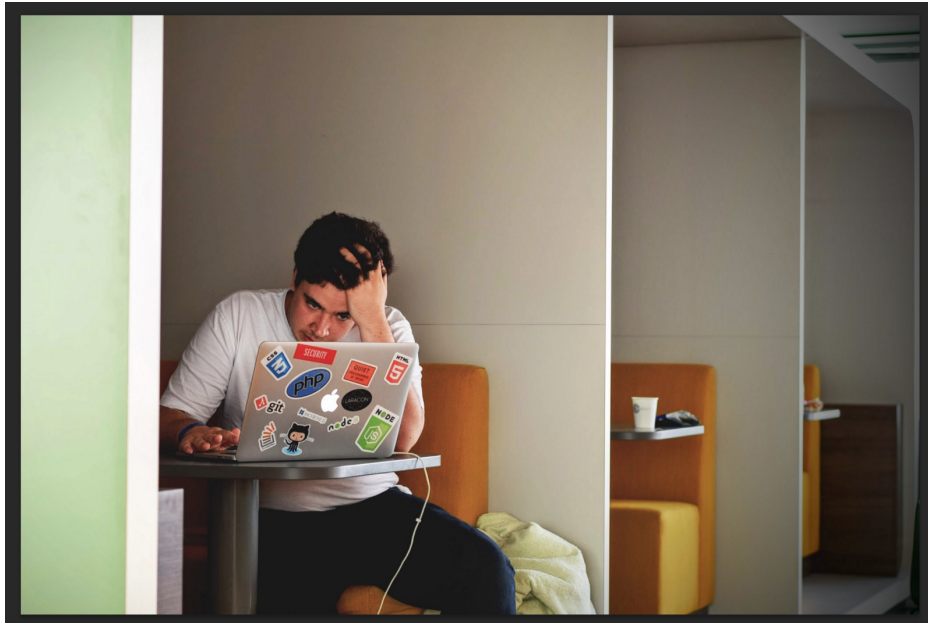




Aleksandr Bulkin [Follow](#)

Software engineer with interests in social innovation, psychology, philosophy, ethics and spirituality. Co-founder @ coinfund.io and Consensus Labs, Inc.

Jan 12, 2017 · 8 min read



Cryptoeconomics Is Hard

Economics is hard in general. The reason is that economics studies interactions in a very large group of people and people are not something you can model mathematically very well. But traditional economics works because it studies behaviors in a long-established system which changes very slowly. The way mainstream economic structures work is a product of years of research, governance, and social dynamics. In some sense you can say it was designed but a better way to look at it is that it was partly designed, partly discovered, and partly evolved on its own.

So cryptoeconomics is harder, precisely because the economics of every single cryptoasset is designed from inception. This includes supply, inflation, rewards, fines, and so on. Essentially, cryptoeconomics of a token is a hybrid between rules programmatically implemented on a blockchain and the entire world of interactions real human beings have

with it. Designing good rules necessarily entails understanding the way humans will interact with them.

We are not used to designing economic structures. This is a wholly new territory. This article is an attempt to illustrate some very subtle problems people encounter on this road, often well after fixing them stops being easy or even possible.

Bitcoin

Bitcoin confused people. It made some believe that a functional cryptocurrency will be valuable just by virtue of being out there. A number of copycat currencies came out quickly after this sentiment arose, and some even claimed to have better properties than Bitcoin. Some really may have been superior. None ever came close to the value of bitcoin for a long time, until Zcash (for about a day). Many died shortly thereafter. What happened?

Let me introduce an analogy here, one that can help illustrate that this is *purely* a social dynamics and partially explains why Bitcoin is still the largest market cap cryptocurrency in existence.

Imagine a world where people like hanging out in large groups and only governments have technology to build houses with large public spaces. In such a world everyone naturally goes to large government-built houses. But there is a problem: governments do nasty things occasionally. They sometimes evict people for no reason at all, or make people jump through hoops to enter their spaces.

Lo and behold, someone invents a revolutionary way to build a large public space very easily and they proceed to construct one. The house is empty at first. Some people look at it and say, “Why would I go spend time in your house—it’s empty!” Meanwhile, others say, “You built a large house where government is not in control? Cool! I want to come in and look around just for novelty of it.” There is another group who says, “A house with no government control? I’m coming and I am going to sit there alone for a while, but I am certain that others will see a value proposition in that and will come eventually. Everyone will be in your house soon enough, I can wait!”

Eventually a few people come, then a few more. Now this novel house is suddenly a place where a small group is hanging out and some people from the first group see that and say, “Oh, your house is no longer empty? I might come in for a while.” Some people tell their friends to come spend time with them in the new house. There are newspaper articles, publicity. More and more people come. In this world where people love to spend time together there suddenly is an alternative to government-run public spaces.

At some point, others learn about this technology (it is, after all, open source) and build similar houses. But the dynamic there is completely different. Their houses barely ever get visitors, because they are no longer novel, so they stay empty or underpopulated. The publicity of being *the first* is not there. Nobody ever hears in the mainstream news about Litecoin.

That’s the aura and the mystique around Bitcoin and it has a real good reason for it. People want to hang out where others hang out. Why would people go to another house which is empty?

