(Note: this is a repost of something I've once posted onto r/cryptocurrency but got no useful replies. I only recently discovered ethresear.ch, so please tell me if such a post is off-topic)

It seems like stablecoins aiming to peg themselves to, say, USD essentially fall into three approaches:

1. Centralized currency board maintaining 1:1 link with fiat, like in TrueUSD or Tether. This obviously works as long as you trust the centralized party, and is the most reliable way to peg real world currencies like the HKD to the USD.

2. Collateralized debt with reserves denominated in virtual assets, like Dai

3. Algorithmic central bank, like Basis, with no concept of reserves. Basically tries to be the Fed except implemented as a smart contract.

It's often claimed that algorithmic central banks are the most flexible since black swan crashes in asset backings do not cause issues, and they can theoretically target any exchange rate with anything, including things like baskets of goods. (Aside: I find this highly suspect. Taken to the logical extreme Basis can target a perfectly oscillating sine wave of prices so that everybody can buy low and sell high and get free money, which is obviously false. I am not really knowledgeable enough to know where exactly the argument that anything can be targeted fails though)

The main problem with algorithmic central banks seems to be that without reserves, it's hard to defend a peg when the market price of the coin drops. When the price is higher than the peg the smart contract can simply give everybody helicopter money to drop the price, but if the price is too low there's little that can be done. Basis claims that selling discounted bonds payable only if the peg is restored somehow fixes this, but I remain skeptical — it seems to imply Venezuela can somehow borrow its way out of hyperinflation using cleverly designed bonds, which seems absurd.

However, I wonder whether or not there's an obviously robust solution to fixing algorithmic-central-bank stablecoins — demurrage

, basically a negative interest rate. Imagine I make a stablecoin called PUSD, for Perishable USD, as a token with an algorithmic central bank running on an Ethereum smart contract. Like with any other algorithmic central bank, we print helicopter money if the price (based on some median of oracles) is too high.

However, every year 5% of every PUSD account balance disappears into thin air. Essentially, this means there will always be demand for freshly printed

PUSD. Even if everybody dumps PUSD and the price tanks, eventually the dumped pile will get exponentially small, so that eventually PUSD becomes scarce and the tiny number of "survivors" still wanting to get PUSD must pay 1 USD again. This creates a market expectation that PUSD will always go back to 1 USD, which should prevent price crashes in the first place. PUSD will behave sorta like a fixed production cost perishable good like milk: milk prices won't ever crash significantly under the cost of production.

Clearly, due to the demurrage nobody would prefer to hold PUSD rather than USD, but for applications like hedging risk in crypto-only exchanges, or having a reasonable store-of-value for people living in places like Venezuela, 5% a year might not be too big of a negative interest rate to bear. Perhaps this percentage can be made much smaller and we'd still have a stable currency.

Is there any idea like PUSD floating out there? It seems like quite an obvious way of fixing the problems with algorithmic central banks, at the cost of course of imposing this carrying cost that makes it strictly worse than fiat for people who can use fiat conveniently. Is there some "duh!" gotcha I am missing here?