in which everyone is either better off or in the same place that they were before.* When markets fail and produce bad outcomes, regulation can address the failure.

Example: Lemons

The market for used cars can be high-quality or low-quality. But buyers have trouble discovering high- from low-quality used cars. Say that cars can be valued anywhere from $5,000 to $10,000 at a uniform distribution. If you're risk neutral, you'll pay $7,500.

Sellers, on the other hand, have perfect information about the quality of their cars. Thus, they will only bring a car to market if it's worth less than $7,500. But buyers will, in turn, recognize this and then only pay less than $7,500.

In an iterative process, value is driven out. We could solve this problem with regulation, e.g., requiring some sort of inspection before putting a used car on the market.

BitLicense

The BitLicense proposal comes from the New York State Department of Financial Services (NYDFS). New York is an important market for a lot of businesses, so they have some authority over the Bitcoin companies operating there.

BitLicense is built on the idea of Virtual Currency Business Activity, defined as anyone conducting any of the following and involving New York or a New York Resident:

- Receiving Virtual Currency for transmission.
- Securing, storing, or holding Virtual Currency (i.e., wallets, mixers).
- Buying or selling Virtual Currency as a customer business (i.e., exchanges).
- Performing retail conversion services (i.e., exchanges).
- Controlling, administering, or issuing a Virtual Currency (i.e., the Bitcoin Foundation– but does it include miners? The intent of this is *not* to include those categories).

The reason that these entities are included is that they need to attain a license and retain records of identity on their customers (hence, these regulations are most concerned with targeting mixing services). Categories that are not included here: developers, miners, and maybe even *merchants* (by many reasonable interpretations). That's kind of huge.

There's a lot of uncertainty around how these would play out in practice. In the end, some things will be open to interpretation and enforcement will come down to courts and prosecutors.

Professor Felten predicts that some sort of BitLicense will be put in place eventually. It won't kill Bitcoin anonymity completely, but it will have some effect–it could even improve consumer confidence now that there are clearer and existent rules around use of Bitcoin.