Burning has a lot of potential as a general cryptoeconomic primitive as an expensive way to signal something. For example, recent threads like Spam resistant block creator selection via burn auction or Burn relay registry: Decentralized transaction abstraction on layer 2 describe using burning as a costly signal for sybil/spam resistance.

I am interested in whether time-locking capital (or Ether) has been considered in place of burning in various situations as a potentially cheaper and more accessible signaling mechanism that still enacts a tangible “cost”. Time-locking your Ether, even if you can sell the future right to it, can have a tangible cost, perhaps roughly calculable by comparing to Compound or staking over the lockup time. Here would be my naive framing:

Burning is expensive because you’re spending the money on nothing except for the signal you’re trying to send. The lever you have to increase or decrease the signal’s strength is the amount you burn. A “burn” could be considered a time-lock with a lockup of forever. However, time-locking in place of burning gives you the lockup period as an additional lever to adjust the strength of the signal more finely. For instance, a lockup of 1 ETH for 1 week is a weaker signal then a lockup of 1 ETH for 1 month. Both of these would be far weaker signals than a burn of 1 ETH.

A concrete application where time-locking may make more sense than burning: an on-chain registry of IPFS hashes, and IP addresses claiming to have the files available. For this kind of registry system, popular or sensitive files may be vulnerable to bad IP addresses being spammed as fake hosts; the problem ends up looking similar to the meta-tx-relayer problem, where you need at least one of the posted IP addresses to be honest.

Initially I thought the burn mechanism was the best way to fight spam for this sort of thing, but am now wondering whether time-locking instead breaks the security model, or is a free UX win. The advantage I have in mind is that relayers may be more willing to signal repeatedly with the same money, knowing that in a week (or however long ends up being a reasonable lockup period), they’ll get their money back. Of course, files with only weakly signaling hosts are still vulnerable to spam, so stronger signaling would be needed in those cases.

My hesitation is that the burn could be done with arbitrarily small amounts of money, which may defeat the need for the additional lever to get such fine-grained control of the signal strength. But seems there may be a real UX gain of not actually losing any money when signaling that may be worth the added complexity. Or maybe there’s something else important I’m missing

Appreciate any thoughts!