An Optimal ICO Mechanism

David Cerezo Sánchez[†]

Calctopia[†]

david@calctopia.com

October 19, 2017

Abstract

Initial Coin Offerings (ICOs) are raising billions in funding using multiple strategies, none justified from the point of view of mechanism design, resulting in severe underpricing and high volatility.

In the present paper, an optimal ICO mechanism is proposed for the first time: a truthful multi-unit Vickrey-Dutch auction of callable tokens (i.e., a new hybrid security of tokens packaged with callable warrants). Truthful bidding is an ex-post Nash equilibrium strategy and the auction terminates with an ex-post efficient allocation; additionally, the callability of the warrants eliminates the winner's curse of the auction and its underpricing.

An implementation demonstrates its practical viability.

JEL classification codes: G23, G24, G32, D44, D82, C72, O33, L26

Keywords: Optimal ICO, mechanism design, multi-unit auction, callable warrant, cryptoeconomics

1 Introduction

Initial Coin Offerings (ICOs) have raised $1.5 billion through 91 ICOs (14 July 2017, [Tok17]) and have already passed VC funding in the blockchain market[Sun17]. The most used models for token sales are capped sales (i.e., selling a fixed number of tokens at a fixed price) and uncapped sales (i.e., selling as many tokens as possible): these mechanisms offer no price discovery and usually result in severe underpricing. When the tokens get listed on exchanges, the high appreciation that they display are evidence of the underpricing experienced during the ICO sale. For example, the following table lists the recent ICOs of projects which have not yet released working products but show a very high appreciation (19/7/2017, [STA17]):

Name	Appreciation(%)	ICO Date	ICO Price	Curr. Price
Ark	+4525.68%	11/07/16	$0.010	$0.460
Golem	+2447.49%	11/11/16	$0.010	$0.267
Aeternity Phase I	+1130.92%	04/03/17	$0.043	$0.526
Melonport	+736.14%	02/15/17	$5.800	$48.496
Gnosis	+666.14%	04/24/17	$25.510	$195.441
SingularDTV	+631.24%	10/05/16	$0.015	$0.110
Quantum Ledger	+466.65%	05/01/17	$0.077	$0.436
adToken	+275.87%	06/26/17	$0.009	$0.033
Mysterium	+260.29%	05/30/17	$0.176	$0.635
Humaniq	+247.71%	04/06/17	$0.039	$0.137
Aragon	+121.76%	05/17/17	$0.917	$2.033
iEx.ec	+115.19%	04/19/17	$0.178	$0.383
ChronoBank	+91.03%	12/15/16	$7.604	$14.527
EOS	+79.83%	06/26/17	$0.925	$1.663
TaaS	+77.09%	03/27/17	$1.000	$1.771
VOISE	+50.46%	06/05/17	$0.867	$1.305

The case of Gnosis requires special mention: although the ICO was conducted using a Dutch auction[Lis16], it also suffered from the same underpricing that is also found on previous IPO auctions and that is usually attributed to the winner's curse and the lack of truthfulness of the used mechanisms.

The confusion in the ICO market has spurned a quest for optimal token sale mechanisms[But17, Mag17], a search that ends with the present mechanism that offers:

- truthful price discovery of the market valuation of the project
- solving the winner's curse of the auction
- the high volatility of ICOs gets priced into the deal: the issuer raises more funding based on the volatility and the bidders will be able to buy more tokens in the future at a low strike price

2 Related literature

Investors in ICOs often don't hold financial securities that give them ownership rights on the cash-flows of the projects: unlike the traditional paradigm separating the financial side from the product/market side of the firm, investments in ICOs are directly integrated with the real side of the firm, that is, the demand structure for their digital services. Although the general ideas contained in previous literature applying mechanism design on crowdfunding or IPOs are right and could be useful on the ICO setting, their models and proofs are unuseable since there are many significant differences, as explained in this section.

2.1 Crowdfunding Literature

Previous crowdfunding literature[Cha15, BOP15, KLZ15, BLS12, EH16] is based on the following assumptions that can't be found on an ICO token sale:

- The entrepreneur has pricing power, ex-ante and post: in an ICO token sale, the entrepreneur has limited pricing power, especially after the token sale because the price fluctuates.
- Entrepreneurs are able to differentiate between informed/uninformed investors, high/low-value investors: in an ICO token sale, the entrepreneur can't discriminate between the buyers.
- Entrepreneurs can control the number of produced units: in some ICO token sales, the number is fixed.
- During a crowdfunding, the entrepreneur can charge higher prices than the post-crowdfunding market price: in an ICO token sale, the token is usually sold at a lower price.
- A crowdfunding sells a future product, ICOs sell a token, usually a right-of-use to a future digital service.

Nonetheless, there are important parallels between ICO and crowdfunding:

- Both ask for an all-or-nothing contribution to start the project, setting a minimum contribution price to start the project.
- Both enable to test the demand for the product/digital service, that is, they allow to adapt production to market demand.

2.2 IPO Literature

Previous IPO literature[BF04, BBR02, BF08, DW03, Mal05, PS09] is based on the following assumptions that can't be found on an ICO token sale:

- Shares represent a fraction of a real business with cashflows, valuable assets and voting rights: in an ICO token sale, the business may not yet exist and tokens usually represent a right-of-use to a digital service.

