Master Thesis Abstract

Trustable Oracles Towards Trustable Blockchains

Pedro Duarte da Costa[a], Filipe Figueiredo Correia[a,*], Hugo Sereno Ferreira[a,*], Mário Ribeiro Alves[b,**]

[a] *Faculty of Engineering of the University of Porto, Oporto, Portugal*
[b] *BRPX - Bright Development Studio, S.A. - BRPX S.A*

Keywords: Blockchain, Oracles, Distributed Systems, Trust
CSS Concepts: •Computer systems organization → Architectures → Distributed architectures → Peer-to-peer architectures •Security and privacy → Formal methods and theory of security → Trust frameworks

The blockchain concept was proposed as a way of processing and recording monetary transactions in a peer-to-peer network while avoiding the double-spending problem[1] without requiring any centralized authority.

Later, smart contracts[2] were introduced as applications that run on the blockchain. Smart contracts are self-verifying, self-executing and immutable contracts whose terms are directly written in lines of code which persist on the blockchain.

In order to become relevant and replace existing real-world contracts, smart contracts need to be able to access information outside of the blockchain, for example, the current price of the US dollar. However smart contracts cannot directly query the internet for information due to the non-deterministic nature of the internet. Meaning that the information retrieved at some point in time cannot be entrusted to be available or equal in another point in the future, which may result in different states when validating smart contracts by querying the internet in different moments. Oracles solve the non-deterministic problem, of querying the internet, by inputting external information on the blockchain through a transaction making sure that the blockchain contains all the information required to verify itself.

The problem here is that we must trust third parties, oracles, to honestly provide information. If the oracles are compromised we risk compromising the trust of the underlying blockchain by inputting falsified information in a system that is trusted to always have a valid state.

Currently, there are a few projects trying to solve the oracles trust problem. Town Crier[3] takes advantage of trusted hardware to scrape HTTPS-enabled websites and serve

*Supervisors
**Proponent
Email addresses: pedro.duartecosta@fe.up.pt (Pedro Duarte da Costa), ffcorreia@fe.up.pt (Filipe Figueiredo Correia), hugosf@fe.up.pt (Hugo Sereno Ferreira), mario@brpx.com (Mário Ribeiro Alves)

December 16, 2018

source-authenticated data to the smart contracts. Oraclize.it provides Authenticity Proofs[4] for the data it fetches guaranteeing that the original data-source is genuine and untampered and can even make use of several data sources in order the gather trustable data, but its centralized model does not guarantee an always available service. ChainLink[5] and other Consensus-based oracles, such as Hivemind (previously Truthcoin[6]), Augur[7], Gnosis[8] and Astraea[9], although with varying architectures, base their data feed on "Wisdom of the Crowd" and incentives, in which participant behaviour effectively acts as the data source, and then report the result.

The goal of this project is to develop a method of guaranteeing trustable off-chain oracle operations. For example, the correct validation of off-chain data with its on-chain proof or untampered relaying of vote count result to the smart contract. Unlike other similar works, this project doesn't intend to query the web for data or retrieve the answer for a query but instead guarantee that the user input and post-input off-chain operations are honestly processed, sent to the chain and verifiable.

With this work, we expect to provide users with an extended level of trust in blockchain applications and their interaction with off-chain data.

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Technical Report, Bitcoin, 2009.

[2] Gavin Wood, Ethereum: A secure decentralised generalised transaction ledger, Technical Report, Ethereum, 2014.

[3] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town Crier: An Authenticated Data Feed for Smart Contracts, Technical Report, 2016.

[4] Oraclize.it, Oraclize Documentation, 2018.

[5] S. Ellis, A. Juels, S. Nazarov, ChainLink A Decentralized Oracle Network, Technical Report, 2017.

[6] P. Sztorc, Truthcoin Peer-to-Peer Oracle System and Prediction Marketplace, Technical Report, 2015.

[7] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, S. Alexander, Augur: a Decentralized Oracle and Prediction Market Platform, Technical Report, 2018.

[8] Gnosis Whitepaper, Technical Report, Gnosis, 2017.

[9] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, A. Kastania, ASTRAEA: A Decentralized Blockchain Oracle, Technical Report, 2018.