Everything here is my personal opinion. I do not speak for my employer.

Back: April 2011 Next: June 2011

2011-05-08 »

Why bitcoin will fail

> *Reading about bitcoin. Thought about writing a blog rant, but "OMG they're all totally crazy" wasn't long enough, so here we are. Filler.*
>
> -- Me on twitter

> *I now have had my foggy crystal ball for quite a long time. Its predictions are invariably gloomy and usually correct, but I am quite used to that and they won't keep me from giving you a few suggestions, even if it is merely an exercise in futility whose only effect is to make you feel guilty.*
>
> -- E.W. Dijkstra

I'm in the "commerce" group at work, and I've done quite a bit of work in the world of banking, so it seemed vaguely relevant when I ran into the technical paper about bitcoin (Google it) and its associated various web sites. This led to my above, admittedly rather smarmy, twitter post...

...and then someone, yes, inevitably, asked me for clarification.

See, a bitcoin rant is almost too over-the-top for me. Asking why I think bitcoin won't work is like asking why the sky isn't red. I mean, wait, you think it *is* red? You actually took that seriously? Oh boy. Where do I even start?

But just for you, because I know all the valued subscribers to this diary have been deprived of my ranting lately, I will expand on it a little.

Just one more side note. Most of the time, I try to give projects the benefit of

the doubt. If they don't affect me, then it's really no matter to me if they succeed or fail. I might keep an eye on them to see if my prediction (usually failure) comes true or not, and try to learn from the result. But I don't actively *want* projects to fail. I would much rather they succeed.

In this case as well, I don't really care. I don't own any bitcoins. I don't particularly want to. If one day I have to own some for some reason, I will buy them at the market rate and get screwed, just as I do today with U.S. and Canadian dollars.

Since I don't actually care, I had a bit of trouble motivating myself to write more than 140 characters about it. I wasn't going to bother. So, um, thanks to my followers on twitter for providing the motivation.

So here we go:

FAIL #1: If you like bitcoin, then you must think the gold standard was a good idea.

The gold standard, for those who don't know, was the (now thoroughly discredited) idea that for every dollar you print, you need to have an appropriate amount of gold stored away somewhere that someone, someday, theoretically, could demand to get back in exchange for your worthless piece of paper. If you honestly believe that abandoning the gold standard was a bad idea - and there are indeed people who believe this - then you might as well stop reading now. Wiser men than I have explained in excruciating detail why you're an idiot. This article will not convince you, it will just make you angry.

Still with me?

Okay, just for background, for people who don't already have a pre-formed opinion, the gold standard is a bad idea for several reasons. Here are some of them:

In order to create currency, you have to do a bunch of pointless busywork. Originally, that meant *mining* for gold, so you could take this gold (obtained at great expense) and hide it in a fortress where nobody would ever see or feel or admire it. In all of history, it is extremely doubtful that anybody has *ever* walked into a U.S. government office and demanded their gold in exchange for dollars. That's because:

Gold is a stupid inconvenient currency that's worse than paper. Go up

to the street vendor selling a hot dog, and try to get him to give you a hot dog in exchange for the equivalent value in gold dust. (That's really not very much dust.) See what happens. Gold is the universal currency, is it? The thing that anybody would and will take, any time, throughout history? No. It's heavy, messy, hard to measure, and I can't get my ATM to withdraw or deposit it. If I want 1000x as much gold as one gold nugget, I can't just get a $1000 bill; I have to get a gold nugget 1000x as big and heavy. Who wants this?

Believing in the gold standard is disbelieving in capitalism. The magic of capitalism is entirely contained in the following two words: MAKING MONEY. Have you ever thought about those two words? What's interesting about them is they don't seem to make any sense. When I go into the office and do work, am I literally "making" money? Why do they call it that? Well, as a matter of fact, you *are* literally making money. You are a machine: you eat food and breathe air and magically, you produce outputs that can be sold for much more money than the cost of the food and air. You produced actual value, and that value can be measured, and that measurement is called money. You made money. Out of nothing. *That* is capitalism. (Compare with digging up useless coloured rocks and then hiding them in a fortress so nobody can see them. Those people make the economy go round?)

If the gold standard worked, the 1930s depression wouldn't have happened, and we couldn't have recovered, period, from the recent banking crisis.

Back in the 1930s, the U.S. still had gold-backed currency. Why was there a depression? Because people stopped producing valuable stuff. The amount of money was constant; the gold didn't disappear. But somehow, suddenly people didn't have enough food or housing. Why? Because they refused to produce unless they got paid for it. When they didn't get paid, they couldn't spend that money, and so they couldn't pay for other things, and so other people refused to produce since they wouldn't get paid either, and so on in a giant cycle. The money was there, but it stopped moving.

How did the depression get resolved? In short, people started doing stuff (especially a big war) whether they could afford it or not. It turned out that all those idle people could be productive if they had a good reason. Gold turned out not to be a good enough reason.