- Bookbuilding is the usual method to price an IPO: in an ICO token sale, capped/uncapped sales are the most used method. Auctions are almost never used on IPOs/ICOs.
- A third party, an underwriter, handles the IPO: in an ICO token sale, the entrepreneur manages the whole process.
- The underwriter can discriminate between institutional and retail investors: in an ICO token sale, the entrepreneur can't discriminate between the buyers.
- The mechanisms/allocation rules proposed in the literate use direct allocation with full preference elicitation: in an ICO token sale, capped/uncapped sales are the usual method.

2.3 Previous IPOs/ICOs

A number of previous experiences provide guidance to the design of an optimal mechanism for ICOs:

- Previous Dutch-auction IPOs: much has been written about the failure of Google's IPO[Cho05, TL08, Ana05] to properly price the auction, a disadvantage common to other Dutch-auction IPOs[RR12, DW03].
- Previous warrant auctions: JP Morgan Chase and Capital One Financial raising funds[Wil09] based on the high volatility due to the financial crisis while sharing the upside with the bidders as they recover.
- Previous ICO using an auction: Gnosis[Lis16] displayed underpricing[But17].

Several papers have documented the empirical superiority of auction-like mechanisms ([DW03, DDW10, Van03, KSW99]). Experimental comparatives of IPO mechanisms[BV11, BFC02] demonstrate the optimality of specially designed auctions for IPOs (i.e., the Ausubel's auction[AC98, Aus02, Aus04]): nonetheless, the Ausubel's auction[Aus04] has never been tried in the IPO environment and it's the ascending counterpart of the auction used in this paper (see section 3.2.2).

3 Optimal ICO Design

In this section, a model defining an ICO is introduced, followed by detailed descriptions of the auction and the design of the hybrid security of callable tokens (i.e., a token packaged with callable warrants).

3.1 ICO Model

Entrepreneur. Consider an entrepreneur that needs capital investment of $C > 0$ to develop a digital service/product that will be used at some marginal cost $m_c \in [0, 1)$.

Initial Coin Offering (ICO). Let c be the total number of bidders and denote a specific consumer by the index $i \in \mathbb{N} = \{1, \ldots, c\}$; every bidder has a binary valuation of the service, $v_i = 1$ or $v_i = 0$. Let $v = (v_1, \ldots, v_c) \in V = \{0, 1\}^c$ be the c-dimensional vector of the valuation profile of the bidders and $\pi(v)$ denote its corresponding probability. The probability that b bidders value the product is

$$Pr(b) = \begin{matrix} \sum \pi(v) \\ \left\{v : \sum_{i \in N} v_i = b\right\} \end{matrix}$$

Since $m_c < 1$, b can be interpreted as the potential demand for the entrepreneur's service: its randomness expresses the demand uncertainty.

Entrepreneurship without demand uncertainty. Consider perfect knowledge of the project's future revenue, p_r: it's socially optimal to invest if the project's revenue covers the cost of production $C + p_r m_c$, that is

$$p_r \geq c^* = \frac{C}{1 - m_c}$$

In this case, the ex-ante expected aggregate surplus is

$$S^* = \sum_{p_r = \lceil c^* \rceil}^{c} Pr(p_r) \left[(1 - m_c) p_r - C\right]$$

If the entrepreneur raises the funds, investing in the project and selling the results would be the optimal strategy: therefore, a credit market will lend the C at zero interest rate in perfect foresight of the entrepreneur's plan.

Entrepreneurship with demand uncertainty. In case p_r is not known, it's optimal to set $p = 1$ and it would be optimal to invest with positive profits

$$\overline{\mathit{\Pi}} = \left(\sum_{p_r = 0}^{c} Pr(p_r)(1 - m_c) p_r \right) - C \geq 0$$

Under demand uncertainty, the entrepreneur invests with positive (negative) profits $\overline{\mathit{\Pi}} \geq 0$ (resp. $\overline{\mathit{\Pi}} < 0$) and this may imply overinvestment (underinvestment) because the entrepreneur executes the project when it turns out that $p_r < c^*$ (resp. $p_r < c^*$).

ICO Crowdfunding. An entrepreneur announces an "all-or-nothing crowdfunding" defined by a pair (t, T): a minimum token value t for b bidders (i.e., a bidder could contribute multiple tokens as different bidders), so that if the total collected pledges $P = bt$ are greater than T, $P > T$, the entrepreneur receives all the pledged funding to produce the digital service; but if $P < T$, the entrepreneur collects no funding from the bidders.

An all-or-nothing crowdfunding scheme (t, T) with $t \in (0, 1]$ yields the entrepreneur the expected profit

$$\mathit{\Pi}^c(t, T) = \sum_{p_r = \lceil T/p \rceil}^{c} Pr\{p_r\} \left[(t - m_c) p_r - C\right]$$

Profit is maximized with a token level $t = 1$ and target level $T = c^*$, the entrepreneur extracting the maximum aggregate surplus S^*, thus yielding an efficient outcome: it implements the first best in dominant strategies and respects ex-post participation constraints.

