A Third Endgame For Bitcoin
or, Creating a Truly Free Coin

Owen Gunden
ogunden@phauna.org

September 19, 2011

Abstract

A commonly held belief is that bitcoin[1] exchange values will either go down to nearly zero, as interest in the currency wanes, or will explode upwards by many orders of magnitude as the currency becomes a major player in the economy. This paper outlines a third endgame, whereby a bitcoin-like cryptocurrency becomes a major player in the economy, yet the exchange value remains relatively stable. I argue that bitcoin will not acheive widespread adoption without one key change, and that those who understand the potential of bitcoin as a force for good have a moral imperative to make this change. I further argue that competitive market forces will either promote a successor to bitcoin, or force bitcoin to evolve, driven by the key feature of value stability.

1 Introduction

> "There are only two endgames for Bitcoin: either it fails for some reason, in which case it will be worthless, or it fulfills its promise and becomes an anonymous widely-used exchange currency, in which case, today's values are magnitudes below the endgame." – falkvinge.net, May 2011 [2]

> "I hope in 5 years, Bitcoin is really boring." – Gavin Andresen, lead developer for core bitcoin [3]

How do we reconcile these two visions for Bitcoin? Is it possible for Bitcoin to enjoy widespread adoption and still wind up being a boring old technology?

At present, something is amiss in the bitcoin economy. For a currency that's really going to be the future of digital money, a currency that has a limited supply of merely 18 million coins, to see a stagnant exchange rate around $5 per coin does not make sense. The market is telling us something is amiss.

2 Free-market competition

I'm as much a fan of earning lots of money for free as anyone else. Yet, I'm exhibiting my own uncertainty before pouring my life savings into bitcoins. The reason I'm uncertain is perhaps shared by many, but not often stated.

Quite simply, I hesitate because I keep hearing about these things called "Solidcoins" and "Ixcoins" and "I0coins" and I'm thinking.. exactly why is bitcoin better than these? Do I have a better chance at making a quick buck by getting in on one of these others while it's still cheap?

I'm not alone. Just a couple of weeks ago, a question[6] was posted to Stack Exchange saying: "Is there an easy way to diversify your Bitcoin holding among the other popular forks?" This sounds like somebody looking for an ETF, or mutual fund. And for good reason. With limited supply, all of the current cryptocurrencies look much like many other commodity investments (such as gold), so we might consider that we have to run and grab some before it's all gone.

While there are some differences, all of the currencies are technically quite similar. It's only *economically* that bitcoin stands apart.

Let's examine what sets bitcoin apart from the others economically:

1. It has a liquid exchange. Mt. Gox deals directly between dollars and bitcoins, and facilitates the exchange of over 1 million coin per month[4]. The other currencies' exchanges are tiny in comparison, and most of them are not trading for dollars directly, but only for bitcoins.
2. Bitcoin has far and away the most users, including web merchants and a few brick-and-mortar merchants, and the most well-known name.
3. Bitcoin has the longest and best reputation of legitimacy, due in part to having a core group of trusted developers.

All of these could be acheived by a competing crypto-currency. #1 is easy. We've seen enormous numbers of exchanges pop up to trade bitcoins, and there's no reason they could not start trading other crypto-currencies. In fact, at btc-e.com you can already trade solidcoin directly for USD. Getting more liquidity is not a technical problem, it's merely a matter of a bunch of people deciding to trade one of the other currencies instead of bitcoin.

Which brings us to #2. Could another currency start being accepted for payment of services on the web, threatening bitcoin's network-effect monopoly? Why not? One of bitcoin's greatest strengths is it's relative ease of use and zero startup cost. Anyone can fire up the software, get an address, and post it on their website saying "pay here". This translates directly to the competitor currencies.

#3 is similarly not unchallengable. For example, a well-known and trusted company could espouse a competitor to bitcoin.

Fundamentally then, the only thing that really sets bitcoin apart is the network effect, and while that is a powerful effect, it has been overcome many times before. So yes indeed, bitcoin is vulnerable to free-market competition from other currency systems.

But why bother to jump ship from one perfectly good cryptocurrency to some less-established upstart competitor? Nobody would do this lightly, because bitcoin's prominence offers so many advantages. One would need a good reason.