Cryptoasset Value

Principle 1. *The value of a cryptoasset is determined by an expectation of what participants can do with it.*

If you can exchange a bitcoin for something valuable (a dollar) then the bitcoin has the same value as its dollar price. If you can exchange Filecoin for a decentralized storage service, its value is the value of that storage service.

It is slightly more complicated when you realize that an “expectation” can apply to some future time and so can be *speculative*. Speculative expectations is what gave Bitcoin its value from the start and they still play a major role in determining how much people are willing to pay for it.

Make no mistake. If you offer something in exchange for your cryptoasset, then you have to ask yourself why that is useful to users. If you expect someone else to offer something in exchange for your

cryptoasset, then you have to ask yourself why they would do that. Unless you, personally, ensure that your asset is useful, chances are it won't be. You simply cannot count on Bitcoin as a good model.

And so we get to Principle 2.

Principle 2. *If you issue or pre-mine your own cryptoasset, you have just created something that has zero value.*

There is no way around this whatsoever. If this is not obvious, let's simply notice that if issuing your own asset is easy, then anyone can do it, so why would anyone buy or need yours?

Principle 2 is an operating principle until Principle 1 (expectation) kicks in successfully. So, if you have issued an asset then nobody will want it until there is a reason for them to want it. As a designer of a cryptoeconomic system, you must understand that Principle 1 is the only way to move past Principle 2.

Principle 3. *Value is relative. The only meaning of the price of a cryptoasset is to compare its value with that of the asset in which it is being priced. Absolute value does not exist.*

Principle 3 comes into play when you think about such things as stablecoins. This is where it is easiest to lose track and implicitly decide that value is absolute. After all, wouldn't it be nice if you could create a coin that has constant value?

Unfortunately, the answer is that there is no such thing. Controlling the value of a coin is not done through some magical programming. You can only control the value of a coin (Principle 1) if you can control how much people want it. You can only have stable value if you express that value in *another coin* (Principle 3) and (again, Principle 1) offer that other coin or its equivalent in exchange for your stablecoin. Otherwise you have something that has zero value (Principle 2).

This is, in fact, what both Digix and Maker are doing. Digix physically guarantees that you can redeem its gold token for physical gold, so Digix is stable *against gold*. Maker takes a slightly different approach and

allows participants to put up a significant USD-denominated collateral to guarantee that DAI can be exchanged for something that has a given value expressed in USD. (In reality it's SDR, but that's close enough to USD that the distinction is not important here)

So, **Corollary 1.** *A coin A can be made stable against coin B only if there is a known and reliable mechanism that allows one to exchange A for B at a fixed price at least in the quantity of A's entire outstanding market capitalization.*

Such mechanism requires a collateral in the form of coin B. To guarantee the exchange, total collateral of B must be equal to a total B-denominated value of A's market cap. B-denominated here simply means "expressed as B at stable-price".

To be clear here, unless your system physically offers the guarantee of exchange of B for A or some clear incentive for others to offer such an exchange, then A will not be stable against B.

And, additionally, there is an obvious Corollary 2.

Corollary 2. *If coin A is stable against coin B and coin B loses value against coin C, then coin A loses value against coin C.*

This is what complicates the life of Maker but not of Digix. Digix stabilizes their coin against gold and takes collateral in gold. But Maker takes collateral in the form of blockchain assets but promises to stabilize DAI against USD. DAI is stable against the collateral put up, but if ever blockchain collateral loses value in some correlated catastrophic fashion then DAI can not be kept stable. (To be fair, Maker is going to also offer a way to put up non-blockchain collateral. When this happens, it will become less of an issue).

In conclusion

Designing a cryptoeconomic structure is like designing a robot that will be released into a large crowd of people with the goal of not only surviving, but also of herding the crowd to do something for it. The robot will be kicked, drenched in sulphuric acid, unplugged, and interacted

with in a wide variety of unexpected ways. But what the robot needs is to be given electricity, repair, and other resources. Also it will need people to give it directions and information.

The Bitcoin example is a really bad model for others. It induces the perception that all you need to do is create a currency and people will do the rest. The uniqueness and original novelty of Bitcoin is not to be underestimated as the reason for its success. It is not to be matched by copycats.

However, if one designs an economic system with a real value proposition one might expect a significant amount of both buy-in and momentum. With the right approach a startup business can self-fund, perform cheap and effective user acquisition and meet a number of other goals in novel, creative, and effective ways.

But your economic design must account for both early stages (Principle 2) and late stages (Principle 1) of your token's lifetime. You must ensure that people don't game the system in a way that leaks its value. You must ensure that it doesn't start growing too fast, but also that people don't get frustrated or disincentivized from using it. Economic value is a social phenomenon so traditional programming skills are not enough. In essence, you are trying to program a crowd. That is the hard part.

. . .

Alex Bulkin is co-founder at CoinFund, a blockchain technology research firm and proprietary cryptoasset investment vehicle. CoinFund's team brings together expertise in high technology, quantitative finance, private equity research, and social innovation research to generate insights into this exciting growth space. CoinFund provides consulting and research services to investors and companies interested in blockchain technology. Follow us on Twitter or join the discussion on our open community Slack.

