Technical Disclosure Commons

Defensive Publications Series

November 2019

SUPPLY CHAIN TRUST AS A SERVICE USING TRUST MANAGEMENT IN BLOCKCHAIN AND INTERNET OF THINGS TO PROVIDE REPUTATION SCORES FOR SUPPLY CHAIN ENTITIES

Johnson Manuel-Devadoss

SUPPLY CHAIN TRUST AS A SERVICE USING TRUST MANAGEMENT IN BLOCKCHAIN AND INTERNET OF THINGS TO PROVIDE REPUTATION SCORES FOR SUPPLY CHAIN ENTITIES

AUTHORS:
Johnson Manuel-Devadoss

ABSTRACT

Techniques are described for Supply Chain Trust as a Service (SCTaaS). SCTaaS may provide trust and reputation scores for supply chain entities using trust management in a blockchain and the Internet of Things (IoT).

DETAILED DESCRIPTION

Traceability and integrity are major challenges for the increasingly complex supply chains of today's world. Although blockchain technology has the potential to address these challenges by providing a tamper-proof audit trail of supply chain events and data associated with a product lifecycle, it does not solve the trust problem associated with the data itself. Reputation systems are an effective approach to solving this trust problem by allowing users to rate each other in online communities. However, current reputation systems are not suited for blockchain based supply chain applications as they are based on limited observations, lack granularity and automation, and have unexplored overhead.

Accordingly, described herein are techniques for Supply Chain Trust as a Service (SCTaaS) as a multi-layered trust management framework which uses a consortium blockchain to track interactions among supply chain participants and to dynamically assign trust and reputation scores based on these interactions. This approach is based on the use of Distributed Ledger Technology (DLT) deployed on a fog infrastructure for a trust and reputation model provider in a multi-data owner and multi-service provider environment, where there is not necessarily any trust between these parties.

DLT is a time-stamped series of immutable data records that can enhance existing supply chains with traceability, provenance techniques, ownership information, and anti-counterfeiting measures. In DLT-based supply chains, events such as trade, ownership and location data are hashed and linked to DLT transactions. These transactions are grouped into blocks that are linked together with cryptographic hashes, making them immutable.

Published by Technical Disclosure Commons, 2019

The significance of the unsolicited confirmation of supply chain events can be realized well in supply chains such as food and drug where there is a need to trace the origin of products or identify a point of fraud. The goal is to prove that a consortium permissioned blockchain can make otherwise siloed supply chain event data available to all authorized participants, thereby making traceability more robust and time efficient.

However, the integrity of data is identified as an unsolved problem for DLT based supply chains. Most conventional DLTs are based on the creation and transfer of digital assets. In supply chain applications, DLT provides not only immutability but also a proof that the stored data is correct and trusted. This feature is a result of the integration of creation and transfer of digital values with the distributed consensus mechanisms based on public key cryptography and digital signatures. For example, in Bitcoin DLT, creation and transfer of bitcoins is integrated to the Proof of Work (POW) consensus mechanism. However, for physical commodity and asset trading applications, the hashed data on the DLT represents digital observations of physical events. Although data related to supply chain events is immutable once recorded on a DLT, the DLT cannot ascertain the authenticity of observations provided by supply chain entities. The authenticity and trust of the data becomes questionable, and thus raises the concern of data integrity on the DLT.

As described herein, blockchain is an effective technology for managing supply chain traceability, but it alone cannot support the trust and reliability of data regarding the quality of commodities and the trustworthiness of supply chain entities. False data generated by the supply chain entities becomes immutable once recorded on the blockchain platform. One approach to improving the trust and reliability of the data is to use accountability and reward mechanisms to penalize and incentivize dishonest and trustworthy participants, respectively. These mechanisms rely on a trust management system which may be integrated within a supply chain blockchain. Such a system may also benefit from the data generated by Internet of Thing (IoT) sensors (e.g., temperature, location, etc.) which are being increasingly embedded in various stages of the supply chain lifecycle (e.g., farms, manufacturing plants, shipping containers, etc.).

However, IoT sensors are also susceptible to faults or malicious attacks and thus cannot be blindly trusted. There are many challenges to devising an effective reputation system in supply chains. One such challenge is the need for a multi-faceted assessment of

the trustworthiness of the data logged in the DLT which incorporates inputs from IoT sensors, feedback provided by supply chain entities, physical audits, etc. A supply chain participant may trade more than one type of commodity. A participant must be evaluated distinctively for each of these types and so should the individual commodity based on whether its quality was preserved during the product chain. To provide the sanctions and incentives, an automated framework is required which not only provides traceability of supply chain events but also relates each of these events to a trust value of a participant and the quality of commodity. The associated overheads should be minimal and not impact the scalability of the platform.

To address these challenges, a multi-layered DLT-based supply chain trust management framework is provided (also referred to as SCTaaS). A DLT based reputation and trust framework for supply chains may operate at both agent and resource level and evaluate the various evaluation metrics such as correctness of predictions and/or performance to determine the quality of commodities, and the trustworthiness of entities based on multiple observations of supply chain events. The system also examines the dynamic behavior of supply chain peers and the kind of threat analysis involved, which usually considers how a reputation model behaves in badmouthing, collusive manipulating of reputation, oscillating behavior, and traitors attacks. Smart contracts may be leveraged for automation of reputation calculation with DLT transactions and sanctions to provide the rewards and accountability for both supply chain participants and quality of product being traded. Based on the output of the smart contracts, supply chain participants and commodities receive reputation scores as a measure of their trustworthiness for a trade event. Supply chain participants are then penalized by revoking their participation in the supply chain or rewarded by obtaining higher published ratings.

The data that provides traceability and integrity of supply chain events, product data stating its properties, IoT sensor data, and other supplementary sources of data (such as crypto-anchors) and regulatory endorsements should be recorded in a tamper-proof way. The recorded data should be authentic and represent the true observations of sensor devices, supply chain entities, and other data sources. The DLT satisfies the first requirement with a distributed tamper-proof ledger. The aim of this idea is to address the second requirement by devising mechanisms to establish trust in data at the point of origin and ensure that the

data recorded on the DLT is trusted. As supply chains involve multiple entities and product types, the trust should be established at a granular level that takes into account the different product types, entities, and their interactions. Furthermore, the process can be automated by providing real-time traceability. SCTaaS may include a DLT integrated trust and reputation module that evaluates the truthfulness of the supply chain data and calculates reputation scores for commodities and supply chain entities at a granular level.

The SCTaaS framework may be organized into six layers (Network, Data, Blockchain, Reputation, Security, and Application) with supporting components.

The Network layer enables easy connection to distributed devices ("things") to the network. Those data may be extracted, normalized, and securely moved from those devices to other layers such as Data, Blockchain, and Reputation. The Data layer encompasses supply chain data produced by sensor devices, trade events between entities, and regulatory endorsements. The raw data may be stored in a database at the application layer, while the message digest of the data is sent to the Blockchain layer in the form of transactions. At the Blockchain layer, the transactions are stored on the ledger and processed following a set of access rules defined by the Access Control List (ACL) in the Security layer. The access rules specify who can read or write the data on the ledger. The transactions invoke smart contracts, which generate reputation and trust values for entities and quality ratings for commodities using the reputation and trust module. The smart contracts also emit warning events depending on predefined conditions. The reputation and trust values are stored on the digital profiles of supply chain entities and commodities on the blockchain.

Finally, the application layer interacts with the Blockchain layer through queries. The administrators and regulators query about the trust and quality scores of entities and commodities respectively. The quality of commodity is also made available to the consumer when it finishes the product chain. Based on the retrieved scores, they provide rewards and sanctions, which recompense the entities with high scores by publishing their scores, sanction the entities with low scores by revocation from the network, and publish the product ratings for final consumers.

The permissioned DLT network is managed by a business network administrator sitting between the supply chain entities and the DLT network. The business network administrator has administrative control over the DLT and defines the business network

model. The Reputation layer is responsible for validating the actor and commodity to determine the reputation scores based dynamic behavior analysis. The reputation layer examines whether the dynamic behavior of peers between supply chain entities is simulated and performs threat analysis using the Security layer. This usually involves considering how a supply entity behaves in one or more attacks, such as badmouthing, collusive manipulating of reputation, oscillating behavior, and traitors' attack.

Badmouthing involves peers sending negative recommendations regarding honest peers. Collusive manipulating of reputation involves peers forming collusions to boost their own reputation with positive recommendations for each other and decreasing the reputation of honest peers by sending unfairly negative recommendations regarding the honest peers. Oscillating behavior involves peers with an unstable transactional behavior (e.g., trying to keep high reputation values while cheating in a small fraction of transactions). Traitors' attack involves peers behaving honestly in their transactions for some time to acquire a high reputation value and then beginning to cheat.

An example end-to-end commodity trade in the SCTaaS implementation is described as follows. Initially, an instance of the quality contract is created for the commodity with the temperature conditions specific to the type of the commodity. The supply chain entities register on the SCTaaS network and are assigned initial trust scores. The initial trust scores are defined based on the prior dynamic peer behavior. When the commodity is ready for trade, the primary producer generates a create transaction, and then the verifier of the security layer verifies the create transaction to create the unique signature to permit the certifier of the Security layer to bind it to the smart contract and assigns the quality smart contract private key to the commodity.

Once the create transaction is committed in the ledger, sensory transactions indicating the temperature conditions of the commodity are stored on the Blockchain layer of SCTaaS and alerts are generated if the temperature readings exceed the thresholds defined in the contract. The primary producer's storage facility is periodically assessed by the regulator in accordance with 36 C.F.R. § 1234.10. The respective regulatory ratings are assigned with cross-references to the SCTaaS verifier rules. The ratings may be stored in the primary producer's profile. The regulator ratings are sent to the Reputation layer of SCTaaS to determine the reputation score for the primary producer. The primary producer

reputation score is determined based on the dynamic behavior among peers and trustworthiness of the commodity's quality and storage facility requirements set by the regulator in accordance with 36 C.F.R. § 1234.10.

The reputation score of each actor (e.g., primary producer, trader, supplier, retailer, etc.) may consider how the actor behaves in one or more of the reputation attacks such as badmouthing, collusive manipulating of reputation, oscillating behavior, and traitors' attack. SCTaaS may create the trade transaction when the commodity trade takes place between the primary producer and the shipper, and designate the shipper as the new owner of the commodity. The shipper provides the reputation rating for the trader to the primary producer based on the quality of the received commodity along with the dynamic behavior of the primary producer among the supply chain peers. The shipper reputation rating for the trader to the primary producer is stored in the primary producer's profile.

The SCTaaS triggers the trade transaction rating smart contract for the trader which computes the reputation score of the commodity using the Reputation layer and the primary producer's rating, and stores them in the respective profiles of the commodity and the primary producer. This sequence may be repeated for the trade between the shipper and the retailer by replacing the primary producer and the shipper with the shipper and the retailer, respectively. The retailer is the final purchaser of the commodity. The retailer issues a commodity transaction which also generates the commodity rating using the quality smart contract.

These sequences are repeated for other commodities of the same type for a trade event happening at similar times, and the seller has reputation scores for each commodity type. The regulators and the administrators can request to compute the reputation score and trader trust score which will be stored in the seller's profile. A seller is either sanctioned or rewarded through SCTaaS based on dynamic behavior and trustworthiness. Consumers of the commodities can query from SCTaaS regarding the commodity reputation score in order to check any the temperature threshold violations throughout the supply chain lifecycle.

The reputation model evaluates the various evaluation metrics such as correctness of predictions and/or the performance to determine the quality of commodities, and the trustworthiness of entities based on multiple observations of supply chain events. The

system may also examine the dynamic behavior of supply chain peers and the type of threat analysis involved. This may involve considering how a reputation model behaves in badmouthing, collusive manipulating of reputation, oscillating behavior, and traitors' attacks. The system also determines the reputations scores of supply chain participants with dynamic behavior, threat analysis, predictions, and performance between supply chain participants and products, and also enables the assignment of product-specific reputations for the same participant. Smart contracts may be used for transparent, efficient, and secure predictions, trustworthiness, and automated calculation of reputation scores.

In summary, techniques are described for SCTaaS. SCTaaS may provide trust and reputation scores for supply chain entities using trust management in a blockchain and the IoT.