NOT a TON Binary System

By Mitja Goroshevsky and Andrey Lyashin

Abstract

Cryptocurrency's main use case is a store of value and participation in the success of the smart contract platform. Token stability is a separate use case that can not be realized within the framework of the same token. We propose a binary system design where interaction between two tokens, the native cryptocurrency of Free TON platform and a stablecoin backed by it, guarantees the price stability of the latter and allows for algorithmic monetary policy of the former.

I. The Money

Money's a matter of functions four,
A Medium, a Measure, a Standard, a Store
— Alfred Milnes[1]

According to the current economic teachings, money has three main characteristics: medium of exchange, unit of account, and store of value. This definition may be correct 100 years ago. Today it is nothing but a lie[2]. From 1913, when the first inflation measurement was taken the US Dollar lost 26 times its value, meaning you need $26 today to buy something you could for just $1 a hundred years ago. This is hardly a store of value. Yet the US Dollar became a world reserve currency and used as a global medium of exchange and unit of account. It is worth mentioning that the US Dollar lost its "store of value" property long before the gold standard was abandoned in 1980 as it has already lost 7 folds its 1913 buying power.

In fact it would be probably correct to say, that the money in the modern economy must gradually lose its value in order to be an attractive medium of exchange. Quite simply when a person holds on to something that loses its value over time, it will most likely try to exchange it with something more valuable. Such a person would not hesitate going to a shop and buying not only things they dearly need, such as pizza, but also things they need not so much, such as entertainment, or things they don't need at all, such as a new phone.

Most of the traditional economists understand a value losing property of the money as one of its key properties. After all, the Federal Reserve conducts its inflationary monetary policies not as an act of complete loonacy. Yet, when in 2008 Bitcoin was created, it seems that Satoshi Nakamoto did not fully realise the main use case of the thing he himself created. In the opening sentence of his otherwise brilliant white paper they write: "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."

[1] Milnes, Alfred (1919). *The economic foundations of reconstruction*. Macdonald and Evans. p. 55
[2] Mankiw, N. Gregory (2007). "2". *Macroeconomics* (6th ed.). New York: Worth Publishers. pp. 22–32. ISBN 978-0-7167-6213-3.

We have an exact date and a name of the person who has proven Satoshi wrong. On May 22, 2010, known now as “Bitcoin Pizza Day”, Laszlo Hanyecz has bought two pizzas[3] from his local Papa John's. In today’s prices this pizza is worth ~$ 400,000,000.

If the US dollar is quite hardly a store of value, Bitcoin is most definitely not a medium of exchange. Quite simply one would probably try to hold on to something that appreciates in value over time, rather than buying even things they dearly need, not talking about pizza.
Unfortunately it seems the idea of trying to make cryptocurrency a “proper money” has been dominating minds of crypto enthusiasts all that time. If Bitcoin developers would understand economics they would not propose something like lightning network[4] in the first place. You should be really crazy to buy a cup of coffee that could be worth millions in the next few years.

There is now a whole range of different cryptocurrency projects with all sorts of money supplying models. Some following Bitcoin with highly restricted monetary policy, some will mint coins over time with something that would resemble a 2% inflation target of US Federal Reserve[5]. This is probably the reason Nikolai Durov in the first TON Whitepaper proposes a 2% emission target for TON blockchain[6]. We believe all these approaches are quite opportunistic and are not based on a sound economical model. There is no way an asset can be both a store of value and a medium of exchange at the same time. If so, why would someone propose an inflationary target for store of value or trying to constantly increase the asset value to encourage its use as a medium of exchange?

The predominant use of cryptocurrency today is a store of value. With the introduction of smart contracts in particular and the notion of a distributed verifiable computation, in general, additional use of the native platform cryptocurrency started to emerge. When a developer is contributing to the code of one of those smart contract platforms, they effectively become participants in the success of that platform. Holding the native token and developing applications on the underlying platform make such a developer an active participant, which in turn produce more use cases. This is clearly indicated by the DeFi movement, for instance. Naturally, these use cases are related mostly to investment. Indeed, smart contracts introduce a possibility to extract further value from an asset one stores on the blockchain, without a need to sell it. This falls within the concept of value storage perfectly. The stability of an asset and required for such stability lack of volatility — does not. Thus for many use cases, which require a stable medium of exchange, the basic property of blockchain’s native token represents a limiting factor. In fact for most use cases where a consumption is a centerpiece, for instance paying someone for performing a work.