Relatedly, the U.S. survived the 2008 banking crisis - which had a legitimate opportunity to convert itself into another depression - by spending its way

out. As it happens, the U.S. was able to spend money it didn't actually have. Why? Because they don't care about the gold standard. If they had had a constant amount of gold, then they would not have been able to spend more than they had, and so people wouldn't have been paid, and those people would have refused to produce, and they wouldn't be able to buy things, so more people would refuse to produce... and we're back to square one.

Motivation is everything. Gold is nothing.

Which leads us to the last, most important reason to abandon the gold standard:

The ability of governments to print (and destroy) money is a key tool in economic management.

The Federal Reserve (and other related institutions in each country, like the Bank of Canada) has the right to print money. It largely does this through a pretty blunt mechanism, the interest rate. I won't go into a lot of detail - look up "federal funds rate" if you want to learn more. But in short, when they lower the rate, banks are willing to "borrow more money" from the federal reserve (which they then lend to you, and so on). When the federal funds rate is high, banks need to give back this money, so they don't give out as many loans, and so on.

What is this money that the federal reserve "lends" to banks? It's fictional. Bits in a computer database. No fancy encryption. They just manufacture it on the spot, as needed. And when it's returned, they make it disappear.

> **Update 2011/05/08:** Some gold standard supporters will tell you that in fact, this ability to print money is what causes hyperinflation, which causes economic collapse. But no, the causality doesn't work like that. Hyperinflation occurs when government nutbars try to stop an economic collapse by wildly printing money. No economic system can protect you when nutbars are in charge. But yes, the early symptoms of failure will look somewhat different.

The Federal Reserve uses this control to speed up or slow down the economy and try to reduce fluctuations. The results aren't always perfect (humans aren't very good at acting like math equations) but it's actually not too bad overall.

If governments can't control the money supply, then they can't set interest rates. If they can't set interest rates, they can't control the economy, and if

nobody is controlling the economy, then the economy will act like any uncontrolled complex system: it'll go crazy.

(Incidentally, this is also why it's important that the Federal Reserve not be controlled directly by politicians. Find me a politician who will say anything other than, "OH YEAH! MAKE THAT ECONOMY GO FASTER!" at election time.)

...

Okay, so, back to bitcoin. Bitcoin is exactly like the gold standard, only digital:

- "Mining" (they even borrowed the word!) bitcoins is pointless busywork that produces nothing of real value.
- Bitcoins are less convenient than paper currency.
- Bitcoin denies the truth of capitalism, that it's about *value*, not about money, by preventing the money supply from expanding when the economy does.
- Bitcoin allows for random unrecoverable effects like the 1930s depression.
- Bitcoin removes government control over the economy, which means there is *no* control over the economy.

By comparison, look at our current currencies:

- Generating money is essentially free (most money isn't even paper, but printing the paper is pretty cheap too).
- Current currency is very convenient and has many convenient forms.
- When more valuable stuff is created, more money appears without having to mine for unrelated crap first.
- Current currency allowed us to spend out of a depression caused by the banking crisis.
- The current system allows the government to reduce economic fluctuations.

FAIL #2: Even if it was a good idea, governments would squash it.

In the previous section, it might have sounded like I think governments are altruistic peace-loving tea-drinking hippie commies.

I don't actually think that. (I think the government of British Columbia might be like that, which explains why they don't get any work done, but that's

another story.)

The truth is that governments are power structures. Governments control ("govern") things. And while the economy - like any complex engineering construction - needs to have controls on it, some of the controls end up going too far, and all of them end up being manipulated by people in power.

One of the lures of bitcoin is the idea of taking power away from the people in power. Admit it. That's one of the reasons why you like it.

Well, word to the wise: if there's one thing the people in power *already know*, it's that **money is power**. It's not like you're going to catch them by surprise here. They don't have to be the smartest cookies in the jar to figure that part out.

Digital money is *not* like pirating digital music and movies. The government sort of cares about those, but let's be serious: pirating a few movies will not topple the U.S. government. Losing control of money will.

Governments have *big weapons* and *propaganda machines* and *actual secret agents* and *citizens who believe that keeping the economy under control is a good idea*. If you threaten the currency, you are threatening the entire power structure of the civilized world. You are, quite literally, an enemy of the state. You are attempting to build nuclear weapons in your bedroom. Or at least they'll see it that way.

Do you think you'll get away with it because your monopoly money is made of bits instead of paper? I don't.

The only reason you'd get away with it is if you're too small to matter. Which is certainly the current situation.

FAIL #3: The whole technological basis is flawed.

Bitcoin is, fundamentally, a cryptosystem. Some people argue that it's "as strong as SHA256" and that "if someone could break SHA256, then banks would be in trouble as it is."

Wrong on both counts.

First of all, I admit, I don't totally understand the bitcoin algorithms and systems. I don't really need to. I understand only this: the road to crypto hell is paved with the bones of people who thought that a good cryptosystem can be designed by combining proven algorithms in unproven ways. SHA256

may be the strongest part of bitcoin, but a cryptosystem is only as strong as its weakest link.

