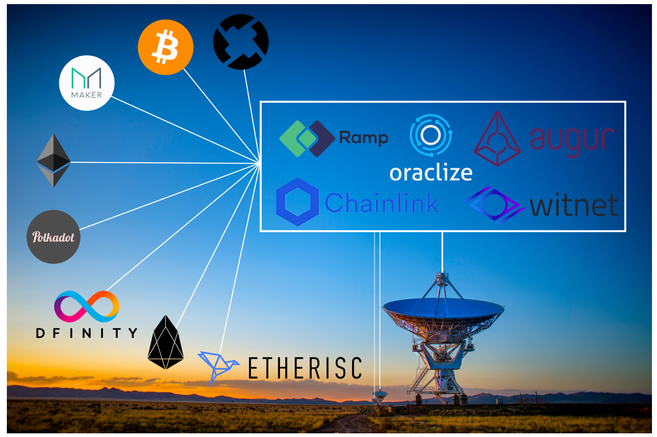
Infochain: A Decentralized, Trustless and Transparent Oracle on Blockchain

Naman Goel*, Cyril van Schreven*
Aris Filos-Ratsikas
Boi Faltings

https://goelnaman.github.io naman.goel@alumni.epfl.ch

MOTIVATION

- Smart contracts on a decentralized blockchain network allow trusted transactions and agreements to be executed without a third party.
- But smart contract require oracles to link them to the real world (by providing data about the real world events).



- So far, the only solution is to use trusted third party data sources for oracles, which violates the basic motivations of the blockchain.
- For the first time, we introduce a working fully decentralized solution to the oracle problem.

RESEARCH QUESTIONS

- How to incentivize self-interested agents to report correct information?
- How to implement the incentive mechanism in a transparent and trustless manner?

- How much is the cost and how can we optimize it?

INFOCHAIN

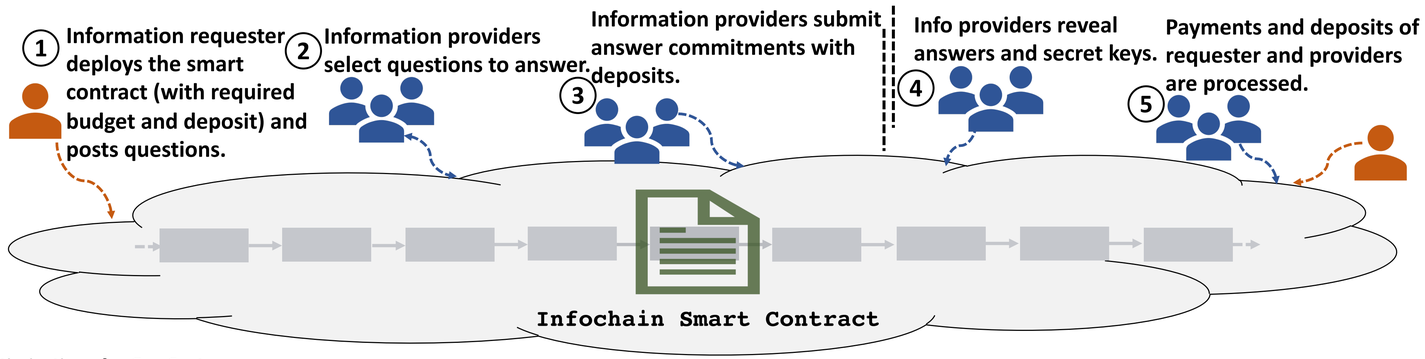
Incentive Mechanism:

Infochain uses peer-consistency mechanisms to incentivize truthful reporting.

- Currently Supported: the Peer Truth Serum for Crowdsourcing (PTSC), the Dasgupta and Ghosh (DG) Mechanism, and the Output Agreement (OA) Mechanism.

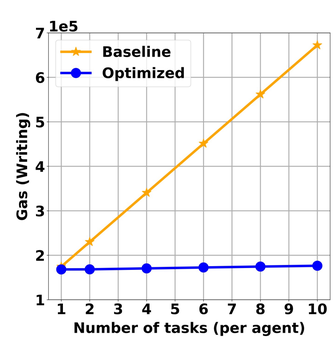
Ethereum Implementation:

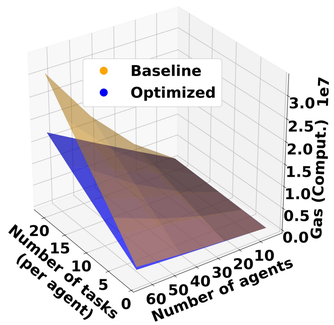
- Proposed commit-reveal and random peer selection protocols ensure incentive compatibility of the mechanisms even in a transparent blockchain environment.
- Proposed write and compute optimizations minimize gas cost ($) significantly.



Optimizations for Gas Cost:

- Performing computations on Ethereum's Virtual Machine (EVM) remains an expensive affair. This contributes to the overall cost of information acquisition.
- We show how to implement peer-consistency mechanisms in Solidity with several optimizations to significantly reduce the gas cost.
- To reduce the costs of writing on the chain, agents on Infochain combine multiple answers in the form of a bit vector.
- To reduce the cost of computing the rewards, a set of so-called intermediary values is introduced. These values naturally appear at intermediary states of reward computation. They will be precomputed and reused for each agent. This approach allows for the computation to traverse the data a minimum number of times.





Complementary Theoretical Results:

Peer-Prediction in the Presence of Outcome Dependent Lying Incentives (IJCAI 2020). Naman Goel, Aris Filos-Ratsikas and Boi Faltings.

1. The payments in the peer-consistency mechanisms can be scaled appropriately to deal with the external lying incentives. The payments required to elicit truthful information are a small fraction of the external lying incentives.
2. Lying equilibrium can be eliminated by either a threat of verification or a non-zero probability of honest reports.

Comparsion of Peer-Consistency Mechanisms:

- The PTSC not only offers stronger incentive compatibility but, as shown in the figure on the right, it also outperforms other mechanisms in terms of gas cost. The Correlated Agreement mechanism generalizes the DG mechansim, and exhibits computations similar to DG mechanism.
- We present an important new criterion for comparing or evaluating these mechanisms by their implementation complexity on the Ethereum blockchain.