3.2 Dutch Auctions

3.2.1 General Results

Dutch-auction have been used in some IPOs[RR12] and ICOs[Lis16] due to the following properties:

- In theory, strategically equivalent to a first-price sealed-bid auction, although not in practice[CRS82, LRBC+99, KK08].
- Using a Dutch auction, the market-clearing price is found.
- Speculators do not make profits in first-price/Dutch auctions[GT05]
- If the numbers of bidders is large, the Dutch auction produces more revenue than a first-price auction[Mie13]
- The most efficient and largest revenue outcome occurs when bidders are not provided information on either group size or units remaining[BGP16]
- At fast clock speeds, revenue in the Dutch auction is significantly lower than in the sealed bid auction. When the clock is sufficiently slow, however, revenue in the Dutch auction is higher than the revenue in the sealed bid auction[KK08]

The limited use of Dutch auctions in IPOs despite their potential for more fully pricing the issue is due to low underwriter compensation[RR12]: in French markets, there is a smaller degree of underpricing using auctioned IPOs than traditional IPOs[DW03].

Unfortunately, they also present the following undesirable properties:

- IPOs using Dutch auctions experience an underpricing effect, although in smaller magnitudes that in traditional IPOs[RR12]
- Dutch auctions are not incentive compatible, that is, truthful bidding is not an efficient strategy. Some later works introduce variants of the Dutch auction that are incentive-compatible[MP08, AE13].

3.2.2 Multi-Unit Clinching Vickrey-Dutch auction

The simple multi-unit Clinching Vickrey-Dutch auction[MP08] is a modern extension of the traditional Dutch auction for multiple homogeneous goods, featuring truthful bidding in an ex-post Nash equilibrium and terminating with an ex-post efficient allocation. It assumes a private value setting, where each bidder knows his own valuation function and its does not depend on the valuations or allocations of other bidders. And although the auction is discriminatory (i.e., winning bidders pay different prices according to their own bids), it maintains a single price for the tokens in each iteration, allowing their listing on cryptocurrencies exchanges; actually, discriminatory prices protect less-informed investors because when they bid, they obtain exactly the quantities they demand at the desired price.

This auction is also iterative, taking bids from buyers in each iteration and avoiding the revelation of unnecessary private valuation information through price discovery. Iterative auctions ease the valuation problem faced by bidders, often costly and time-consuming: price discovery guides bidders in deciding how to invest effort in refining their beliefs about their private valuations. Additionally, unnecessary preference elicitation from losing bidders is completely avoided since it's a descending auction.

Definition 1. The maximal demand given the marginal price of a unit, q^t, is:

$$\overline{D}_i\left(q^t\right) = \begin{cases} 0 & \text{, if } v_i\left(1\right) - v_i\left(0\right) < q^t \\ \displaystyle\max_{j \in \{0,1,\ldots,n\}} j \quad \text{s.t. } v_i\left(j\right) - v_i\left(j-1\right) \geq q^t & \text{, otherwise} \end{cases}$$

Definition 2. The residual demand without buyer i is the amount of the supply that is allocated to buyer i in the main economy that is also demanded (in aggregate) by other buyers and is defined as $r_{-i}\left(q^t\right) = \min\left(x_i, \sum_{j\neq i}\left[\overline{D}_j\left(q^t\right) - x_j\right]\right)$ for all iterations $t \geq t^m$, in which t^m is the first iteration in which $\sum_{i\in B} x_i^t \geq n$. For iterations $t < t^m$, define $r_{-i}\left(q^t\right) = 0$ for all $i \in B$.

Definition 3. The **simple Clinching Vickrey Dutch auction** is an iterative procedure with the following steps:

(S0) Start from a high price q^0. Set $t := 0$. Set the total number of units clinched by buyers, $(c_1, \ldots, c_m)$ to zero. Set the total payments of buyers, $(s_1, \ldots, s_m)$ to zero.

(S1) In iteration t of the auction with price q^t:

(S1.1) Collect maximal demand $\overline{D_i}\left(q^t\right)$ of every buyer i at price q^t. Impose $\overline{D_i}\left(q^t\right) \geq \overline{D_i}\left(q^{t-1}\right)$ for every buyer for all $t > 0$.

(S1.2) If $\sum_{i\in B}\overline{D_i}\left(q^t\right) < n$ then $c_i = \overline{D_i}\left(q^t\right)$ for all $i \in B$. Set $q^{t+1} := q^t - 1$, $t := t+1$, and repeat from Step (S1.1).

(S1.3) If $\sum_{i\in B}\overline{D_i}\left(q^t\right) \geq n$ and $\sum_{i\in B}\overline{D_i}\left(q^t\right) < n$, then set $t^m := t$ and set c to be any sequential allocation.

(S1.4) Set $s_i := s_i + q^t * \left(r_{-i}\left(q^t\right) - r_{-i}\left(q^{t-1}\right)\right)$ for all $i \in B$.

(S1.5) If $r_{-i}\left(q^t\right) = c_i$ for all $i \in B$ or $q^t = 0$, then go to Step (S2). Else, set $q^{t+1} := q^t - 1$, $t := t+1$ and repeat from Step (S1.1).

(S2) Final allocation is $(c_1, \ldots, c_m)$ and the final payment vector is $(s_1, \ldots, s_m)$.

Theorem 4. *Truthful bidding is an ex-post Nash equilibrium strategy in the simple Clinching Vickrey Dutch auction under the activity rule and the auction is ex-post efficient in the homogeneous items Non-Increasing Marginal Valuation environment.*

Proof. See [MP08]. □

3.2.3 Bidding Language

Let $v_i(j)$ denote the value of the bidder i for j units of the item. Assume $v_i(0) = 0$ for every bidder and $v_i(j) \geq 0$ for every unit $1 \leq j < n$ and bidder i. The valuations of each bidder must respect that only Non-Increasing Marginal Values (NIMV) are accepted, that is,

$$v_i(j) - v_i(j-1) \geq v_i(j+1) - v_i(j)$$

for every bidder i and every unit $1 \leq j < n$.