---

[3] https://bitcointalk.org/index.php?topic=137.msg1195#msg1195
[4] https://ln.pizza/
[5] https://www.federalreserve.gov/faqs/economy_14400.htm
[6] Nikolai Durov, https://test.ton.org/ton.pdf A.3. Original supply, mining rewards and inflation, p. 128

This limitation has been one of the leading driving factors for creation of a cryptocurrency pegged to some real life asset price. Usually to the US dollar.

There are two types of Stable Coin designs used today: one is a stable coin backed by real world assets, such as USDT and another, such as Maker DAO — backed by cryptocurrency itself.

We do not consider a stable coin backed by real assets to be of any interest. Generally speaking they are just as bad as having coins on centralized exchanges. They are completely untransparent, centralized, bulky and generally suck.

Of the cryptocurrency backed stable coins, all of them require separate governance tokens and over collateralization to provide for a catastrophic scenario of dramatic price fall of their reserve asset. They rely heavily on 3rd parties to provide an oracle data feed of current prices, which represents an attack vector and a point of failure, regardless of how good the oracle network is.

In general the approach is Layer 2 protocols as now fashionable in Ethereum and which we regard as not tightly-coupled which limits the level of services and security guarantees one should expect from a modern blockchain system.

In this work we not only propose a mechanism of a stable coin, but a monetary system of two interconnected coins within a Free TON blockchain that will enable both use cases: the store of value/participation and a medium of exchange. Instead of trying to sit on two chairs simultaneously let's have two chairs and use them appropriately.

II. NOT a binary companion of TON

'In the presence of total Darkness, the mind finds it absolutely necessary to create light.'
— Isaac Asimov[7]

Let's consider an economic system of two interconnected native tokens[8] on Free TON. TON — the native cryptocurrency of Free TON blockchain and NOT — a reverse native currency, with the opposite properties of its binary companion. TON would be used as a store of value, or as an "asset" and NOT as a stable currency, or "money".

Let's think of both TON and NOT as native tokens for two separate yet interconnected blockchains, where dynamics of user behavior in one can influence some parameters of another — much like in planetary binary systems[9].

TON token security is ensured by validators submitting stakes which are locked for a period of time. The validators create, submit and come to a consensus about blocks on the Free TON blockchain. They are incentified to do this work and put a stake because of the commissions and fees they earn from the network. Validators also incentified to run DePools, which can earn them even more commissions for stakes other people add. Most important metric for a decision to stake with TON is the gain users make on their investment. Usually they measure this gain in US Dollars.

Let's imagine NOT also having validators. Let's call them "NOT the Validators". Instead of blocks NOT the Validators will create, submit and come to a consensus about prices of the TON/USD pair in the outer world. Let's call them "NOT the blocks". They will transfer their stake in TON DePools to the Issuer smart contract (let's call it NOT the Elector, of course) for the duration of their stake in TON. Once submitted those stakes will participate in elections to become NOT a Validator in NOT the Elector smart contract. Much like the Elector smart contract, the stake they transfer to NOT the Elector can be "slashed" if the validator is providing wrong data to NOT the blocks. More on that later.

---

[7] Isaac Asimov, Nightfall

[8] Nikolai Durov, https://test.ton.org/ton.pdf 2.1.18. TON coins and multi-currency workchains.

[9] https://en.wikipedia.org/wiki/Binary_system

It is worth mentioning that while transferred to NOT the Elector smart contract TON stakes will continue earning rewards in TON blockchain. The motivation to become NOT the Validator is that on top of these rewards NOT the Validators will earn a commission on all NOTs that will be issued. Thus the Validator of TON blockchain can now effortlessly become NOT the Validator and earn additional rewards. Of course technically it means connecting their node to a data feed from some exchanges and supplying the correct data to NOT the Elector. In fact we can not care less how the prices ending up in NOT the Blocks, as long as this data is correct.

Now let's consider a user which holds some TONs would like to exchange them for a stable coin on TON blockchain. In order to accommodate the user we will create a couple of special smart contracts called, NOT the Auction and D'Auction respectfully. A user can go to one of them and demand NOTs for their TONs. We will discuss below the exact mechanism of issuing the NOTs, but for now let's just say that after certain procedure NOTs will be issued in exchange for TONs using the precise exchange rate from the outside data feed provided by NOT the Validators.

