This is much more of a question than a proposal. This idea is something I have thought about recently and I hoped to get feedback on feasibility.

BLUF: Using the latest Physical Uncloneable Function (PUF) technology, could a gold dealer (let's say someone like Peter Schiff) create chips from physical gold that either cannot be cloned, or would cost more to clone than to manufacture new chips? And once created, these chips could be distributed (from the issuer) to anonymous entities (trustees) where anyone could verify on the Blockchain that these chips are in the possession of the trustee. The goal is to have distributed storage of physical gold that cannot be confiscated by a corrupt organization. It would also add an additional layer of trust against fractional reserve banking.

Limitations:

Must have trust in the chip manufacturer / issuer. Perhaps this could be minimized with some form of "trusted setup" in the physical/manufacturing domain. This includes both trusting that the issuer did not build in a back door, and trust that the issuer is not creating more tokens than physical assets (i.e. fractional reserve banking). While this limitation cannot be fully overcome, the result may be an improvement over current practices.

Other considerations:

These chips would theoretically have embedded private keys that cannot be extracted without considerable cost. (Challenge being that the costs cannot reduce with scale)

Peter Schiff could say he has manufactured a million one ounce gold "chips" and release the public keys to a public ledger. He could distribute them to trustees and post the public address of each and their inventory of gold chips. The trustees names / locations would not be known to local governments.

Each trustee would have a physical machine where say 100 chips are placesd inside. The trustee would log in with his hardware wallet and periodically post to the blockchain a hash proving that the chips and the hardware wallet are in the possession of the trustee.

Over time each chip would get a trust score, with competing ratings algorithms in place to issue a trust score for each gold chip depending on the issuer / trustee reputation.

If Bob sends Alice 10 gold chips, Alice can keep the chips with the trustee and pay warehouse fees periodically, or Alice can pay for shipping to have the chips in her possession. She can melt them down (and trigger a trust rating of zero since she can no longer prove possession) or she can become a trustee herself.

Over time, the trustee would build up a reputation based on the consistency of possession posts, shipping costs, shipping times and warehouse fees. Each chip would now have an NFT associated with it depending on the issuer / trustee reputation and these chips could be priced accordingly in the market.

If successful, this could be a way to create stable coins based on something other than fiat currency and be used as collateral that would make other cryptocurrencies "backed" by physical gold.

Concerns about exit scams could be handled through an additional "insurance" layer, and the market could determine the optimal trustee setup. i. e. anonymous trustees in a shady country vs a publicly listed gold warehouse in a safer jurisdiction, with insurance companies offering lower rates for lower risk issuers / trustees. Something akin to the bond market ratings system.

Curious to hear what people think about this. I know this will never have the security of L1 Ethereum, but perhaps it would still be of value.