For example, the following is a valid bidding valuation matrix[MP08]:

j	1	2	3	4
$v_1(j)$	7	9	10	10
$v_2(j)$	8	13	15	15
$v_3(j)$	4	8	10	10

In case the number of units is higher, $j = 1.000.000$, and the bidders are willing to bid for 100.000 units at 10 monetary units each, they could express that bid in the following ways:

j	1	2	...	99.999	100.000	...	1.000.000
$v_1(j)$	10	20	$j \cdot 10$	999.990	1.000.000	1.000.000	1.000.000
$v_2(j)$	1	2	j	999.990	1.000.000	1.000.000	1.000.000
$v_3(j)$	1	2	$j \cdot 8$	999.990	1.000.000	1.000.000	1.000.000

Note how each bidder express their preferences in different ways, even if sharing the same valuation: bidder 1 always bids their truthful valuation for every token; bidder 2 is not interested in acquiring a low amount of tokens, only a number of tokens around 100.000 units; and bidder 3 is also interested in acquiring 100.000 tokens at 10 monetary units, but a lot lower than 100.000 units is also desired. All the bidders are not willing to bid for more than 100.000 units, so they maintain their valuations constant until reaching the total number of units.

3.3 Callable Tokens

As shown in the Introduction, there is evidence in the ICO market of the manifestation of underpricing as in IPOs: the potential presence of better-informed investors than others entails that investors with less information end up with a smaller (larger) allocation of shares when the issue is underpriced (overpriced)[Roc86]. Therefore, investors with less information require a lower subscription price to start with.

Definition 5. Warrant. Financial derivative that confers the right, but not the obligation, to buy or sell a security at a certain price (exercise price or strike price) before expiration: an American warrant can be exercised at any time on or before the expiration date, while European warrants can only be exercised on the expiration date.

To minimize the costs of the winner's curse, we focus on the design of the security that minimizes the sensitivity to information asymmetries of the different investors, irrespective of the mechanisms being used (i.e., compatible with the multi-unit Clinching Vickrey Dutch auction). Risk-averse entrepreneurs can signal the high quality of their project when outcomes are risky by including warrants[CF99]: they value their risky high-state payoffs less than investors when they want to diversify their position, thus they could use warrants that pay in high-state payoffs to signal the quality of their project because it's cheaper than underpricing[GH89]. This is conceptually similar to commitments to buy back debt or equity that allow to provide signaling and to finance valuable projects[CG89, BK87], or to the optimal financing of projects with callable convertible bonds in the presence of adverse selection[CY11].

Definition 6. Callable warrant. A warrant where the issuer has the right to call the warrant during a certain period.

Riskier projects in down markets can lower the cost of ICOs by combining tokens and warrants together: when the information from better-informed investors is about the downside risk of the project, investors with less information are less disadvantaged combining tokens and warrants together, reducing the cost of doing an ICO and the negative effects of the winner's curse. Moreover, the winner's curse can be fully eliminated for projects that have a sizeable growth potential even in down markets by making the warrants callable, yielding the first-best outcome[CGY10]: if the potential success and profitability of the project in down markets is sufficiently large, the callability of the tokens allow the dynamic creation of a security whose ultimate payoff is insensitive to the initially held private information of informed investors.

Definition 7. Callable token. A token packaged with callable warrants that confer the right to convert them into tokens.

A token with warrants entitles the tokenholder to convert the warrants into tokens of the issuer. On the other hand, in order to cap the unlimited upside potential of the warrant, the warrant indenture usually includes a clause where the issuer can call back the warrant at a predetermined call price. Upon calling, the tokenholder either chooses to receive the cash amount equivalent to the call price or to convert into tokens (this is direct, cashless conversion). For these two rights, the convertible feature is the right conferred to the tokenholder while the callable feature is the right held by the token issuer.

For the issuer, warrants are an optimal form to raise funding: since volatility is an important component of warrant pricing, and there is much volatility of token issues and the token market in general, the price of the warrants will be high and thus the entrepreneur is raising a large amount of investment based on said high volatility. The use of warrants also justifies that the issuer must hold a large percentage of tokens[But17] to satisfy the future conversion/recall of tokens: unlike warrants on shares, there won't be dilution when converted/recalled, just transferred from the issuer's token pool.

3.3.1 U.S. Securities Laws

Any utility token would be transformed into a security whenever packaged by warrants because warrants or any asset packaged with warrants are securities according to the Howey test[Cou46]: offering securities to US citizens in an ICO requires registration with the SEC according to its latest report on the DAO[SC17a]; other countries may follow with similar or more restrictive regulations (e.g., China's ICO ban[Zha17], Hong Kong's statement[SC17b]). As the requirements for registration are complex and costly, many ICOs are not being offered to US citizens.

