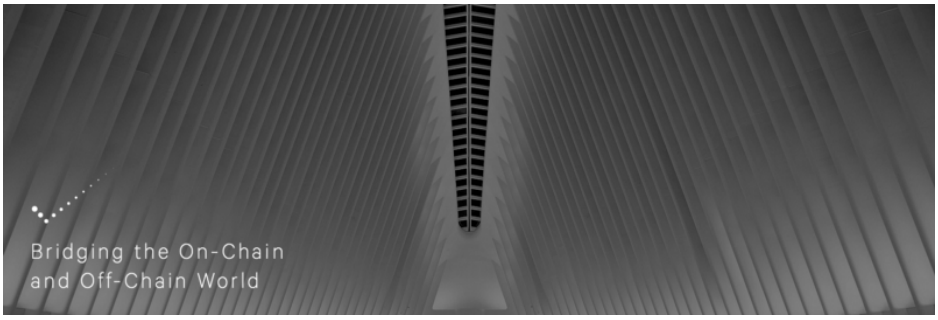
Rob Bent Follow
Truebit since Day 1 — Helping Smart Contract Platform's Scale #Bridging the Onchain and Offchain World
Sep 26, 2017 · 7 min read

Interactive Coin Offering — A Protocol Explained



The majority of token sales to date have been met with some form of criticism. This indicates there has yet to be a protocol developed that includes all of the properties contributors would like. The two major variations of current public tokens sales include:

- Capped Sale—a fixed number of tokens sold at fixed price resulting in a fixed valuation. These sales tend to be oversubscribed and sell out quickly, making it difficult for everybody to participate, leading to congestion on the network and allowing for a "free trade" for early contributors. Some sales end up with massive transaction fees and many failed transactions as people rush to get in. Overall, this model relies on the Token Issuer to set the price and seems to be broken.

- Uncapped Sale—often criticized for being greedy, but more importantly they give participants high uncertainty about the valuation that they are buying in at. This can lead to strange behaviours where buyers have sometimes been caught between

buying in early to take advantage of a discount and waiting until the final stage to better gauge valuation.

There have been a number of attempts at better systems, well documented by Vitalik Buterin here http://vitalik.ca/general/2017/06/09/sales.html, but it's clear a suitable solution has yet to become commonplace.

According to Vitalik—there are a two conflicting desired properties in a crowdsale—that lead to "the first token sale dilemma".

- Certainty of valuation—you should have certainty of a ceiling on the valuation
- Certainty of participation—If you try and participate in a sale, you will succeed

The Interactive Coin Offering is a protocol from creators Jason Teutsch and Vitalik Buterin to solve the "first token sale dilemma". If you are interested in further details and implementation, you can read the Whitepaper detailing the protocol at the bottom of this article.

So—what is the Interactive Coin Offering Protocol? It's an ICO purchase protocol, in which each individual contributor will choose an amount of tokens they'd like to purchase and a "Personal Cap":

- Personal Cap = the specified LIMIT of the total amount of ETH raised in the sale for a participant. If the total amount of ETH raised in the sale is more than the personal cap, the contributor will be removed from the sale or "poked out."

For any Company's ICO, alist of contributor's initial bid's might look like the table below—For illustrational purposes of the protocol, we assume the amount of tokens a contributor chooses are converted to their corresponding value of ETH.

Table 1 - Initial Bids		
Name	**Contribution (ETH)**	**Personal Cap (ETH)**
Christian Address 1	5,000	100,000
Christian Address 2	10,000	85,000
Robbie	8,000	110,000
Farzad	7,500	105,000
Sami	12,500	65,000
Ryan Address 1	5,000	1,000,000,000
Ryan Address 2	20,000	80,000
Jason	7,500	95,000
Zac	15,000	90,000
Vitalik	7,500	70,000
	98,000	

In the case above, the contract consider all bids and make “Automatic Removal” adjustments, “poking” out those contributors where the personal cap was exceeded—starting with the lowest bids.

- The lowest personal cap is Sami at 65K, so his bid would be removed, resulting in 85.5K ETH remaining in the sale (98K—Sami’s Token Contribution of 12.5K=85.5K)
- The next lowest personal cap is Vitalik at 70K, so his bid would be removed leaving 78K in the pool (85.5K—7.5K).

After Vitalik is poked from the pool, we see that all the total Contribution is below all remaining personal caps resulting in a crowdsale value of 78K ETH.

Table 2 - First Set of "Poke-Outs" Removed		
Name	**Contribution (ETH)**	**Personal Cap (ETH)**
Christian Address 1	5,000	100,000
Christian Address 2	10,000	85,000
Robbie	8,000	110,000
Farzad	7,500	105,000
Sami		65,000
Ryan Address 1	5,000	1,000,000,000
Ryan Address 2	20,000	80,000
Jason	7,500	95,000
Zac	15,000	90,000
Vitalik		70,000
	78,000	

Contributors can play this game with multiple addresses and if a contributor would like to guarantee participation in the crowd sale, they can select a large enough personal cap to guarantee their token's are allocated to the sale—(We see this with Ryan address 1).

