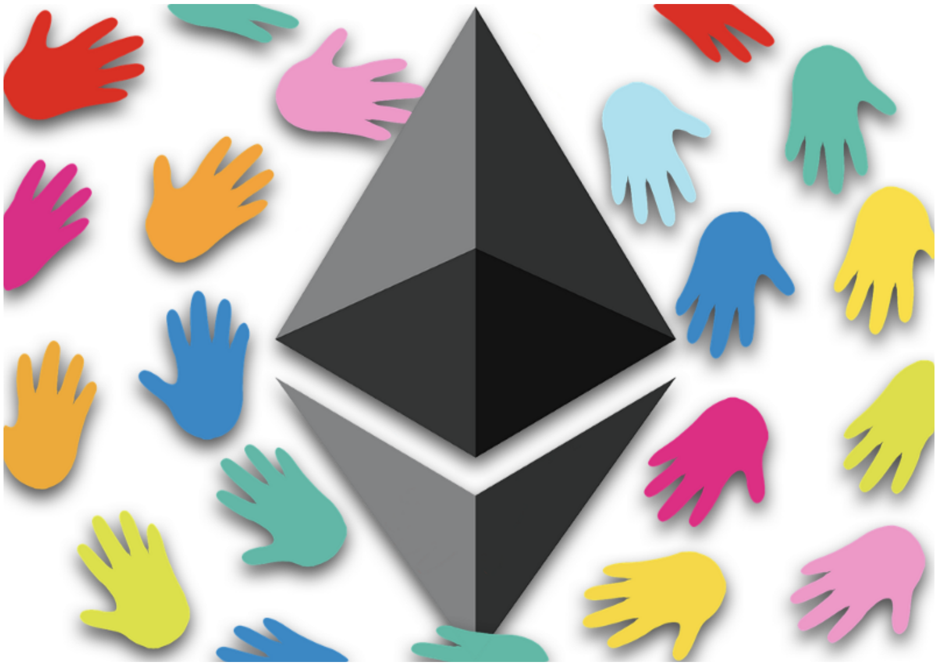
Jason Teutsch Follow
Sep 25, 2017 · 2 min read

Interactive coin offerings



Ethereum has ushered in a remarkable new era of token crowdsales. In a recent blog post, Vitalik Buterin distilled two desirable properties of such distributions.

1. Everyone who wishes can successfully purchase tokens.

2. A fixed amount of currency buys at least some minimum fraction of the total tokens.

Unfortunately, as Vitalik argues, these two properties are mutually exclusive. Uncapped sales satisfy property 1 and capped sales satisfy property 2, however each of these traditional distribution methods fails to satisfy the corresponding complementary property.

Despite the “dilemma” noted above, we can construct a crowdsale protocol such that if each participant specifies a desired purchase quantity at each valuation, then the ultimate, universal, per token cost to sale percentage ratio satisfies all buyers. In contrast to a reverse Dutch auction, where increasing purchase power and limited supply may cause buyers to jump in too soon, we consider a protocol which not only monotonically converges to a sale valuation but also guarantees token availability and fair market information throughout the fixed duration of the crowdsale.

We wish to achieve a market equilibrium through buyer interactions. In the scheme discussed in the link at the end of this paragraph, buyers not only submit bids for tokens but may also voluntarily withdraw their bids after committing them to the sale (within certain limits). In addition, each buyer submits to the crowdsale smart contract a *valuation table* which maps total sale amounts to the buyer’s contribution amount. The smart contract continuously and automatically withdraws bids according to the present bids and valuation tables. Our implementation introduces incentives which enable the smart contract to manage the complex operations of adding, deleting, and finding the minimum value in a list as well as identifying a subset of entries whose sum exceeds a target value. Check out my joint article with Vitalik, “Interactive coin offerings,” for further details.

Cryptoeconomic research opportunities abound on both empirical and deductive fronts. Systems must “prove” security and effectiveness by enduring the test of time in order to become cryotoeconomic “theorems.” On the other hand, pioneering protocol designs require rigorous analysis to ensure a good chance of success. I hope that the present foray into algorithmic game theory will encourage our community to continue to think explicitly about assumptions and goals for crowdsales as we experiment with and build upon the trustless, cryptoeconomic power of smart contracts.

I conclude with some exploratory musing. Until now, crowdsales have focused exclusively on distributing integer quantities of identical tokens to buyers. In the future, however, protocols may launch sets of tokens representing distinct group elements, linked lists (hat tip Hampus Jakobsson), or even complex-valued currencies. Many elementary, mathematical and computer science structures loom on the token horizon.