Any ICO token sale must then consider the trade-off between selling to US Citizens, or offering packaged warrants and risk losing 20-30% capital that is typically raised from US citizens, that is,

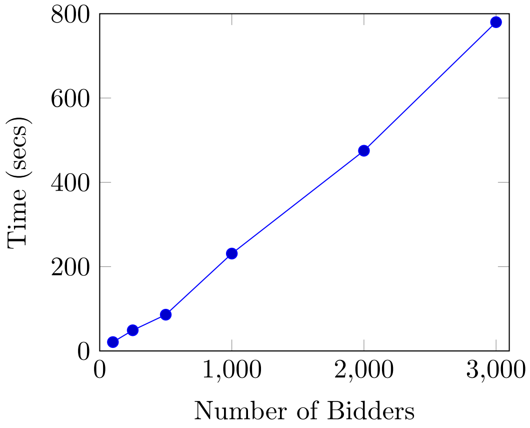
$$\text{Value of warrants} > 20\% - 30\% \text{ raised capital}$$

After the token sale, warrants may become detachable from utility tokens to list them on non-US exchanges, while the utility tokens are listed on US exchanges: this prevents them from being banned from listing or being delisted from American exchanges[Sha17].

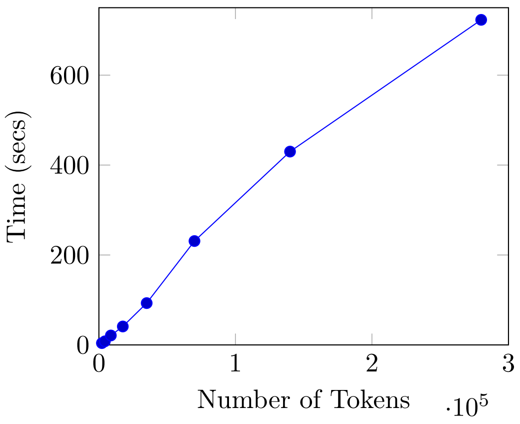
4 Implementation

The simple Clinching Vickrey-Dutch auction (see Definition 3) is implemented as pseudo-code on Appendix A: although it's a very efficient algorithm, to run it on Ethereum would be prohibitively expensive and slow; additionally, to prevent signaling/collusion most information must be hidden except the prices.

The following is a timing experiment of a Python implementation of the simple Clinching Vickrey-Dutch auction, varying the number of bidders while maintaining fixed the number of tokens to be auctioned (70000) and the final price (2).

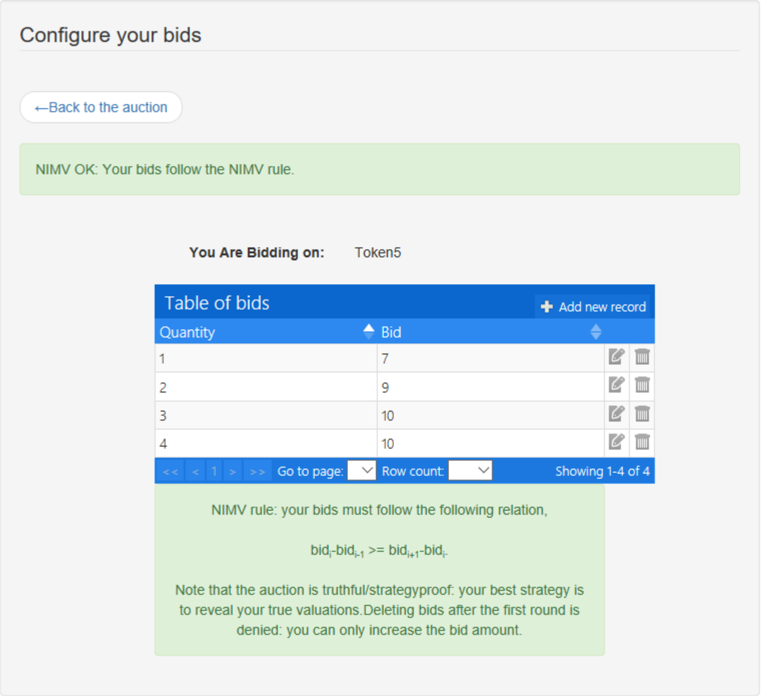


Additionally, the next figure shows another timing experiment, this time varying the number of tokens to be auctioned while maintaining fixed the number of bidders (1000) and the final price (2).



4.1 Web implementation

A PHP/AJAX implementation of the web interface will be open-sourced at `https://github.com/Calctopia-OpenSource`. Its bidding page is as follows:



Configure your bids

NIMV OK: Your bids follow the NIMV rule.

You Are Bidding on: Token5

Table of bids

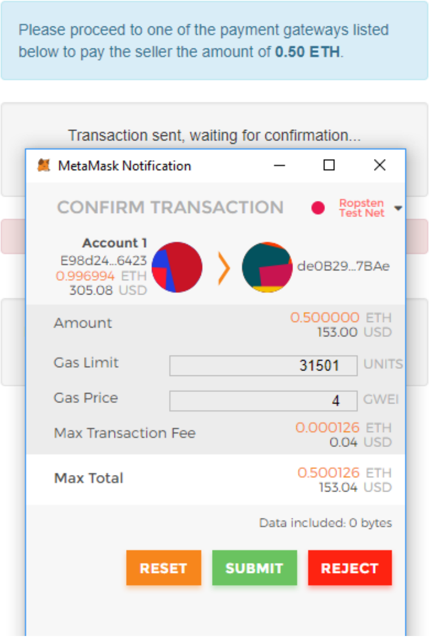
Quantity	Bid
1	7
2	9
3	10
4	10

NIMV rule: your bids must follow the following relation,

$bid_i - bid_{i-1} >= bid_{i+1} - bid_i$.