In addition to the "Automatic Removal" described above, we also propose a "Voluntary Removal Period" whereby user's can choose to remove a bid within a set time frame during the the issuance. For example, after the initial Bid / Poke-Outs above, lets assume the following:

Table 3 - Adjustments Happen While in Voluntary Removal Period

Name	Contribution (ETH)	Personal Cap (ETH)
Christian Address 1		100,000
Christian Address 2	10,000	85,000
Robbie		110,000
Farzad	7,500	105,000
Sami	15,000	100,000
Ryan Address 1	5,000	1,000,000,000
Ryan Address 2	20,000	80,000
Jason	7,500	95,000
Zac	15,000	90,000
Vitalik	15,000	100,000
	95,000	

- Christian and Robbie look at the 78K ETH Contribution and believe there isn't enough demand for the sale. Both decide to voluntarily remove their bids. (denoted in red)
- Sami and Vitalik (who we're automatically poked out in the initial round) decide they really want to be in the sale and increase both their contribution and personal caps. (denoted in green)
- Total contribution of ETH in the crowdsale is now 95K, but this is above some of the personal caps—so the Poke-Out loop is run again!
- The Protocol find's the lowest personal cap (Ryan Address 2 at 80K) and makes adjustments. Reducing Ryan's contribution by 15K brings the total ETH contribution to 80K, leaving him with contribution of 5K at that personal cap. See the table below.

Table 4 - Results after the Next Set of Poke-Outs		
Name	**Contribution (ETH)**	**Personal Cap (ETH)**
Christian Address 1		100,000
Christian Address 2	10,000	85,000
Robbie		110,000
Farzad	7,500	105,000
Sami	15,000	100,000
Ryan Address 1	5,000	1,000,000,000
Ryan Address 2	5,000	80,000
Jason	7,500	95,000
Zac	15,000	90,000
Vitalik	15,000	100,000
	80,000	

The Interactive Protocol will continue for multiple rounds until the Voluntary Removal Period Ends. At this point, contributors can only add bids or be removed automatically. For our example, we assume some individuals review the 80K total ETH contribution in relation to their personal cap and decide to increase contribution size:

- Farzad and Sami increase their contribution to 25K (in the protocol, users will actually need to form a new contract/address to increase their bid as detailed in the white paper)
- Ryan is nervous that his 5K contribution at 80K personal cap is going to get poked out, so he issues a new 15K contribution at 110K cap
- Jason increases contribution to 20K
- A whopping 135K in ETH has now been raised. As in previous rounds, we start by finding the minimum bids and poking them out.

Table 5 - Automatic Lock-In		
Name	**Contribution (ETH)**	**Personal Cap (ETH)**
Christian Address 1		100,000
Christian Address 2	10,000	85,000
Robbie		110,000
Farzad	25,000	105,000
Sami	25,000	100,000
Ryan Address 1	5,000	1,000,000,000
Ryan Address 2	5,000	80,000
Ryan Address 3	15,000	110,000
Jason	20,000	95,000
Zac	15,000	90,000
Vitalik	15,000	100,000
	135,000	

- The protocol removes Ryan's contribution of 5K at 80K cap, Christian's bid of 10K at 85K cap, followed by Zac's bid of 15K at 90K cap.
- There is now total contribution of 105K ETH (135K—5K—10K—15K), but Jason's personal cap is 95K.
- 10K of Jason's contribution is removed, leaving Jason with 10K remaining contribution and 95K total contribution

Table 6 - Final Results		
Name	**Contribution (ETH)**	**Personal Cap (ETH)**
Christian Address 1		100,000
Christian Address 2		85,000
Robbie		110,000
Farzad	25,000	105,000
Sami	25,000	100,000
Ryan Address 1	5,000	1,000,000,000
Ryan Address 2		80,000
Ryan Address 3	15,000	110,000
Jason	10,000	95,000
Zac		90,000
Vitalik	15,000	100,000
	95,000	

The interactive protocol allows for a number of interesting properties that come about through price discovery over multiple rounds and interaction with the crowd. This example included:

- Voluntary drop-outs
- Increase the contribution size due to perceived low valuation before the end of sale
- Using a large personal cap to guarantee participation
- Poke outs

In reality, the protocol will execute these loops seamlessly, and in real-time over a very large number of rounds. We can see a number of interesting principles at work here:

- After the Voluntary Removal Period, the value of the total contribution will rise monotonically in each round
- **We expect pricing and total contribution to converge to a natural equilibrium as a result of the interactive protocol**

Due to the interactive nature of the game, the ability to set a personal cap, and the ability to raise this personal cap until the end of the game, we are solving the dilemma put forth requiring a trade-off between guaranteed participation and guaranteed valuation. We hope that this idea will spur discussion amongst the community and will take advantage of some of the new aspects that smart contracts allow!

At Truebit, we are extremely excited to use game theory and protocols to create deep innovation in the space. In addition to delivering the Truebit Protocol, we take research seriously. It is a Truebit core value to be a source of honesty and truth in the community and a haven for builders, creatives and academics. We want to attract a mixture of implementation experts looking to build and academics looking to research and contribute to big problems in the blockchain space. We hope you enjoy our first contribution to that effort!

Footnote 1: It is also pertinent to note that a discount can be provided for those entering bids in earlier stages of the sale to encourage participation. This is called an inflation ramp and will provide incentives to ease the uncertainty of an initial illiquid environment (when people

are unsure of prices). A proposed discount in a 20 day sale may include a 20% initial discount declining by 1% per day.

Footnote 2: