February 14, 2019

Prof. Christopher E. Wilmer
Managing Editor of Ledger

Dear Dr. Wilmer:

We wish to submit our paper, “Decentralized Common Knowledge Oracles” for your consideration as a Research Article to the journal Ledger.

Incentive compatible oracles are an important area in the context of cryptocurrencies because any smart contract that conditions its behavior on *a posteriori* information about the world requires trusted oracles to operate.

In order for smart contracts to condition their execution on the state of the world, they need access to information about the world. While smart contracts can verify some *a priori* claims with mathematical or cryptographic certainty, they cannot independently verify *a posteriori* claims about the world with the same assurances. As a matter of epistemological necessity, smart contracts which condition their behavior on *a posteriori* knowledge must rely on trusted oracles to provide that knowledge. As a result, we can trust these smart contracts only if we can trust their oracles.

With no possibility of mathematical or cryptographic verification of *a posteriori* claims about the world, we instead look to economic incentives when considering whether to trust an oracle. In particular, we require that truth-telling be incentive compatible.

A common approach to designing a decentralized oracle is to create a coordination game in which individual human players are presented with an oracle query and are asked to report the correct outcome by staking some tokens. Such oracles outputs whichever outcome received the most stake and then players are rewarded if an only if they they staked in agreement with the winning outcome. The hope with these approaches is that the “Truth” will act as a Schelling point in these coordination games, which would result in the oracle returning the true outcome to the oracle query. (This approach is so common that, despite our best efforts, we were unable to find a single example of a decentralized oracle design that does not follow this coordination-game approach -- with the exception of Augur’s oracle which follows the paradigm described in our paper.).

Unfortunately, this coordination-game approach to decentralized oracle design has serious drawbacks that limit its real-world applicability. Most importantly, for these kinds of oracles, truth-telling is not incentive compatible in the cooperative model (where players can engage in

pre-play communication and can make binding agreements). This is important because in the cryptocurrency setting we know that players *can* engage in pre-play communication and make binding agreements.

In our paper we describe a new approach to decentralized oracle design that breaks from the coordination-game paradigm. We present three specific mechanisms for which truth-telling is incentive compatible in both the non-cooperative and the cooperative setting.

We believe our manuscript will be of interest to the readers of Ledger because it provides a new way to think about decentralized oracle design that breaks away from the common coordination-game approach.

We would like to suggest the following researchers as potential reviewers of this work:

Name: Sarah Azouvi
Areas of expertise: Applied Cryptography, Distributed Systems, and Game Theory
Organization: University College London
Address:
Sarah Azouvi
University College London
Department of Computer Science
Gower Street
London WC1E 6BT
United Kingdom
Telephone: n/a
Email: S.Azouvi@cs.ucl.ac.uk

Name: Aditya Asgaonkar
Area of expertise: Blockchain Research
Organization: Ethereum Foundation
Address: n/a
Telephone: n/a
Email: aa_192@usc.edu

Name: Georgios Piliouras
Area of expertise: Game Theory
Organization: Singapore University of Technology and Design
Address:
Georgios Piliouras
Singapore University of Technology and Design
Engineering Systems and Design (ESD)

8 Somapah Road
Singapore 487372
Telephone: +65 6499 4545
Email: georgios.piliouras@gmail.com

Name: Joseph Bonneau
Areas of expertise: Cryptography, Security Protocol Design, Security Economics, and Human Factors in Security.
Organization: Electronic Frontier Foundation
Address: n/a
Telephone: n/a
Email: jbonneau@gmail.com

Included in this submission:

Main Article Manuscript
approx. 12000 words
11 figures
approx. 70 equations (including simple inline declarations, equations, and inequalities)

The manuscript was prepared using Ledger's Overleaf template found here:
https://www.overleaf.com/latex/templates/ledger-journal-template/pwdmxkkxfnnj

The manuscript itself will be uploaded as a PDF, but can also be seen here:
https://www.overleaf.com/read/cdgkzhbcyjjg

Thank you for considering our paper.

Yours sincerely,

Austin Williams
Researcher, Forecast Foundation OU
austin.williams@onewayfunction.com