O: Provable Scarcity and a Trustless Mint Without Explicit Consensus?

Sam Williams
sam@arweave.org

Abhav Kedia
abhav@arweave.org

DRAFT-2
June 2022

Abstract

In this paper we propose a new digital currency ledger, O, for discussion. O is an experiment in digital currencies without a consensus layer. This protocol exists without work or stake. Typically, in such a consensus-free system the dominant strategy is assumed to be overwriting other node's blocks perpetually ('Greedy Mining' [1]), however we hypothesize that at some point in order for any participant's work to be credited at all they must negotiate with one another. We theorize that the Nash equilibrium of this game may in fact still be consensus, but with long latencies in the early phases and potential recurring periods of consensus change. We further observe that average confirmation latency is also likely to decline over time. If this additional consensus latency can be accepted, the resulting protocol has the following significant properties:

- Close to maximal theoretical throughput. The ledger progresses as fast as people can verify transitions, competing for greater speed.
- Incentivizes minimizing mining costs (both financial and environmental), rather than maximizing them.
- Moves consensus to the social, trust layer.
- Incentivizes the creation of faster single-thread performance chips.
- Extraordinarily simple. Almost all mechanics and properties are emergent.

1 Protocol Definition

In totality, the O protocol in pseudo-Erlang syntax is defined as follows:

```
sign_tx(PrivKey, PubKey, To, Amount, Fee) :: TX

apply(TX, RewardAddr, Ledger) ->
        L2 =
            replace(
                TX.from,
                lookup(TX.from, Ledger)
                    - TX.amount - TX.fee,
                Ledger
            ),
        L3 =
            replace(
                TX.to,
                lookup(TX.to, L2) + TX.amount,
                L2
            ),
        replace(From, lookup(From, L3) + 1, L3).

verify_transition(Ledger, RewardAddr, TX, NextLedger) ->
        (lookup(TX.from, Ledger) >= (TX.amount + TX.fee)) &&
                (lookup(TX.to, NextLedger)
                    == (lookup(TX.to, Ledger) + TX.Qty) &&
                (lookup(TX.from, NextLedger)
                    == (lookup(TX.from, Ledger) - TX.Qty - TX.fee) &&
                (lookup(RewardAddr, NextLedger)
                    == (lookup(RewardAddr, Ledger) + TX.fee + 1) &&
                crypto:verify(sigAlg, TX.PubKey, TX.sig, NextLedger).

verify(Transitions = [{_Ledger, _RewardAddr, _TX}|_]) ->
        lists:all(
            parrallel_map(
                fun verify_transition(
                    Ledger,
                    RewardAddr,
                    TX,
                    NextLedger
                ),
                Transitions
            ).
```

2 Discussion

Fundamentally, this model of digital currency differs from prior ones by embracing off-chain/out-of-protocol negotiation by the miners. In order for any miner to get their transactions accepted and their rewards claimed, they must be part of the ledger that people end up using when they refer to the name of the currency. Their state transition must – one way or another – become part of the 'meme'. This mimics Bitcoin's incentive for miners to accept each other's blocks such that their block is more likely to be included later [2], but across far greater blocks times.

This mechanism incentivizes minimizing negotiation and corruption cost. If another party can negotiate getting their block at a height for a cheaper price, theirs will be the transaction that gets added to the ledger. This is because they will be able purchase slots as a cheaper price and will subsequently accrue more. This can be essentially be modelled as an MEV market.

As a result of this open consensus layer, the value of an O token on a given ledger can be understood as derived from its likelihood to become part of a chain that others continue to use in the future, and the total perceived worth of the O ecosystem.

2.1 Incentives to Collaborate

If consensus is reached on the chain successfully, having the ability to add to this network becomes valuable. On the other hand, if miners develop 'silos' where they simply mint their own coins without finding consensus (combining efforts with others), then those coins are unlikely to gain value.

For miners looking to mine on a valuable network, an incentive to collaborate and share rewards from minting rather than mining their own private chain is present. Specifically, the value of mining rewards in a **collaborative** system can be specified as:

$$Reward_c = s * Value_c * Inflation_c$$

,

where s is a miner's share of the total network rewards, and *Value* is the price of the token of the collaborative system. The *Value* of the token depends on the acceptance of this particular network in the O ecosystem, or in other words the *memetic prominence* of the network in consideration. The inflation rate, by design of the system, depends upon the single-thread processing speed of miners.

Naturally, it is most profitable to have the fastest miner mine blocks in such a system, such that a value close to the maximum theoretical throughput is obtained. Denoting the processing power as P, we have the following version of the above statement, with k constant,

$$Reward_c = k * s * M_c * P_{max}$$

,

If a new miner were evaluating joining this system, they would have to weigh the option of joining this network (with a smaller s coefficient) or bootstrapping a new network on their own. If they were to choose to **selfishly** mine to maximize their own mint, the *individual* miner's value of mining rewards is:

$$Reward_s = k * M_i * P_i$$

This reward is unlikely to be significant, because M would be close to 0 for almost all individual miners. The greater the memetic prominence of the shared ledger, the greater the value obtained by participating in the network rather than attempting to individually mine.

The intrinsic value in the O ecosystem is unlocked only when one or more forms of the networks come to be widely accepted i.e., gain *memetic prominence*, and this is likely to only happen if miners come together to collaborate and share rewards. A collaborative situation – if it can be successfully bootstrapped – is likely to become a system of multiple counterparties that mine and validate the network together, keeping it honest and sharing inflation rewards from participating in the system.

2.2 Negotiation Bootstrapping

User transaction acceptance should be expected to be much slower – particularly at the start. At the start of the network there will be essentially zero consensus on what the state of the canonical chain is. This will make settlement time virtually infinite. However, over time the miners should start to negotiate with one another to build consensus on what the ledger should be at every time step. If they do not, none of them will be paid at all. Over time the cost of erasing this Ledger and restarting becomes greater and less likely, giving Nakamoto-style eventual consensus expectations.

2.3 Censorship Resistance

The censorship resistance of O is primary affected by the willingness of users to accept a ledger which they know is the result of censorship. If miners know that users will not accept a ledger that resulted from censorship the risks of honoring movements on that ledger increase, and subsequently the value of the tokens inside it decrease. Users could easily be equipped to detect censorship by having each other commit their transactions to Arweave after giving them to miners. If inspection of Arweave yields many TXs that were not finding their way into the canonical chain, the users could move to a non-censoring ledger as a Schilling point.

2.4 Verification

As in Solana's proof-of-history [5], prior ledger transitions can be performed in a massively parallel fashion, while new transactions additions can only be scaled by increasing 'vertical' compute speed – repeated compute whose output is only computable with full knowledge of its inputs.

2.5 Monetary Considerations

2.5.1 Mining Costs and Rewards

The outlined currency features a 1 O reward for every transaction (user or 'nop' transactions) processed, as well as a fee from the user. This incentivizes miners to:

- Attempt to maximize the number of amount of fees that they gain from processing transactions.
- Maximize the speed of their 'nop' transaction production and processing if no user TXs are available.
- Minimize the costs that they must pay to other nodes in order to encourage them to adopt their ledger transitions.

2.5.2 Inflation

In this model inflation has an Ethereum-style asymptote but is also relative to the speed that signatures can be consecutively made by the fastest available processors, modified by the total number of transactions in the ledger so far. This makes inflation proportionate to the pace of single-thread compute improvements, while also exponentially decreasing. Specifically:

```
inflation_year(n) ->
    (
            max_sigs_per_sec_in_year(n) *
            24 * 24 * 365
    ) / ledger_height.
```

If Monero's RandomX [3] is added to the signatures the only hardware advances that will be incentivized are very close to single-threaded x86-64 compute performance. This can be seen as a pro-social outcome for the currency, as it will additionally reward improvements in generally available computing power.

Inflation could be made static by modifying the protocol to take groups of TXs, minting one token on a per step basis. This introduces proof-of-stake style questions about the integrity of the clock syncing in the network, when analysed after the fact.