It is important to mention that when buying NOTs, there will be no need for overcollaterization. Let's stop here for a brief moment because this point is one of the most important illustrations of the proposed binary system. Usually when creating a completely separate stable coin with algorithmic design, such design requires a protection mechanism for the scenario when the prices for underlying cryptocurrency are rapidly and violently falling. In fact the same problem exists for stable coins backed by fiat currency reserves, such as USDT. But because of the untransparent nature of the latter it is impossible to say when and under which conditions such stable coins may become insolvent. Bottom line, all of the current designs require some assets overcollaterization because the assets they take as a collateral are not under their control. In the real world economy the stability of money (or at least the stability of inflation of money should we say) is ensured by the monetary policy of some authority which controls the supply of said money.

One of the reasons for proposed binary system designs is precisely the fact that here we do have control over TON monetary policy and we intend to use it.

In order to achieve stability in case of a disaster we should share some of the "gravitational" force of TON with its NOT companion. Namely a large portion of TONs should be provided to the NOT system as a stabilisation fund. Say, 1 bln tokens. One can remember that it does resemble the idea of Nikolai Durov expressed in his TON White Paper[10]. Except this time the stabilisation fund will not intervene in price stabilisation per se, nor it will do it to stabilize the native TON cryptocurrency, a very wrong idea as discussed above. Instead it will be used as a collateral to fulfill the obligations of NOT in case of dramatic drop in the prices of TON.

[10] Nikolai Durov, https://test.ton.org/ton.pdf A.4.1. Exponentially priced cryptocurrencies

We argue that such use of TON reserves is prudent and will not create a further pressure on TON price in case of a catastrophe.

Let's come back to the user which just exchanged his TONs with NOTs using a precise pricing mechanism of NOT the Elector. TONs that the user has exchanged for NOTs will now be used to give back to the TON by staking this in the DePool on behalf of NOT the Elector. The rewards from staking will be split in half: one half distributed to NOT the Validators proportionally to their stakes and another half will go to the TON Reserve as a payment for providing collateral.

Additional points of interconnectivity between TON and NOT could be a use of some NOT metrics within the TON system. For example an increase in supply of NOTs can indicate the need to increase the validator rewards. This will allow dynamic block reward adjustments, making it more attractive for users to stake TONs in DePool, instead of holding NOTs. This by itself will decrease the market supply and increase the price of TONs on the open market. Such mechanisms will realise the main idea of the binary system design — to create two tokens with different use cases while measuring interactions between them to allow algorithmic monetary governance.

Let's also view the proposed system from the standpoint of real market participants. Most of the stable coin designs recognise today three types of users: one that wants stabilisation of its asset, aka risk-free, one that is looking for income with relatively low risk and the one which is looking to maximise its revenue potential with high risk investments. In this paper we mostly consider two users: one that is looking for stabilisation for which they are buying NOTs in exchange for TONs, and the validator, who is looking for additional income on its capital. But of course it is easy to imagine that a derivatives market can be created on top of our Binary System which will accommodate most users' appetite for risk and high yield.

The derivatives market in its turn helps to adjust the gathered pricing contract utilizing the inversing of Black Scholes equation : $C = S_t N(d_1) - Ke^{-rt}N(d_2)$ which can be considered as a relation for S_t and solved with respect to it. Feeding the system with correct (market) values of realized deals (strong data) and proposed prices (weak data) allows therefore to estimate the price estimation (which is smoothed by derivatives effect).

III. NOT The Elector

> "The observed outcome may be one that everybody prefers, it may be one that nobody prefers, or it may be one that some prefer and others deplore."
>
> — Thomas C. Schelling

NOT the Elector contract is designed to collect the external TON/USD pricing value and is permanently running and therefore collects the data in an instant way. But the collecting is made in an encrypted way. The revealing mechanism is not performed on each data collection.

Quotation is made based on a decentralized and blind (sealed bidded) scheme by NOT the Validators. This ensures no one of the validators is aware of the quotes made by others in the commit-reveal scheme as discussed below. More sophisticated ZKP algorithms could also be implemented to raise the non-disclosure properties.

At a computationally unpredicted (cryptographically random) moment the check of then given prices is performed. That is, all the data is to be revealed by submitters, and then checked with the given hash (commit) and analyzed. The correct in just mentioned sense values are considered as the initial price set. Those participants who cannot correctly reveal the data are considered as pre-malicious.