3 What's wrong with bitcoin?

We begin with what's *not* wrong with bitcoin, at least not wrong enough:

> Solidcoin transactions happen faster and more reliably than Bitcoin [...] Bitcoin is vulnerable to a drop off in mining power [...] we have learnt from the mistakes of Bitcoin [...]
> – from the Solidcoin website, September 19, 2011

Competing crypto currencies have shiny websites, with bunches of reasons for switching to their currencies. Some of them may be pretty good reasons, but none has proven good enough to overcome the network effect and unseat bitcoin. Yet.

There is one reason that is good enough, yet no competing currency has implemented it. In fact, all the competing cryptocurrencies have the same basic problem as bitcoin.

In an interview dated August 30, 2011, Bruce Wagner pointed to three major factors holding back widespread adoption of bitcoin:

> "I've been saying that the three major hurdles for Bitcoin are security, liquidity, and currency risk, and all three problems will be solved in three months, maximum. Once these hurdles are dealt with, Bitcoin will roll out as fast as Facebook has." [5]

Security is a technical problem and will be resolved over time with improved software. Liquidity and currency risk are both intrinsically tied to adoption of the currency by commerce. With increased adoption, liquidity will become deeper. And mitigating currency risk is a necessary precursor to increased adoption.

The problem with bitcoin is hard for many enthusiasts to see, because it's the reason they got interested in bitcoin in the first place.

The problem is that you can get rich just by buying it.

4 Two Words: Value Stability

It's a documented economic fact that wild swings in the value of currency is bad for an economy. It's also common sense. If you're a store owner, how can you accurately price your goods if the currency might halve or double in value overnight?

No matter the value of a bitcoin, there will never be more than 21 million. What this means in the case of a highly successful bitcoin scenario has been touted many times over on the internet: a nearly-unfathomable, orders-of-magnitude rise in the value of each coin. And therein lies the problem. If it's possible for there to be so much upside to bitcoin's value, then there's always the possibility of major valuation changes in the future, be they upwards or otherwise. The very possibility of such an event means value stability is nearly nonexistent, which means people won't trust the currency to hold its value. In other words, **if the potential exists to get rich off bitcoin, bitcoin can by definition never achieve value stability**.

True, many fiat currencies of today have the opposite problem; namely, they are subject to enormous inflation risk. It turns out that, while it's important for the value of currency not to go way down fast, it's equally important that it not go way up fast. Before you protest, consider again the merchant who is pricing his goods in bitcoin. If the value of bitcoins moves up even just 10%, he has to reprice his goods down to match. The energy he spends doing this is wasted, and if it threatens to happen often enough it will discourage him from accepting the currency.

> "For the three major problems that still exist, that I mentioned earlier, the solutions will be here in three months, tops. Once they're in people's hands, they'll spread like crazy, and the price [of Bitcoins] will go way up and interest will be hot like before." [5] – Bruce Wagner

The trouble with this theory is, if the price of bitcoins will go way up, then currency risk is high, negating Bruce's insistence that the "third hurdle" will be easily overcome. The point here is not to pick on Bruce or anyone else involved in promoting bitcoin—it is simply to point out that bitcoin's value-upside is exactly what's holding it back from widespread adoption. This is a catch-22. There's simply no way to have value stability and still have the exchange rate "go way up."

Of course, you can still get rich by starting a company to process merchant transactions, exchanging currencies, or some other ingenious idea that fills a real market need. But you can't get rich by speculating on it. It's just not going to get widespread adoption until the speculation risk goes away.

This may be a splash of cold water for many, but there is a silver lining. Since cryptocurrency is software-based, we can change the way it works (or introduce new, competing currency). Counterintuitively, a cryptocurrency could emerge as a winner from all this by volunteering to be the biggest "loser" of the bunch, namely, by giving up on wild price appreciation, and instead focusing on achieving value stability.

5 What is value stability?

First of all, what is meant by value stability? I use the term "value" stability, so as not to be confused with "price" stability. I will define a currency with value stability as:

> A currency who's value is not subject to extreme changes in short time intervals.

And what is the "value" of a currency? This is broad and market-based, and includes the exchange value versus other currencies, as well as how merchants and consumers view the value relative to goods.

Let us consider a cryptocurrency, similar to bitcoin in many respects but with the key difference that it has been designed with value stability in mind. In reality, this could wind up being a modified bitcoin, or one of the other competitors, or a new coin. For lack of a clear answer to what form said currency would be in the real world, let's say it's a coin called "FreeCoin".

