Is it real or is it

apenwarr

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

← *October 2021* *December 2021* →

2021-11-17 »

10 years of... whatever this has been

I guess I know something about train wrecks.

One night when I was 10 years old, me and my mom were driving home. We came to a train crossing outside of town. There was another car stopped right on the tracks, stalled. A lady was inside, trying to get her car to start. It didn't.

Train crossings are bumpy, cars were worse then, it was a long time ago, I don't know, I don't remember clearly. Anyway, it was cold out and most people didn't have cell phones yet, so when the car wouldn't start and it was too heavy to push, there wasn't much to be done. My mom convinced her to get the heck away from the tracks and come sit in our car to warm up and make a plan. We heard the whistle of an arriving train. And I made what I now consider one of the (several) biggest mistakes of my life: I closed my eyes.

It was only a few seconds later when I realized OH MY GOD WHAT WAS I THINKING I COULD HAVE WATCHED A TRAIN DESTROY A CAR RIGHT IN FRONT OF ME!!! But I wasn't brave enough, I panicked, I closed my eyes, and you know what? The train wreck happened anyway. I just didn't get to see it.

It was in the local newspaper a couple days later. The newspaper said the car ran into the train, and not the other way around. I was boggled. I learned later that this was my first, surprisingly on-the-nose, encounter with the

Gell-Mann Amnesia Effect. (To this day, I still believe some of the things I read. I have no idea why.)

What's the point of this story? That the train crash still happens, whether or not you're watching. And everything you've read about it is probably wrong. And I'm glad my mom helped that lady get out of the way.

Anyway that's why I don't mute blockchain-related keywords on twitter.

The blockchain train crash

Ten years(!) have passed since I wrote Why bitcoin will fail. And yet, here we are, still talking about bitcoin. Did it fail?

According to the many cryptobots who pester me, apparently not. They still gleefully repost my old article periodically, pointing out that *at the time, bitcoins were worth maybe three dollars, and now they're worth infinity dollars, and wow, that apenperson sure must feel dumb for not HODLING BIGTIME back when they had the chance, lol.*

Do I feel dumb? Well, hmm. It's complicated. Everything I predicted seems to have come true. If your definition of "failure" is "not achieving any of the stated goals," then I guess bitcoin has profoundly... not succeeded. But that doesn't really tell the whole story, does it? A proper failure would be in the past tense by now.

What I do know is I've learned some stuff in 10 years.

What I got right

But first, let's review the claims I made in the original article:

- **If you like bitcoin, you must think the gold standard was a good idea.**
  To create gold currency, you do pointless busywork ("mining"). Gold is a stupid inconvenient currency that's worse than paper.
  Printing and destroying money is a key economic tool.

Yup. Over the years we've seen an ongoing, embarrassing overlap between "goldbug" zealots and bitcoin zealots. The busywork mining has gotten absurdly more expensive than it was in 2011, and somehow is now a

significant fraction of worldwide energy usage (what. the. heck), and various blockchains' environmental impact is now the most common argument people use against them.

Beyond my imagination, bitcoin has achieved the unlikely goal of being even *less* convenient than gold for actually buying things (the job of a currency). The exchange rate of bitcoin is almost completely a random walk, impossible for anyone to manage (unlike a regular currency), and much worse than even gold.

- **Even if it was a good idea, governments would squash it.**
  The only reason they haven't is it's too small to matter.

Yes and yes.

Congratulations, we've now seen the bitcoin movement get big enough to matter! There's a corresponding increase in regulation, from SEC investigations, to outright banning in some countries, to the IRS wanting to tax you on it, to anti-terrorist financing and KYC rules. Each new regulation removes yet another supposed advantage of using something other than cash.

Also, it's now obvious that use of bitcoin (and related blockchains) for payments is almost entirely scams and illegal stuff. This agrees with my prediction, but in a way I didn't expect. It turns out to be maybe tautological. Like the old American saying, "If you outlaw guns, then only outlaws will have guns," you could argue that we have now regulated bitcoin so much that only criminals can productively use bitcoin.

But it's grown enough to now be producing the largest (and ongoing!) ransomware outbreak the world has ever seen, so, you win, I guess.

- **The whole technological basis is flawed.**
  The weak link is not SHA256, it's the rest of the cryptosystem.

Yes, in multitudes.

We've seen forked chains, theft, mysteriously reversed transactions, 51% attacks.

It turned out bitcoin is irreconcilably privacy-destroying. (Law enforcement teams say thanks!) This was originally billed as a feature until some drug dealers got caught. The feature, or maybe bug, can't be fixed without changing the system, which can't be done without getting everyone to upgrade.

But ha, it's a decentralized system. Since nobody could figure out how to get everyone to upgrade a decentralized system all at once, it was more profitable to instead spin up zillions of new blockchains, each with its own systemic flaws, but all sharing the one big systemic flaw: it's an ownerless distributed cryptosystem, so when each fatal flaw is inevitably revealed, nobody can fix it.

On top of the technical problems, there were social problems. Jo Freeman's Tyranny of Structurelessness showed up here, as it does whenever you try to pretend you have no social control hierarchy. We learned that the people who write the code, and the people who have the biggest mining rigs, and the people who operate exchanges, and the people who go on expensive and very shady cruises to hobnob with the cabal, and something about North Korea, and basically everyone who is *not you*, all have disproportionate control over what happens with this "decentralized" "currency." And this is equally true in all the other "decentralized" chains invented to either scam you or solve technical problems in the original, or both.

For heaven's sake, people, it's software. You built a system, or series of systems, that will fail in completely predictable ways, forever, if you didn't get the software perfectly right the first time. What did you think would happen.

- **It doesn't work offline.**
  Paper money does.

Still true. On the other hand, the global expansion of cellular data availability has been relentless and perhaps this never did matter.

What I got wrong

Okay, well. The title.

"Why bitcoin will fail" wasn't right. It would have been better to call it "Why bitcoin *should* fail," because it really should have! But it didn't, at least not yet, at least in the minds of its ever-growing user base. I feel like this is important.

A few years ago I learned the investor variant of Sturgeon's Law. Here's what a VC told me: 90% of new things will fail. Therefore you can just predict every new thing will fail, and 90% of the time you'll be right. That's a pretty good way to feel good about yourself, but it's not very useful. Anybody can do that. Instead, can you pick the 10% that will succeed?

Even though I accurately predicted a bunch of things about bitcoin that wouldn't work, I didn't predict *all the other things about bitcoin that wouldn't work.* Maybe that seems like splitting hairs, but it isn't. If you miss the reasons something won't work, then you might just as easily miss the reasons why it will work. It suggests that you don't know what you're talking about.

Here are some reasons I missed for why bitcoin (and blockchains generally) didn't and still don't work, for anything productive:

- **Scams.** Lots and lots of scams. Blockchains became the center of gravity of almost all scams on the Internet. I don't know what kind of achievement that is, exactly, but it's sure something.

- **Citizens moving money out of authoritarian regimes.** This is, by definition, illegal, but is it a net benefit to society? I don't know. Maybe sometimes.

- **Other kinds of organized crime and trafficking.** I don't know what fraction of money laundering nowadays goes through blockchains. Maybe it's still a small percentage. But it seems to be a growing percentage.

- **More and more blockchains.** There are so many of them now (see "scams", above), claiming to do all sorts of things. None of them do. But somehow even bitcoin is still alive, even though a whole ecosystem of derivative junk has sprouted trying to compete with it.

- **Corrupt or collapsed exchanges.** I predicted technical problems, but most of the failures we've seen have been simple, old fashioned grifters and incompetents. Indeed, the failures of this new financial system are just like the historical failures of old financial systems, albeit with faster iterations. Some people are excited about how much faster we can make more expensive mistakes now. I'm not so sure.

- **Gambling and speculation.** I wrote the whole article expecting bitcoin to fail at being a *currency*, but that charade ended almost immediately. What exists now is an expensive, power-hungry, distributed, online gambling system. The house still always wins, but it's not totally clear who the house is, which is how the house likes it. Gambling has always been fundamentally a drain on society (a "tax on the uneducated," someone once told me), but it's always very popular anyway. Bitcoin is casino chips. Casino chips aren't currency, but they don't "fail" either.

Despite all that - and I didn't even need to exaggerate! - bitcoin has still not failed, if failure means it's gone. It's very much still around.

That's because I forgot one essential reason bitcoin has survived:

Because people really, really, really want it to.

If there's one lesson I learned over and over in the last ten years, that's it. Projects don't survive merely because they are good ideas; many good ideas get cancelled or outcompeted. Ask anyone who works at an overfunded tech company.

Similarly, movements don't die just because they are, in every conceivable way, stupid. Projects live or die because of the energy people do or do not continue to put into them.

…

Here's a metaphor. Blockchains today are like… XML in the early 2000s. A long-burning overcomplicated trash fire that a bunch of large, cash-rich, unscrupulous, consultant-filled mega-organizations foisted on us for years and years, that we all now pretend we weren't dumb enough to fall for. Remember SOAP? Remember when we tried to make HTML4 into XHTML? Ew, no.

The thing is, a ton of major tech infrastructure spending was somehow justified in the name of XML. A lot of computer systems, especially in the financial and manufacturing industries, got a long-needed overhaul. Fixed-width COBOL databases couldn't do XML, so bam, gotta replace some fixed-width COBOL databases (or at least slap a new API translator in front). The XML part sucked and still sucks and we'll be dealing with it for decades.

But is that really so bad, in the name of progress?

Epilogue

It's been ten years, and it all went pretty badly, so let me make a new prediction.

A lot of stuff will get redesigned in the name of blockchains. Like XML, the blockchains will always make it worse, but if carefully managed, maybe not *too much* worse. Something good will eventually come out of it, by pure random chance, because of all those massive rewrites. Blockchains will take credit for it, like XML took credit for it. And then we'll finally move on to the next thing.

Nowadays if someone picks XML for a new design, we look at them like they're from another planet. So, too, it will be with decentralized consensus blockchains, someday.

So, too, it was for the gold standard for international trade.

But it took more than 50 years.

Related

XML, blockchains, and the strange shapes of progress (2018)

Why bitcoin will fail (2011)

Unrelated

SimSWE 4: Wants, needs, and chasm-crossing (2021)

← *October 2021* *December 2021* →

Try **Tailscale**: mesh networking, centralized administration, WireGuard.

Why would you follow me on twitter? Use RSS.

apenwarr-on-gmail.com