Those participants whose values lie between 25^{th} and 75^{th} quartile are considered as honest and are rewarded. Those participants who feed the outlying data are considered as pre-malicious with some cumulative rank and they lose the current reward which goes to the honest participants with respect to this rank.

So let rank r be a number in $[0,1]$ real valued interval. We set that $r = 0$ corresponds to the honest participant and $r = 1$ to a malicious one. Initially all participants have $rank = 0$. With the given rank the reward is calculated as $(r-0.5)*r_0$ where r_0 is the reward for an honest participant.

The rank is updated as follows: new rank is $r' = r*(1-a) + a*r_c$, where r is old rank, a - some constant in $[0,1]$ and r_c - the rank of the currently analyzed feed. r_c is calculated based on the difference between median value which is assumed as consensus value (see also explanations below) and given by the current participant.

$$\begin{cases} r_c = 0, \text{ for } v_{25} < v < v_{75}; \\ r_c = 1\text{-}P\,(v_i < v), \text{ for } v \le v_{25}; \\ r_c = 1\text{-}P\,(v_i > v), \text{ for } v \ge v_{75} \end{cases}$$

where $P\ (v \in V)$ is the empirical probability that some random vi from the current price set lies in the interval V. So $1 - P\ (v_i > v) \longrightarrow 1$ with v -> *"max given number"* and the same way $1 - P\ (v_i < v) \longrightarrow 1$ with $v \longrightarrow$ *"min given number"*. v_{25} and v_{75} correspond to the edges of the honesty interval defined above. The iterative relation $r' = r*(1-a) + a*r_c$ accumulate "errorness" of the feed with some rate a. The rate can be understood if we suggest the constant values i.e.

$$\begin{cases} r_0 = 0 \\ r_{n+1} = r_n*(1-a) + r_c*a \\ \\ r_n \longrightarrow r_c \text{ if } n \longrightarrow \infty \end{cases}$$

Besides this, the validator is banned forever (excluded from the validators' set) if it has *undecreased rank* > *0.5* during certain number of checks. Note that if the validator would give the correct answers its rank will be instantly decreasing as $a < 1$ and therefore before it gets the total ban it could potentially clear the cumulative malicious rank.

Refusing to feed the price value is considered the same as feeding data with some constant rank which is a subject to determine based on convergence experiments on the pre-implementation (PoC) phase.

We realize that the quotation can be performed in an automatic or semiautomatic way, e.g. by feeding the contract with the real deal prices from any exchange they trust. That in particular means that they cannot verify each feeded value on each step and therefore permanently punish them for "incorrect" price would be unfair. And that is why we give them the pre-malicious status as a kind of warning to check their systems. On the warning they can stop all feeding processes and fix them.

In the case when Schelling mechanism cannot provide single price (e.g. multimodal distribution) or when the normality check fails the quoting contract can

- provide a series of values (activating a correspondent number of auctions);
- refuse to provide any value, adjusted all participants with a certain rank (is a subject to investigate during the PoC);

- in the case of multiple values, the winner auction ranks the losing modes with a certain rank of suspiciousness.

Incentivization to make a quote should take the following aspects into account:

1. Quote makers are to be incentivized to make a quote - that is to feed the protocol with some information (the price value in our case).
2. They are to be incentivized to feed a correct quote - that is the given price value should be close to real market price as much as possible.

We assume that quote makers are incentivized to do their job by the following reasons:

1. To stabilize network common consensus
2. To make the NOT issuing justified and reasonable
3. To bring the correct economic characteristics in the system
4. Not to lose the validators reward
5. Not to lose their stake at all
6. To gain rewards from stakes made with TONs from NOT the Auction
7. To gain extra reward when suspicious participants slashed

To perform consensus on the given data the Schelling point mechanism is proposed. It had been originally introduced in 1960 by Thomas Schelling in his book “The Strategy of Conflict”[11] and basically is used to represent the method to acquire the common knowledge which is based on unbiased human behaviour in an informationally symmetric world (which we assume as the working case).