Note that the auction is truthful/strategyproof: your best strategy is to reveal your true valuations.Deleting bids after the first round is denied: you can only increase the bid amount.

And its payment page is as follows:



Please proceed to one of the payment gateways listed below to pay the seller the amount of **0.50 ETH**.

Transaction sent, waiting for confirmation...

MetaMask Notification

CONFIRM TRANSACTION

Account 1
E98d24...6423
0.996994 ETH
305.08 USD

de0B29...7BAe

Amount	0.500000 ETH 153.00 USD
Gas Limit	31501 UNITS
Gas Price	4 GWEI
Max Transaction Fee	0.000126 ETH 0.04 USD
Max Total	0.500126 ETH 153.04 USD

Data included: 0 bytes

References

[AC98] Lawrence M. Ausubel and Peter Cramton. Auctioning securities, 1998. http://ausubel.com/auction-papers/98wp-auctioning-securities.pdf.

[AE13] Tommy Andersson and Albin Erlanson. Multi-Item Vickery-English-Dutch Auctions. Working Papers 2012:17, Lund University, Department of Economics, 2013. http://project.nek.lu.se/publications/workpap/papers/WP12_17.pdf.

[Ana05] Anita Indira Anand. Is the Dutch auction IPO a good idea. *Stan. JL Bus. & Fin.*, 11:233, 2005. https://www.researchgate.net/profile/Anita_Anand/publication/228218169_Is_the_Dutch_Auction_IPO_a_Good_Idea/links/00b4952176b18caef3000000/Is-the-Dutch-Auction-IPO-a-Good-Idea.pdf.

[Aus02] Lawrence M. Ausubel. Implications of Auction Theory for New Issues Markets. Center for financial institutions working papers, Wharton School Center for Financial Institutions, University of Pennsylvania, 2002. https://core.ac.uk/download/pdf/6649749.pdf.

[Aus04] Lawrence M. Ausubel. An efficient ascending-bid auction for multiple objects. *AMERICAN ECONOMIC REVIEW*, 94(5), 2004. http://ausubel.com/auction-papers/efficient-ascending-auction-aer.pdf.

[BBR02] Bruno Biais, Peter Bossaerts, and Jean-Charles Rochet. An Optimal IPO Mechanism, 2002. https://www.jstor.org/stable/2695955.

[BF04] Moez Bennouri and Sonia Falconieri. The Optimal Design of IPOs: Price vs. Quantity Discrimination, 2004. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=491002.

[BF08] Moez Bennouri and Sonia Falconieri. The Optimality of Uniform Pricing in IPOs: An Optimal Auction Approach, 2008. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1289175.

[BFC02] Bruno Biais and Anne Marie Faugeron-Crouzet. IPO Auctions: English, Dutch,... French, and Internet. *Journal of Financial Intermediation*, 11(1):9–36, 2002. https://www.sciencedirect.com/science/article/pii/S1042-9573%2801%2990319-5.

[BGP16] Joy Buchanan, Steven Gjerstad, and David Porter. Information Effects in Uniform Price Multi-Unit Dutch Auctions. *Southern Economic Journal*, 83(1):126–145, 2016. http://onlinelibrary.wiley.com/doi/10.1002/soej.12145/full.

[BK87] Michael Brennan and Alan Kraus. Efficient Financing under Asymmetric Information. *Journal of Finance*, 42(5):1225–43, 1987. http://onlinelibrary.wiley.com/doi/10.1111/j.1540-6261.1987.tb04363.x/full.

[BLS12] Paul Belleflamme, Thomas Lambert, and Armin Schwienbacher. Crowdfunding: Tapping the Right Crowd, 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1578175.

[BOP15] Paul Belleflamme, Nessrine Omrani, and Martin Peitz. The Economics of Crowdfunding Platforms, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2585611.

[But17] Vitalik Buterin. Analyzing Token Sale Models, 2017. http://vitalik.ca/general/2017/06/09/sales.html.

[BV11] Stefano Bonini and Olena Voloshyna. A, B or C? Experimental Tests of IPO Mechanisms, 2011. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=972208.

[CF99] Thomas Chemmanur and Paolo Fulghieri. A Theory of the Going-Public Decision. *Review of Financial Studies*, 12(2):249–79, 1999. https://www2.bc.edu/thomas-chemmanur/phdfincorp/MF891%20papers/Chemmanur%20and%20Fulghieri%20RFS%201999.pdf.

[CG89] George M Constantinides and Bruce D Grundy. Optimal Investment with Stock Repurchase and Financing as Signals. *The Review of Financial Studies*, 2(4):445–465, 1989. https://www.jstor.org/stable/2962064.

[CGY10] Archishman Chakraborty, Simon Gervais, and Bilge Yilmaz. Security Design in Initial Public Offerings. *Review of Finance*, 15(2):327–357, 2010. https://faculty.fuqua.duke.edu/~sgervais/Research/Papers/WinnersCurse.RoF.pdf.

[Cha15] Jen-Wen Chang. The Economics of Crowdfunding, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2827354.