You want to replace the world economy with a hard-to-guess math formula? Where's your peer review? Where are the hordes of cryptographers who have spent 30+ years trying to break your algorithm and failed? Come talk to me in 30 years. Meanwhile, it's safe to assume that bitcoin has serious flaws that will allow people to manufacture money, duplicate coins, or otherwise make fake transactions. In that way, it's just like real dollars.

But what's *not* like real dollars is the cost of failure. With real dollars, when people figure out how to make counterfeit bills, we find those people and throw them in jail, and eventually we replace our bills with newer-style ones that are more resistant to failure. And the counterfeiters are limited by how many fake bills their printing press can produce.

With bitcoin, **a single failure of the cryptosystem could result in an utter collapse of the entire financial network.** Unlimited inflation. Fake transactions. People not getting paid when they thought they were getting paid. And the perpetrators of the attack would make so much money, so fast, that they could apply their fraud at Internet Scale on Internet Time.

(Ha, and don't even talk to me about how your world-changing financial system would of course also be protected by anti-fraud laws so we could still punish people for faking it. If we still need the government, what is the point of your currency again?)

The current financial system is slow, and tedious, and old, and in many ways actually broken or flawed. But one thing we know is that it's *resilient*. One single mathematical error will not send the whole thing into a tailspin. With bitcoin, it will.

And no, a break in SHA256 would not break the current financial system or ruin any banks. How could it? What would even be the mechanism for such an attack? How would it make the paper bills in my pocket stop working for buying hot dogs? Can't we just hunt down and arrest the people who forged the fake transactions?

FAIL #4: It doesn't work offline.

Stupid, crappy, printed paper money is old fashioned and flawed, but you know what? It actually works offline, because the easily-forged piece of paper is *just barely hard enough to forge* that normal people won't try to

forge it. It's the original peer-to-peer financial network, although there's a "central coordinator" somewhere issuing tokens.

As soon as you go electronic, forgery becomes trivial to do on a massive scale, so offline just isn't an option. Yes, there are "offline" mechanical paper-based credit card readers, but they aren't anonymous: they have your name and card number. If you bounce too many transactions from one of those, someone will be sent to hunt you down. The risk is contained.

There is no way to make bitcoin even remotely safe offline. There is no fallback mechanism except exchanging your bitcoins for cash. But if you're going to rely on a paper currency anyway, what is bitcoin buying you? It's just yet another way to spend money. As a person currently suffering through managing U.S. versus Canadian dollars, I can tell you, exchange rates are just not worth the hassle.

...

Summary

1. Like the gold standard, a successful bitcoin would send our economy back into the dark ages.

2. Even if it became popular, governments would squash it because of #1 and because they like being in power.

3. A single mathematical or other error in the cryptosystem would cause instant, unresolvable, worldwide hyperinflation. After hundreds of years of analysis, there are no known flaws in the current financial system that could lead to that. (Other than the known causes of hyperinflation of course, ie. total gross mismanagement of the entire country.)

4. It's not even useful except as an online-only addition to normal currency, and my normal currency already works fine online.

The sky is JUST NOT RED, dammit.

Tell me again why you think it is?

...

Update 2011/05/08: Counterpoint!

An anonymous (really, they anonymized their return address) reader replies with the following. I'll just reprint it in full because it's awesome. There's

nothing quite like just letting an unelected representative of a movement embarrass himself. Oh Internet, how I love you.

> Was that for real? I'm not sure if your stupid or just trolling.
>
> The US dollar has lost 97% of it's value since leaving the gold standard.
>
> Germans in the Weimer republic had to buy their sausage with wheelbarrows full of paper currency. Too long ago for you? Mid-90's Yugoslavia, samething.
>
> "Believing in the gold standard is disbelieving in capitalism" and how do you think capitalism came about?
>
> "If the gold standard worked, the 1930s depression wouldn't have happened, and we couldn't have recovered, period, from the recent banking crisis."
>
> You really don't know history.
>
> "The ability of governments to print (and destroy) money is a key tool in economic management."
>
> REALLY? Then why did the Soviet Union fail? They should have been the richest country in the world if your statement was true.
>
> "What is this money that the federal reserve "lends" to banks? It's fictional. Bits in a computer database. No fancy encryption. They just manufacture it on the spot, as needed. And when it's returned, they make it disappear."
>
> Loaned with interest. How does the interest disappear when more money is owed then exists?
>
> I wouldn't be surprised if you said somewhere else that current debts are managable.
>
> "If governments can't control the money supply, then they can't set interest rates. If they can't set interest rates, they can't control the economy, and if nobody is controlling the economy, then the economy will act like any uncontrolled complex system: it'll go crazy."
>
> From, "disbelieving in capitalism"" to that? See also; Soviet Union.
>
> I don't use BitCoin (yet) but your reasoning there is even more pathetic.

> No reply because your the stupidest person I've seen this week and that's saying something.

For the record, I'm stupid *and* trolling. That's why it was hard to tell.

May 9, 2011 02:54

Back: April 2011 Next: June 2011

apenwarr-on-gmail.com