We use the same notions and ideas which originally come from Vitalik Buterin[12] and roughly repeat the main steps of the quoting protocol (based on commit-reveal scheme):

1. During each block, all participants can submit a salted hash of the TON/USD price together with their TON address (commit).
2. During the quoting phase (as well as the check phase, see above), users can submit the value and salt whose hash they provided at the previous stage (reveal).
3. Define the “correctly submitted values” as all values N where Hash (N+ADDR+Salt) was submitted in the first block and N was submitted in the second block, both messages were signed/sent by the account with address ADDR and ADDR is one of the allowed participants in the system.
4. Sort the correctly submitted values.

[11] https://www.amazon.com/Strategy-Conflict-New-Preface-Author/dp/0674840313
[12] V.Buterin. SchellingCoin: A Minimal-Trust Universal Data Feed.
https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed, 2014.

5. Every user who submitted a correct value between the 25th and 75th percentile gains a reward of a certain amount of TON which is collected from the suspicious participants.
6. The quoting phase makes the same procedure for suspicious and malicious accounts as at the check phase.

As mentioned in the same paper, “the protocol does not include a specific mechanism for preventing sybil attacks; it is assumed that proof of work, proof of stake or some other similar solution will be used” (Proof Of Stake in the Free TON case).

The current final price estimation is basically calculated as the median value of the correct dataset. It is later used in auction contracts (the consensus value is a subject to adjust if anomalies have been observed in distribution shapes and parameters).

IV. NOT The Auction

Let him look to his bond.
— William Shakespeare[13]

When the price is determined (it is being determined instantly) the auctions can be performed. We assume two kinds of auction: direct (NOT/TON), reverse (TON/NOT) and their decentralized variants which we note as dAuctions (analogous to dePool).

The main arguing and counter arguments for using the Schelling schemes based on the idea of collusion attacks. That can be a case if the quote makers are biased in their incentives to make correct quotes or live in an asymmetrically conjoined worlds (the latter is not a case as all procedures on the blockchain are symmetrically open for all users). And that is why we propose the auction mechanism to verify the quotations made on the previous step. To re-verify, to be more precise.

We propose the following scheme:

1. Auction is performed on demand with a minimum lot size. It sells as many NOTs as demanded by the winners but filtering participants by the required amount (one cannot participate if bids valued smaller than given).
2. It is designed as Vickrey auction (sealed-bid, second price).
3. The bids sealing is also performed by the commit-reveal scheme similar to the one mentioned above.
4. It has the predefined zero position based on quoting result, so that the winner must submit the bid higher (or same) than quoting price.
5. The quoting price should not be disclosed before the auction starts.
6. The winner address, winning and paid (second) price are disclosed at the end of auction.
7. If no one wins, the auction is considered as failed and the lot is not sold.
8. Auction is paid, and the payment is to go to the validators, and as a payment for larger liquidity (because of minimum lot value).
9. After the auction every participant can buy the desired amount of NOTs by the price determined at the last auction increased by some factor.

We assume that validators are unbiased in their opinion unless they could conspire for some non market reward (bribe). If some potential auction participant bribes the validators at the quoting phase to make the TON/USD price higher to buy NOT cheaper and she wins, then they

[13] The Merchant of Venice (Shylock, Act 3 Scene 1)

will indirectly decrease the TON collateral backing NOT which harms the system which they validate.

In contrast — if they for some reason conspire to agree on a lower TON/USD price, which makes the NOT/TON price higher, there will be no winners in auction, which will locally stop the economic process. So in general the validators have incentives to keep the consensus price close to real market value to:

1. Establish the correct backing of the NOTs
2. To let NOT issuing be performed in proper way

D'Auction

D'Action contract is designed to be the mechanism to allow users with limited amounts of buying power to take part in the auction using the accumulated potential. They can organize the group of players to represent the single auction participant accumulating their demands to reach the restrictions for making bids. That is made in a very analogous way dePools are designed.

The contract contains the following roles:

1. Aggregator (representor). Account which owns the dAuction contract. It's obligations include making a proper bid (which should be not less than a certain percentage of cumulative buying demand), making a bid in a main auction at proper time.
2. Participant. Account which gives the contract rights to bid from her name acting together with aggregator
3. Contract itself. Accumulates the bids in a proper way, allows the representor to make a price bid, sends the bid to the auction contract, pays all correct fees, collects the results and distributes the won lot between them all and returns or rebids the original bids if the contract loses the auction.
4. The aggregator and participants buy price is finally adjusted by their amounts and roles (aggregator has some additional benefits as a reward for being a representor)

All the D'Auction constants are subject to be determined at implementation phase and should establish adequate incentives for all players.

dAuction can be performed once or at an instant (until win) way. If some participant exists the dAuction decreasing total buy potential less than minimum lot size, D'Auction needs to find new participants to fit the requirements. If D'Auction wins it distributes the bought lot and closes.

The D'Auction participants in any way should have more benefits than any user in the after auction phase to incentivize participants to enter it.

As the D'Auction representor should not be a validator no punishment mechanism is currently proposed as well as no reputation is recorded as we suggest that the new auction allows participants to reorganize in a new D'Auction.

The list of currently available open D'Auction should be also available with all important parameters transparently given to let newcomers easily choose and participate based on their internal preferences.

The duration of D'Auction non-winning lifetime can also be specified in advance, after which D'Auction is closed and returns the collected bids back independently on status.

V. Conclusion

- We have introduced above a tightly-coupled system of two tokens, the native Free TON currency TON and its binary companion NOT stable currency. As a consequence the system does not require any additional governance, since all its actions are governed by smart contracts or, whenever necessary, it relies on TON native token governance and security guarantees.
- The proposed system allows us to have two native Free TON cryptocurrencies, one for each of the basic use cases: the store of value/participation and the medium of exchange stable coin.
- The prices are provided by Free TON DePool participants and validated using the adjusted Schelling mechanism, adding suspiciousness ranking, slashing algorithm, distribution properties analysis and secondary after auction corrections both for consensus value and slashing adjustments.
- The incentive scheme is proposed allowing validators to earn extra income on the same stake.
- The system uses TON reserves as a virtually unlimited guarantee for NOT, therefore no overcollaterization is necessary.
- The Vickery auction mechanism for price control and qualification is used for NOT purchases and the reverse Black Scholes price discovery equation is used for NOT derivatives.

Additional bibliography

1. Verifiable Sealed-Bid Auction on the Ethereum Blockchain by Hisham S. Galal and Amr M. Youssef, https://eprint.iacr.org/2018/704.pdf
2. SchellingCoin: A Minimal-Trust Universal Data Feed, Posted by Vitalik Buterin on March 28, 2014, https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/
3. Nash Equilibria and Schelling Points, by Scott Alexander, https://www.lesswrong.com/posts/yJfBzcDL9fBHJfZ6P/nash-equilibria-and-schelling-points
4. The Power of Focal Points Is Limited: Even Minute Payoff Asymmetry May Yield Large Coordination Failures by Vincent P. Crawford, Uri Gneezy, and Yuval Rottenstreich, https://rady.ucsd.edu/faculty/directory/gneezy/pub/docs/focal-points.pdf
5. Trustee: Full Privacy Preserving Vickrey Auction on top of Ethereum, by Hisham S. Galal and Amr M. Youssef, https://eprint.iacr.org/2019/102.pdf
6. Empirical Measurements on Pricing Oracles and Decentralized Governance for Stablecoins by Wanyun Gu, Anika Raghuvanshi & Dan Boneh, https://assets.pubpub.org/vnkw477p/51581338545992.pdf
7. A Smart Contract Oracle for Approximating Real-World, Real Number Values, by William George and Clément Lesaege, https://drops.dagstuhl.de/opus/volltexte/2020/11970/pdf/OASIcs-Tokenomics-2019-6.pdf
8. Secure sealed-bid online auctions using discreet cryptographic proofs by Jose A. Montenegroa, Michael J. Fischer, Javier Lopez, Rene Peralta, https://www.sciencedirect.com/science/article/pii/S0895717711004535
9. Oracle-Efficient Online Learning and Auction Design, by Miroslav Dudík, Nika Haghtalab, Haipeng Luo, Robert E. Schapire, Vasilis Syrgkanis, Jennifer Wortman Vaughan, https://www.cs.cornell.edu/~nika/pubs/main-oracle-efficient.pdf
10. An Iterative Generalized Vickrey Auction: Strategy-Proofness without Complete Revelation by David C. Parkes, https://dash.harvard.edu/bitstream/handle/1/4101696/Parkes_Iterative.pdf?sequence=2
11. Truthful and Faithful Monetary Policy for a Stablecoin Conducted by a Decentralised, Encrypted Artificial Intelligence, David Cerezo Sánchez, https://eprint.iacr.org/2019/1054.pdf