elasticoin-icbc.pdf (151.1 KB)

I want to solicit some discussion on Elasticoin

, which I'm going to present as a short paper atIEEE ICBC 2019, which is a rather weird cryptocurrency issuance scheme I'm using in my blockchain project Themelio.

The goal of Elasticoin is to have a cryptocurrency that has much lower price volatility than coins like Bitcoin, Ethereum, etc, while having an entirely endogenous and trustless algorithm that's resilient to external economic shocks (so no pegs to USD, no price oracles).

The general idea is ridiculously simple: we fix the real cost of minting a coin. If creating 1 coin costs you $1, obviously the price of the coin is capped at $1. Naively you might think this leads to a coin that fluctuates in price just as much as Bitcoin does, except capped at $1, but that's not actually true. Most of the volatility in cryptocurrency prices is based on speculation on the slight chance the price is going to the moon — since traditional cryptocurrencies have fixed supplies, "mainstream adoption" means mooning prices. Thus, every piece of news, or every random investor panic, is going to cause massive price swings due to "chance of Bitcoin worth >$1M in 2030" changing several times in different directions.

The hard problem is fixing the cost without oracles. The naive solution would be to basically use PoW without adjusting the difficulty; this is not going to work because sudden technological advances will cause massive hyperinflation.

Instead, we make it so that one day of sequential computation on the fastest processor available right now

mints you a coin. This can be done trustlessly by leveraging proofs-of-sequential-work that essentially prove that you computed an iterated Argon2 hash a zillion times. Completing a protocol-given sequential puzzle gives you a fixed reward, while difficulties and rewards adjust so that the fastest solver the blockchain has seen solves the puzzle in exactly 24 hours. We also penalize solvers that are slower than the fastest solver, making using GPUs or ASICs where each core is slower but ops per watt are lower, or "free" spare compute cycles on web servers, uneconomical. The exact algorithm is pretty simple and can be seen in the attached paper (read: I'm too lazy to retype a bunch of LaTeX formulas)

(Note that Themelio is a PoS blockchain, so rewards from the Elasticoin minting have nothing to do with incentivizing consensus. Think of the coin as an ERC20 minted by a smart contract verifying people's puzzles)

This is a rather weird metric to use, but empirically the cost of "up-to-date" sequential processing time is actually pretty stable. The price of renting single cores hasn't really changed ever since processors were fully mass-produced. Physically you also don't see massive improvements in sequential processing speed in the future, and it's likely to be really hard to make ASICs dedicated to sequentially computing Argon2 that are much cheaper and faster than CPUs.

What we get is a coin that's basically pointless to HODL in hopes of it mooning, because it's guaranteed that it won't. The trading market would look a lot more like trading fiat currency pairs, and a lot less like the Bitcoin market. Coin prices won't be completely stable (gluts from demand declines will still cause price declines, price shocks in electricity and silicon will affect the coin), but they will almost certainly be much more money-like than Bitcoin. I think that for users wanting a good medium of exchange or gas-paying token, this is a big positive, and could attract the "right" kind of attention and adoption that doesn't correlate strongly with price bubbles.