In the early stages, when conventional currencies are viewed as more stable in value, value stability translates to stable exchange values. That's because today, conventional currencies are a widely accepted measure of value. It is only after people begin to trust FreeCoin as a primary currency that the possibility of significant exchange valuation changes would occur, and at this point, such a change would be viewed more as the value of e.g. the dollar going down rather than the value of FreeCoin going up.

6 How to acheive value stability?

There are a number of technical ways to acheive value stability. The key ingredient in the successful currency will be only this:

> The currency has been designed with value stability as a primary goal.

There are many great technical minds out there that can no doubt come up with many clever solutions. I will present my initial thinking on the matter, and expect it to be corrected and improved upon significantly.

We need a coin that is resilient to value swings. In the current bitcoin design, when a large buyer makes an exchange for dollars, the price jumps, and there's no reason or indication that the price will go back down. In fact, since bitcoin is by design deflationary, the coin would, if it became widely accepted, go wildly up in value. This fact creates a speculative feedback loop, in which there's always enormous speculative incentive to buy the currency.

In order to give our coin resiliency to value swings, we need the following two characteristics:

1. Whenever the value of the coin moves up, there is extra downward pricing pressure.
2. Whenever the value of the coin moves down, there is extra upward pricing pressure.

We already have the solution for #1: mining. We need only modify the current mining parameters so that, instead of aiming for a stable growth in the quantity of coin, we aim for a stable coin value. This implies freeing up the quantity of coin.

It would work as follows. The amount of coin possible in the system is unbounded (or, if for technical reasons it needs to be bounded, then it is bounded at an enormously high figure). We implement a fixed difficulty for mining new coins. Then, whenever the value of the currency goes up, mining will become increasingly profitable with no limit to the increase in profitability. Therefore more miners will join the fray, more coins will be generated, and finally the value will be pushed back down to the point where mining reaches equilibrium profitability. To see how this differs from the current system, one need only consider what happens to mining profitability with the current floating difficulty when the value of coins go up: it does not increase.

For #2, I suggest that the natural attrition rate (lost wallets, crashed hard drives, etc.), together with growth in interest and usage of the currency would be sufficient to keep values up.

Therefore, the key change from the current bitcoin design is to (1) allow unlimited coins to be mined, and (2) fix the difficulty so that increased values create a market for increased mining.

7 Bootstrapping

The astute reader will note that the designers of our new or modified coin will have to decide on an initial difficulty value for mining coins. This is effectively deciding on the initial maximum value of a coin. The more difficult it is to generate each coin, the higher the maximum value. Estimation of valuation is likely to be off the mark so there's not

much point in spending a lot of effort on it, except if we are modifying bitcoin to be value-stable; in this case it may be advisable to target current exchange rates as the initial value of the new coin and to freeze exchange rates during the transition. The designers can use experience gathered on bitcoin mining difficulty thus far to guide the initial difficulty value decision.

There will not be a speculative ”gold rush” for this coin, as any such rush would quickly be balanced out by miners selling more coin. Since the coin will be slightly inflationary, the incentive to hoard will go away. Early adopters who start with a bunch of coins have little incentive to hang onto them, because the value of the coin will in all likelihood remain flat or even decrease slightly over time.

Any number of design decisions could be made on a new coin, such as doing away with fractional coins altogether and instead adopting a lower value and using integral coin amounts, such as with the japanese yen. Such decisions are beyond the scope of this paper.

8 A Moral Imperative

> Hoarders can get piles of money,
> That is true, hackers, that is true.
> But they cannot help their neighbors;
> That’s not good, hackers, that’s not good.
>
> - Richard Stallman, The Free Software Song

The promise of bitcoin is a great gift to freedom on Earth. We are standing on the verge of a revolution.

Yet, bitcoin is plagued with defamation from all over. Do a search for “bitcoin ponzi” (without quotes) and you get over 350,000 results.

The very fact that we have bitcoin millionaires that did not do anything to earn their millions other than being in the right place at the right time lends an air of disrepute to the project.

If we want bitcoin to survive and be accepted by the world writ large, we must withdraw from our ideas of personal gain. We can create a coin that is invincible to disrepute. We’re almost there already. We just have to take that one last step.