[Cho05] Eugene Choo. Going Dutch: The Google IPO. *Berkeley Technology Law Journal*, pages 405–441, 2005. http://www.btlj.org/data/articles2015/vol20/20_1_AR/20-berkeley-tech-l-j-0405-0442.pdf.

[Cou46] United States Supreme Court. SECURITIES AND EXCHANGE COMMISSION v. W. J. HOWEY CO. 1946. http://caselaw.findlaw.com/us-supreme-court/328/293.html.

[CRS82] James C Cox, Bruce Roberson, and Vernon L Smith. Theory and behavior of single object auctions. 1982. http://www.excen.gsu.edu/jccox/research/SingleObjectAuctions.pdf.

[CY11] Archishman Chakraborty and Bilge Yilmaz. Adverse Selection and Convertible Bonds. *Review of Economic Studies*, 78(1):148–175, 2011. http://www.jstor.org/stable/23015851.

[DDW10] François Degeorge, François Derrien, and Kent Womack. Auctioned IPOs: The US evidence. *Journal of Financial Economics*, 98(2):177–194, 2010. https://pure.uvt.nl/portal/files/1096383/2009-08S.pdf.

[DW03] François Derrien and Kent Womack. Auctions vs. Bookbuilding and the Control of Underpricing in Hot IPO Markets. *Review of Financial Studies*, 16(1):31–61, 2003. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.322.2150&rep=rep1&type=pdf.

[EH16] Matthew Ellman and Sjaak Hurkens. Optimal Crowdfunding Design, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2507457.

[GH89] Mark Grinblatt and Chuan Yang Hwang. Signalling and the Pricing of New Issues. *Journal of Finance*, 44(2):393–420, 1989. https://www.jstor.org/stable/2328596.

[GT05] Rod Garratt and Thomas Tröger. Speculation in Standard Auctions with Resale, 2005. https://epub.ub.uni-muenchen.de/13506/1/42.pdf.

[KK08] Elena Katok and Anthony Kwasnica. Time is money: The effect of clock speed on sellers revenue in Dutch auctions. *Experimental Economics*, 11(4):344–357, 2008. http://www.personal.psy.edu/amk17/TimeIsMoney_onlineversion.pdf.

[KLZ15] Praveen Kumar, Nisan Langberg, and David Zvilichovsky. (Crowd)funding Innovation, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2600923.

[KSW99] Shmuel Kandel, Oded Sarig, and Avi Wohl. The Demand for Stocks: An Analysis of IPO Auctions. *Review of Financial Studies*, 12(2):227–47, 1999. http://finance.wharton.upenn.edu/~sarig/sarigo/demand.pdf.

[Lis16] Matt Liston. Introducing the Gnosis Token Launch, 2016. https://blog.gnosis.pm/introducing-the-gnosis-token-launch-3cc4cffb5098.

[LRBC$^+$99] David Lucking-Reiley, Ann Bell, Jim Cox, Rachel Croson, Ron Harstad, Elton Hinshaw, John List, and Preston Mcafee. Using Field Experiments to Test Equivalence between Auction Formats: Magic on the Internet. *Magic on the Internet. American Economic Review*, 89:1063–1080, 1999. http://www.davidreiley.com/FieldExperimentsCourse/papers/FullReadingList/LR-RevenueEquivalence.pdf.

[Mag17] WINGS Magazine. A Gnosis Dutch Auction for All? Coming to the WINGS Smart Contract Library, 2017. https://blog.wings.ai/a-gnosis-dutch-auction-for-all-in-the-wings-smart-contract-library-92b7b698fa9a.

[Mal05] Alexey Malakhov. The Role of Uninformed Investors in an Optimal IPO Mechanism, 2005. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=687167.

[Mie13] Paavo Miettinen. Information acquisition during a Dutch auction. *Journal of Economic Theory*, 148(3):1213–1225, 2013. https://helda.helsinki.fi/bof/bitstream/handle/123456789/7609/170045.pdf.

[MP08] Debasis Mishra and David C. Parkes. Multi-Item Vickrey-Dutch Auctions, 2008. http://www.isid.ac.in/~dmishra/doc/vda.pdf.

[PS09] Pegaret Pichler and Alex Stomper. Primary Market Design: Mechanisms And When-Issued Markets, 2009. web.mit.edu/astomper/www/papers/primary.pdf.

[Roc86] Kevin Rock. Why new issues are underpriced. *Journal of Financial Economics*, 15(1-2):187–212, 1986. https://www.sciencedirect.com/science/article/pii/0304405X86900541.

[RR12] Mary Robinson and Richard Robinson. Dutch-auction IPOs: institutional development and underpricing performance. *Journal of Economics and Finance*, 36(3):521–554, 2012. https://link.springer.com/content/pdf/10.1007/s12197-010-9166-3.pdf.

[SC17a] Securities and Exchange Commission. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. 2017. https://www.sec.gov/litigation/investreport/34-81207.pdf.

[SC17b] Securities and Futures Commission. Statement on Initial Coin Offerings, 2017. http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR117.

[Sha17] ShapeShift. ShapeShift and Tokens as Securities, 2017. https://info.shapeshift.io/blog/2017/08/17/shapeshift-and-tokens-securities.

[STA17] ICO STATS. ROI Since ICO, 2017. https://icostats.com/roi-since-ico.

