Trusting Blockchain Data in Supply Chains

Sidra Malik, Salil Kanhere
UNSW Sydney
{sidra.malik,salil.kanhere}@unsw.edu.au

Volkan Dedeoglu
CSIRO Data61, Brisbane
volkan.dedeoglu@data61.csiro.au

Raja Jurdak
QUT, Brisbane
r.jurdak@qut.edu.au

ABSTRACT

Blockchain technology addresses the major issues of traceability and data integrity in supply chains, but it cannot attest to the authenticity of data itself. This work proposes a trust management solution to promote an honest contribution of data to blockchain enabled supply chains.

1 INTRODUCTION

Blockchain based supply chains can host transactions linked to trade, ownership, shipment, location and other critical supply chain information. These logs not only provide traceability but also ensure they are tamper proof. Traceability is one of the major challenges in supply chains which blockchain promises to solve with a temper proof ledger particularly where the provenance of supply chain products is required. With advent of blockchain technology in supply chains, finding a source of food is now a matter of few seconds for a consumer[2]. However, the question is if blockchain guarantees the correctness of information.

In traditional blockchain systems designed for cryptocurrency, such as Bitcoin, the creation and transfer of bitcoins comes with a heavy computation i.e. Proof of Work (PoW) which certifies the existence of currency accounts and transfer of digital assets. However, blockchain for physical assets such as in supply chain can only promise the immutability of data once recorded on the ledger. It cannot ascertain the authenticity of the data itself. Thus, data integrity on blockchain enabled supply chains becomes questionable. In this work we argue that blockchain alone cannot support the reliability of logged supply chain events. Without incentives or penalties the entities may record false information on blockchain. We solve this problem by integrating a trust management system with blockchain known as TrustChain[1], to encourage contribution of honest data.

2 CONTRIBUTION

Our proposed reputation and trust framework is based on a three layered architecture as shown in Figure 1. The framework is flexible to compute the reputation at different levels of abstractions i.e. for the product and the trading entity.

Data Sources: At the data layer, we collate information from multiple sources such as IoT sensors, trade events and endorsements of trading entities and sites from third party regulators. We formulate various transactions which certify these supply chain events.

Smart contracts: are self executing software programs invoked when some predefined conditions are met. When the transactions from data layer are logged at the blockchain layer, they invoke corresponding smart contracts i.e. *Rating* or *Quality* Smart Contract.

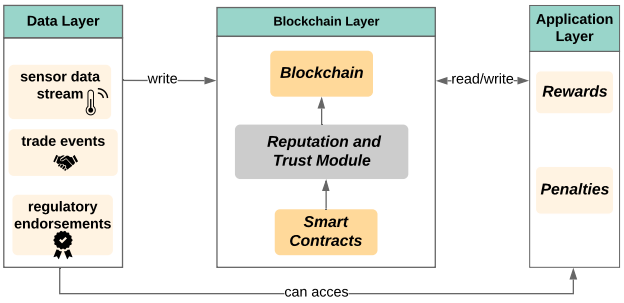

Figure 1: Trust management framework in blockchain-enabled supply chains

These SCs are designed to rate the entities and commodities respectively. For each supply chain event, rating SC computes the trader's reputation score using as a weighted sum of ratings from each of the data sources. The reputation scores over the series of events are then added, where recent scores are given more weight-age. This final score is then used in computation of trader's trust score which must be equal or greater than minimum trust score. Quality SC on the other hand, computes the rating for a commodity based on the assessment of sensing data such as temperature sensors authenticating the freshness of produce. It also emits warning events when critical conditions are met, i.e. rise in temperature for frozen produce.

Rewards and Penalties: At application layer, the entities are then rewarded or penalised based on the computation of overall trust score. They are penalized by revoking their participation in the network and rewarded by getting published as a highly trusted entity on network.

3 EVALUATION

A complete implementation of the framework is carried out using Hyperledger Fabric and Caliper. The results prove that introducing a trust management layer adds minimal overheads to an existing blockchain-based system in terms of throughput and latency. A qualitative security analyses was performed against known attacks in reputation systems which proves TrustChain's resilience to such attacks. Our proposed solution can be generalised for any real-world use-case which used blockchain i.e. healthcare, asset management.

REFERENCES

[1] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak. 2019. TrustChain: Trust Management in Blockchain and IoT supported Supply Chains. In *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 184–193.

[2] S. Malik, S. S. Kanhere, and R. Jurdak. 2018. ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains. In *2018 IEEE 17th NCA Symposium*. 1–10. https://doi.org/10.1109/NCA.2018.8548322

womENcourage-, September 2020, Baku, Azerbaijan
2020. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn