Unenumerated

An unending variety of topics

Saturday, May 28, 2011

Bitcoin, what took ye so long?

So asks gwern in a spectacular display of hindsight.

The short answer about why it took so long is that the bit gold/Bitcoin ideas were nowhere remotely close to being as obvious gwern suggests. They required a very substantial amount of unconventional thought, not just about the security technologies gwern lists (and I'm afraid the list misses one of the biggest ones, Byzantine-resilient peer-to-peer replication), but about how to choose and put together these protocols and why. Bitcoin is not a list of cryptographic features, it's a very complex system of interacting mathematics and protocols in pursuit of what was a very unpopular goal.

While the security technology is very far from trivial, the "why" was by far the biggest stumbling block -- nearly everybody who heard the general idea thought it was a very bad idea. Myself, Wei Dai, and Hal Finney were the only people I know of who liked the idea (or in Dai's case his related idea) enough to pursue it to any significant extent until Nakamoto (assuming Nakamoto is not really Finney or Dai). Only Finney (RPOW) and Nakamoto were motivated enough to actually implement such a scheme.

The "why" requires coming to an accurate understanding of the nature of two difficult and almost always misunderstood topics, namely trust and the nature of money. The overlap between cryptographic experts and libertarians who might sympathize with such a "gold bug" idea is already rather small, since most cryptographic experts earn their living in academia and share its political biases. Even among this uncommon intersection as stated very few people thought it was a good idea. Even gold bugs didn't care for it because we already have real gold rather than mere bits and we can pay online simply by issuing digital certificates based on real gold stored in real vaults, a la the formerly popular e-gold. On top of the plethora of these misguided reactions and criticisms, there remain many open questions and arguable points about these kinds of technologies and currencies, many of which can only be settled by actually fielding them and seeing how they work in practice, both in economic and security terms.

Here are some more specific reasons why the ideas behind Bitcoin were very far from obvious:

(1) only a few people had read of the bit gold ideas, which although I came up with them in 1998 (at the same time and on the same private mailing list where Dai was coming up with b-money -- it's a long story) were mostly not described in public until 2005, although various pieces of it I described earlier, for example the crucial Byzantine-replicated chain-of-signed-transactions part of it which I generalized into what I call secure property titles.

(2) Hardly anybody actually understands money. Money just doesn't work like that, I was told fervently and often. Gold couldn't work as money until it was already shiny or useful for electronics or something else besides money, they told me. (Do insurance services also have to start out useful for something else, maybe as power plants?) This common argument coming ironically from libertarians who misinterpreted Menger's account of the origin of money as being the only way it could arise (rather than an account of how it could arise) and, in the same way misapplying Mises' regression theorem. Even though I had rebutted these arguments in my study of the origins of money, which I humbly suggest should be should be required reading for anybody debating the economics of Bitcoin.

There's nothing like Nakamoto's incentive-to-market scheme to change minds about these issues. :-) Thanks to RAMs full of coin with "scheduled deflation", there are now no shortage of people willing to argue in its favor.

(3) Nakamoto improved a significant security shortcoming that my design had, namely by requiring a proof-of-work to be a node in the Byzantine-resilient peer-to-peer system to lessen the threat of an untrustworthy party controlling the majority of nodes and thus corrupting a number of important security features. Yet another feature obvious in hindsight, quite non-obvious in foresight.

(4) Instead of my automated market to account for the fact that the difficulty of puzzles can often radically change based on hardware improvements and cryptographic breakthroughs (i.e. discovering algorithms that can solve proofs-of-work faster), and the unpredictability of demand, Nakamoto designed a Byzantine-agreed algorithm adjusting the difficulty of puzzles. I can't decide whether this aspect of Bitcoin is more feature or more bug, but it does make it simpler.

Posted by Nick Szabo at 4:35 PM

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ▼ 2011 (12)
  - ► December (1)
  - ► July (1)
  - ► June (2)
  - ▼ May (2)
    - Bitcoin, what took ye so long?
    - Lactase persistence and quasi-pastoralism
  - ► February (2)
  - ► January (4)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ► 2006 (130)
- ► 2005 (44)