Decentralised verfication of real world events

remans, Verethy

December 4, 2017

Abstract

The underlying mechanics and mathematical framework for a decentralised concensus protocol on real world events are discussed.

1 Introduction

Blockchain technology has flourished in recent years and enabled the widespread creation of new cryptocurrencies. The idea of trustless money transfer was then sought to be extended. With the invention of smart contracts, the decentralised consensus idea was no longer solely focused on currencies and allowed the realisation of almost any decentralised, democratic process imaginable.

However, all of these applications are focused on the blockchain or decentralised system they run on and it is to date not possible to connect the trustless system to the real world. Exchange rates to fiat currencies and other real world based information cannot be implemented into the trustless world, since they all rely on some centralised source, a provider, of information. Even though exchange rates, for example, undergo some sort of consensus on the markets, the rate shown on a website or in a newspaper is not necessarily the same as everywhere else. In the worst case a malicious provider might show fraudulent information for their own benfit.

In order to tackle this problem, this paper proposes a decentralised and trustless consensus protocoll to decide on the "state" of the real world, or parts of it, at a given time. If this consensus can be reached on the blockchain, the state of the real world, as seen from a trustless point of view, can be incorporated into the chain and therefore be considered as valid as any other information stemming from the chain itself.

2 Description of the system

The same as with other cryptocurrencies there must be benefits for every party involved in the validating process of real world events. Very much like miners, validators have to be paid and users have to pay for the service. In general, several criteria have to be met in order for all parties to participate in a constructive and productive manner:

- Jurors have to be paid for their work/research to find the truth.
- The "prosecutor", the wallet that files the request for validation, has to receive an answer for a reasonable fee.
- Jurors have to be incentivised to give the correct answer, i.e.: punished for giving the wrong answer.
- Harder validation work has to be rewarded higher than simpler tasks.
- The pool of Jurors has to be randomised so a group of ill-intentioned Jurors cannot take over a case.