2.6 Open Questions

The fundamental question of the design of O is whether consensus is in fact achieved, given the broad and open bounds for it. If trust in consensus is not achieved, the O tokens in the ledgers will not have value and the network effects of currency usage cannot take place. A further question is: assuming that consensus is eventually reached for the ledger, is the latency that is required too long for practical use?

In terms of performance, the only conceivable failure of this model to reach maximal theoretical ledger processing speed is if it does not allow for all possible pluralizations of transaction applications. For example, while it may be true that a sequence of transactions of form 'A -¿ B, B -¿ A, A -¿ B, ...' cannot be executed faster than O can achieve them on present hardware architectures, non-interacting (for example, 'A -¿ B, C -¿ D, E -¿ F, ...') TXs could conceivably be massively parralellised. Whether or not O protocol allows for all possible improvements in this area has not been critically assessed.

Finally, we note that it may be possible to employ Arweave's permanent storage layer [4] to further lessen some of the drawbacks of the approach. In particular, it may be fruitful to explore whether Arweave's total ordering can be used to provide faster certainty in issues of potential double-spending.

3 Bootstrapping

Is it possible for a network without an explicit consensus mechanism to be bootstrapped? How do you get buy-in from a critical mass of users to allow a particular network in the O ecosystem to adopt the meme of the O-coin? Below, we explore a few potential ideas.

3.1 Altruistic Bootstrap

This version of bootstrapping contains the following scheme: Bootstrap a network with a pre-announced launch date, and a fair distribution of tokens to everyone that participates. Subsequently, periodically distribute 1 O-token to every address that is *registered* on the ledger at any given time.

Such a system would likely give a large first-mover advantage, and potentially dissuade future members from joining the community. However, it has strong incentives for early adoption and signaling interest in a network.

3.2 Fair Bootstrap

Bootstrap a version of the network where every address starts with a fixed number of tokens minted for them, regardless of when they choose to join the network. Future rewards may be distributed to validators and users proportionate to their relative contribution to the system.

This system has the benefit of being *egalitarian* in distribution of the tokens, but lacks strong incentives for early participation and subsequently, for promoting adoption of the network.

3.3 Exponentially Fair Bootstrap

This is a version of altruistic bootstrap, but instead of distributing 1 O-coin to everyone in the network periodically, we distribute coins based on the amount of *time* a participant has been on the network, in an exponential fashion - tokens are distributed to a miner m at every timestep t where,

$$t - t_o = 2^n$$

, for some n.

This distribution has the property of providing rewards to early adopters, but also ensuring equitable distribution to all participants in the network in the long run - no matter what *timestep* they choose to join the network at.

Indeed, consider users A and B that joined the network at times t_A and t_B respectively, with $t_B = t_A + t$, for some time t. Assuming no other transactions from/to these addresses, the relative wealth of both of these users at time x is given by,

$$\Delta(x) = w_A(x) - w_B(x)$$

$$\Delta(x) = log_2(x - t_A) - log_2(x - (t_A + t))$$

$$\Delta(x) = log_2 \frac{x - t_A}{x - (t_A + t)}$$

$$\Delta(x) = log_2(1 + \frac{t}{x - (t_A + t)})$$

which goes to $log_2(1) = 0$ as $x \to \infty$.

4 Conclusion

In this paper we have explored a radical simplification of distributed ledger design. This design promises many significantly preferable performance properties, at the potential (but as yet unquantified) cost of higher consensus latency and morphed censorship-resistance properties.

It's interesting, but would it work?

References

[1] Emin Gun Sirer Ittay Eyal. "Majority is Not Enough: Bitcoin Mining is Vulnerable". In: (2013). URL: https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf.

[2] Satoshi Nakamoto. "Bitcoin whitepaper". In: *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* (2008).

[3] *RandomX is a proof-of-work (PoW) algorithm that is optimized for general-purpose CPUs.* URL: https://github.com/tevador/RandomX.

[4] Sam Williams et al. "Arweave: A protocol for economically sustainable information permanence". In: *Arweave Yellow Paper, www. arweave. org/yellow-paper. pdf* (2019).

[5] Anatoly Yakovenko. "Solana: A new architecture for a high performance blockchain v0. 8.13". In: *Whitepaper* (2018).