Journal of Database Management
Volume 32 • Issue 1 • January-March 2021

On Elastic Incentives for Blockchain Oracles

Renita M. Murimi, University of Dallas, USA
Grace Guiling Wang, New Jersey Institute of Technology, USA

ABSTRACT

A fundamental open question for oracles in blockchain environments is a determination of the amount of trust to be placed in the oracle. Oracles serve as intermediaries between a trusted blockchain environment and the untrusted external environment from where the oracles fetch data. As such, it is important to understand the uncertainty introduced by the oracle in the trusted blockchain environment and the implications of this uncertainty on blockchain performance. This paper develops a model for commoditization of trust. The model provides for dynamic trust environments that incorporates oracle selfishness. The work also considers the equilibrium behavior for the demand and supply for trust and introduces elastic incentives for increasing the trust. These results are used to determine optimum size of the network that can be served by an oracle with varying degrees of selfishness. Key consequences and challenges of incorporating oracles in trusted distributed ledger environments are presented.

KEYWORDS

Blockchain, Blockchain Size, Demand Function, Elasticity, Smart Contracts

INTRODUCTION

Oracles in blockchain (Wang et al., 2019) function by serving as a bridge between the trusted world of blockchain and the untrusted world outside the blockchain. Although distributed ledger technologies are able to leverage their trust-free architecture to securely process transactions, a major roadblock to their widespread usage is the lack of mechanisms to securely verify and incorporate data that exists outside the blockchain. The inclusion of an oracle helps to bridge this gap between the blockchain and data sources around it. By fetching data from an external source, oracles help to trigger smart contracts that link together the trusted blockchain environment and the untrusted external data source (Wohrer & Zdun, 2018). For example, in a hedging model, nodes in a blockchain (trusted environment) might be dependent on weather data from an external website (untrusted environment) in order to predict future prices for an agricultural commodity. This information cannot be verified using the blockchain's inbuilt architecture for distributed consensus. As a trusted entity, the oracle fetches this information and supplies it to the nodes, thereby triggering a smart contract.

DOI: 10.4018/JDM.2021010101

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

The implicit assumption in existing literature about blockchain oracles is that of an altruistic oracle. This assumption of an altruistic oracle provides for a high degree of trust placed by the blockchain nodes in the oracle's services. However, this assumption of an altruistic oracle may be challenged by factors such as computational complexity of the oracle's tasks and its impact on oracle performance. An oracle that is required to perform computationally intensive tasks to retrieve data from multiple untrusted environments, aggregate and process it for the blockchain is limited by its own computational capacity, the size of the blockchain network that it serves, the quantity of such requests and inter-oracle communication and computation responsibilities. Thus, oracles that are subject to a high volume of computational processing may suffer from degradation in performance in terms of latency, throughput or data accuracy. Additionally, since oracles serve as intermediaries between trusted and untrusted environments, they serve to function as a unique point of failure in the trust model espoused by blockchain environments. An oracle that is manipulated by malware can compromise the integrity of the smart contracts and jeopardize the applications involving such blockchain environments. Such outcomes can then impact the level of trust placed in the oracle by the blockchain and revert the blockchain back to the original state, where the blockchain only trusts data in the ledger and is thus unable to function in hybrid environments that require smart contracts.

Our work studies trust in the institution of the oracle. Specifically, our work seeks to answer the question: How trustworthy is the oracle, and can we use peer evaluations of the oracle's trustworthiness to assess trust placed by a node in the oracle? To do this, we commoditize trust as a tradeable unit with distinct supply and demand functions. Oracles may demonstrate selfish or fair behavior, where selfish behavior behooves the oracle to conserve its own resources and offer subpar service to the nodes. Similarly, a fair oracle is able to serve the requests of the nodes, even at the expense of consumption of its own resources. One reason for an oracle to demonstrate selfish behavior is the amount of work requested of the oracle. The oracle's selfishness is dictated by the number of requests it serves. The role of the oracle's selfishness sets the tone for the number of nodes it can serve. We explore how incentives added to the nodes' trust valuations can influence the number of nodes that can be served by selfish (fair) oracles.

In our model, each blockchain of nodes demands a certain quantity of trust from the oracle, which is quantified by the demand function. The amount of trust demanded from the oracle by the nodes in the blockchain is based on two components, the collective trust placed by peer nodes and the selfishness of the oracle. To do this, first, we borrow upon sociological constructs for trust in societies to formulate a mathematical framework for collective trust. Specifically, we use the definition in Lewis & Weigert (1985) that collective trust in an entity is not just a personal assessment, but it depends on the trust placed by peers in that entity. This sociological conceptualization of trust is extracted largely from the works of Luhman (1979), Barber (1980), Parsons (1963) and Simmel (1900). Luhmann emphasizes that trust leads to a reduction of complexity since individuals can trust their peers to make informed decisions that lessen the amount of risk. Luhmann also states that familiarity is a precondition of trust as well as distrust, as individuals learn and devise strategies for risk-mitigation from the actions and outcomes of their peers. In related work by Simmel (1900), the author environments with perfect information do not impose the need for trust, since individuals would have perfect information about events and outcomes and would know the appropriate strategies to land those outcomes. However, in imperfect environments, trust provides a valuable intermediary construct with which to assess the impact of certain actions and outcomes in the peer environment. Work in Barber (1980) extends this formulation to state that trust implies a "confident expectation" on behalf of the individual that a certain action will result in a less risky outcome. Parsons (1963) goes on to show how trust holds together societies, noting that the lack of trust can erode public confidence and leads to the disintegration of societies.

Our model for trust work as follows. In a network with four nodes A, B, C and D that is asked to trust an entity S node A might place a level of trust in S that may or may not reflect how its peers $(B, C,$ and $D)$ assess S. In other words, "I trust because they (do not) trust". Additionally,

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/on-elastic-incentives-for-blockchain-oracles/272504

Related Content

Parallel Skyline Computation Exploiting the Lattice Structure
Markus Endresand Werner Kießling (2015). *Journal of Database Management (pp. 18-43).*
www.irma-international.org/article/parallel-skyline-computation-exploiting-the-lattice-structure/153516

Mapping Generalizations and Specializations and Categories to Relational Databases
Sikha Bagui (2009). *Handbook of Research on Innovations in Database Technologies and Applications: Current and Future Trends (pp. 1-11).*
www.irma-international.org/chapter/mapping-generalizations-specializations-categories-relational/20682

Overview of Internet of Medical Things Security Based on Blockchain Access Control
Yikai Liu, Fenglan Ju, Qunwei Zhang, Meng Zhang, Zezhong Ma, Mingduo Li, Aimin Yangand Fengchun Liu (2023). *Journal of Database Management (pp. 1-20).*
www.irma-international.org/article/overview-of-internet-of-medical-things-security-based-on-blockchain-access-control/321545

Measuring the Determining Factors of Financial Development of Commercial Banks in Selected SAARC Countries
Arodh Lal Karn, Girish Santosh Bagale, Bhavana Raj Kondamudi., Deepesh Kumar Srivastava, Ravi Kumar Guptaand Sudhakar Sengan (2022). *Journal of Database Management (pp. 1-21).*
www.irma-international.org/article/measuring-the-determining-factors-of-financial-development-of-commercial-banks-in-selected-saarc-countries/311092

A Measurement Ontology Generalizable for Emerging Domain Applications on the Semantic Web
Henry M. Kim, Arijit Sengupta, Mark S. Foxand Mehmet Dalkilic (2007). *Journal of Database Management (pp. 20-42).*
www.irma-international.org/article/measurement-ontology-generalizable-emerging-domain/3365