Rightly or not, it seems to be considered virtuous for ICOs to sell at below market value - even if there are, for example, $120 million worth of interest in participating at a $120 million valuation, it's considered greedy to either accept the full $120 million, and possibly even (see Gnosis) to accept some limited amount at a super-high valuation set by the market; rather, one should sell to purchasers an even smaller amount, and on even better terms, than they are willing to offer.

In such a sale, in general we can expect token prices to predictably rise after the sale. Some also suggest that this has positive community dynamics, as a community is happier if most of them experience rising prices, and reduces regulatory risk, because (i) smaller ICO size means less scrutiny, and (ii) regulatory action often results due to complaints, and complaints are more likely if participants experience losses, which are less likely here.

However, such sales have an inherent flaw: if a sale is oversubscribed, then everyone has a large incentive to get in, and to use unintended mechanisms to compete with everyone else to do so. If the mechanism is first-come-first-serve, then everyone will pay super-high gas fees. Very often, the mechanism is some opaque registration process, in which case well-connected crypto elites get in.

I propose an egalitarian alternative. Users whose accounts are confirmed as corresponding to unique humans (eg. through PICOPS) can send any amount of ETH into a contract with a defined contribution time, as well as a defined TOTALCAP (eg. 10000 ETH). When the sale ends, there are two cases:

1. The total amount sold is less than or equal to the TOTALCAP. In this case, everyone gets an allocation equal to the full amount of ETH they sent.

2. The total amount sold is more than the TOTALCAP. In this case, the contract selects that highest possible per-person cap N such that, if who anyone bought more than N had the excess refunded, the total amount still in the contract would be less than or equal to the TOTALCAP. Anyone who bought more than N has the excess refunded, and everyone gets an allocation equal to min(what they originally sent, N).

One can compute this by maintaining a data structure that stores all purchases in sorted order of size. Once the sale ends, one can repeatedly call a function to crawl from the end of the data structure (ie. the largest purchaser), saving along the way the total amount of ETH in the purchases already crawled through (HIGHTOTAL) to the point where, for the first time, the crawler is at the P'th highest purchaser, and TOTAL - HIGHTOTAL + CURPURCHASE * P < TOTALCAP. At this point, the per-person cap is set (one can even linearly interpolate to find the per-person cap between two purchase amounts that gives a total of exactly TOTALCAP), and everyone can send a transaction to finalize their purchase and refund any remaining ETH.

This ensures that consumer surplus from an oversubscribed sale is distributed in an egalitarian way, and ensures a wide coin distribution. The main weakness of this scheme is that it creates incentives to buy PICOPS accounts or repeatedly ask one's friends to buy in ICOs on one's behalf. PICOPS account selling can be prevented by identity services that make sure any individual always has the ability to reset their identity to another account, making it very risky or inconvenient to buy accounts; only testing such a scheme in real life can reveal how the second issue plays out.