[Sun17] Alex Sunnarborg. ICO Investments Pass VC Funding in Blockchain Market First, 2017. https://www.coindesk.com/ico-investments-pass-vc-funding-in-blockchain-market-first/.

[TL08] Andreas Trauten and Thomas Langer. Why the Google IPO Might Stay Exotic-An Experimental Analysis of Offering Mechanisms. 2008. http://www.efmaefm.org/0EFMSYMPOSIUM/2008-Oxford/papers/Andreas%20Trauten.pdf.

[Tok17] TokenData. Introducing TokenData.io, 2017. https://medium.com/blockchannel/introducing-tokendata-io-dcd26d9fbc1e.

[Van03] Sigrid Vandemaele. Choice of Selling Mechanism at the IPO: the Case of the French Second Market. *European Financial Management*, 9(4):435–455, 2003. http://onlinelibrary.wiley.com/doi/10.1111/1468-036X.00231/abstract.

[Wil09] Linus Wilson. The Biggest Warrant Auction in US History. 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1521335.

[Zha17] Wolfie Zhao. China's ICO Ban: A Full Translation of Regulator Remarks, 2017. https://www.coindesk.com/chinas-ico-ban-a-full-translation-of-regulator-remarks/.

A Auction Implementation

```
// parameters
n = 4; // number of units
m = 3; // number of buyers
max_t = 9; // starting high price
q[max_t+2]; q[0] = max_t+1;
v[n][m] = 0; // marginal values; note that v_i(0) = 0 for all i
v[0][0] = 0; v[1][0] = 7; v[2][0] = 9; v[3][0] = 10; v[4][0] = 10;
v[0][1] = 0; v[1][1] = 8; v[2][1] =13; v[3][1] = 15; v[4][1] = 15;
v[0][2] = 0; v[1][2] = 4; v[2][2] = 8; v[3][2] = 10; v[4][2] = 10;


//arrays and variables
d[m] = 0; // demand
d_previous[m] = 0; // copy of previous demand
c[m] = 0; // units clinched
r[m] = 0; // residual demand
r_previous[m] = 0; // copy of previous residual demand
s[m] = 0; // payments to buyers
old_sum_demands = 0;
sum_demands = 0;
t_m = 0;
seqEconomyCalculated = false;


for (t = 0; t < max_t+1; t++) {
  if (t>0) // save a copy of previous demand
    d_previous.copyFrom(d);
  if (seqEconomyCalculated) // save a copy of previous residual demand
    r_previous.copyFrom(r);

  // (S1.1) calculate maximal demand for step t
  for (int i = 0; i < m; i++) {
    if ((v[1][i] - v[0][i]) < q[t]) {
      d[i] = 0;
    } else {
      int max_j = 0;
      for (int j = 1; j < n; j++)
        if (v[j][i] - v[j-1][i] >= q[t])
          if (j > max_j)
            max_j = j;
      d[i] = max_j;
    }
  }
```

```
// (S1.2)
old_sum_demands = sum_demands;
sum_demands = 0;
for (int i = 0; i < m ; i++)
  sum_demands += d[i];
if (sum_demands < n) {
  for (int i = 0; i < m ; i++)
    c[i] = d[i];
  q[t+1] = q[t] - 1;
  continue; // goto (S1.1)
}
//(S1.3) -> CE of the main economy
if (sum_demands >= n && old_sum_demands < n) {
  t_m = t; // now residual demands can be calculated
  if (!seqEconomyCalculated) { // set c_i to be any sequential allocation
    int sum_dprevious = 0;
    for (int i = 0; i < m; i++) {
      c[i] = d_previous[i]; sum_dprevious += d_previous;
    }
    if (sum_dprevious < n) {
      int toBeAssigned = n - d_previous;
      bool everyoneClinched = False;
      while (toBeAssigned > 0) {
      if (!everyoneClinched) {
        for (int i = 0; i < m; i++) {
          if (c[i] == 0) {
            if (toBeAssigned > d[i]) {
              c[i] += d[i]; toBeAssigned -= d[i];
            } else {
              c[i] += toBeAssigned; toBeAssigned = 0;
            }
          }
        }everyoneClinched = True;
      }
        int randBuyer = rand(0, m); int demanded = d[randBuyer];
        if (c[randBuyer] < demanded)
          if (toBeAssigned > demanded) {
            c[randBuyer] += demanded; toBeAssigned -= demanded;
          } else {
            c[randBuyer] += toBeAssigned; toBeAssigned = 0;
          }
      }
    }seqEconomyCalculated = true;
  }
}
```

```
  // calculate residual demand
  if (t >= t_m) {
    for (int i = 0; i < m; i++) {
      int sumDemands = 0;
      for (int j = 0; j < m; j++) {
        if (i != j) {
          sumDemands += d[j] - c[j];
        }
      }
      if (c[i] < sumDemands)
        r[i] = c[i];
      else
        r[i] = sumDemands;
    }
  }

  //(S1.4) calculate payments
  for (int i = 0; i < m; i++) {
    s[i] = s[i] + (q[t] * (r[i] - r_previous[i]));
  }

  //(S1.5)
  bool allEqual = true;
  for (int i = 0; i < m; i++) {
    if (r_i != c[i]) {
      allEqual = false;
      break;
    }
  }
  if (allEqual)
    break;
  if (q[t] == 0)
    break;

  q[t+1] = q[t] - 1;
}
// final allocation in c[m], final payment vector in s[m]
```