We must change this from a system that has room for greed into the system that can transform finance and economies worldwide. It is a moral imperative that we take this step. If we do not, bitcoin will in all likelihood fail to achieve it’s true world-changing potential.

9 Remarks and Conclusions

The design of a Free Coin outlined here need only be slightly different from the current bitcoin design. The key difference is that there is no promise of getting rich off the money supply. Whoever looks at the early adopters of the current cryptocurrencies wants to join in and get rich too, like the early adopters. This creates an incentive to jump ship to a competing (and cheaper) currency, where you can still get in early. Until one of the currencies “gets it” and implements value-stability, this ship-jumping risk will remain. The fixed-point solution to this recursive process is value stability which can only be achieved through a flexible money supply.

The good news is that we are on the verge af a monetary system that cannot be centrally controlled, and cannot be abused to the benefit of *any* few at the expense of the masses. The promise of cryptocurrencies, which is about to be realized, is precisely that nobody can get rich solely off the currency.

So let’s stop trying to do just that, and get on with the good fight :).

10 Frequently Asked Questions

- Does this mean I want to dump my bitcoin/solidcoin/ixcoin/etc holdings and run?

  Not necessarily. It will take time for the market to fully realize the importance of value stability, and in the meantime there will be many ups and downs of the various cryptocurrencies. However, if you understand the arguments put forth in this paper, you will see that you are unlikely to become super-rich simply by buying and holding bitcoin.

- You're a bitcoin hater! You want it to fail!

  On the contrary. I think we are on the verge of one of the greatest revolutions in money and economics of all time. I do, however, not want the value of bitcoins to go way way up. That's because I want it to succeed. Many people are confused about bitcoin because they equate success of the currency with radically high exchange rates, and this is fiction.

  We have to be honest with ourselves and recognize that any currency that has the potential to make us rich, also by definition is unstable. The way to truly enrich us all is to give us a truly free and stable digital monetary system.

- FreeCoin sounds inflationary. I thought a fixed money supply was better than an inflationary one. Are you a Keynesian?

  Heavens no, I'm more of an Austrian. It's true that FreeCoin may well be slightly inflationary, because of the increase in mining power per value of energy spent over time. However if the cost of energy increases, this effect could well be mitigated. Only time will tell.

  The importance of sound money is that the monetary system is left up to markets, and that it is not abused by any one person or group in favor of another. In the physical world, we must have gold, silver, or other hard assets to truly acheive these ideals, and the resulting deflation is perhaps a nuisance, but certainly better than the alternative. In the cryptocurrency world, however, the rules are a little different: We can achieve a truly free-market system that is also value-stable.

- If the difficulty of mining is fixed, why wouldn't miners just keep mining and making more and more coins, devaluing the currency until it's worth nothing?

  Mining is not free. It has costs in terms of equipment, and importantly, electricity. When the value of coin gets on par with the cost of electricity, miners will be faced with the choice between stopping their mining operation or losing money. They will therefore stop mining until the value of coins increases.

- Won't this create an incentive to create really cheap sources of energy?

  Perhaps. Not such a bad thing, eh?

- Don't we already have a market-based value? Why do we need to change?

  Yes, we do already have a market-based value. The reason we need to change is that we need a more stable market-based value. For that, we need to unfix the money supply and remove the incentive to speculate.

- You just want to create a new cryptocurrency and get rich like the other guys.

  I don't care if another currency is created or not, or if bitcoin is modified. The currency I'm proposing is get-rich-proof. That's the whole idea.

  I will admit to a small bit of egotism here: I am somewhat partial to the name FreeCoin. However, I want most of all to see this technology flourish and reach its true world-changing potential; whatever the name.

References

[1] Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System 2009

[2] Rick Falkvinge Why I'm Putting All My Savings Into Bitcoin May 29, 2011

[3] Adrianne Jeffries Bitcoin Enthusiasts Gather in NYC to Meet IRL and Show Off Bitcoin Start-Ups August 28, 2011

[4] Bitcoin Charts Mt. Gox Exchange Statistics Accessed September 19, 2011

[5] Bitcoin Trader Interview with Bruce Wagner, Part 2 August 30, 2011

[6] Stack Exchange Bitcoin Stack Exchange question Accessed September 19, 2011