Establishing Trust and Facilitating Cloud Chain Management with Blockchain Technology

T .Rajesh Kumar

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

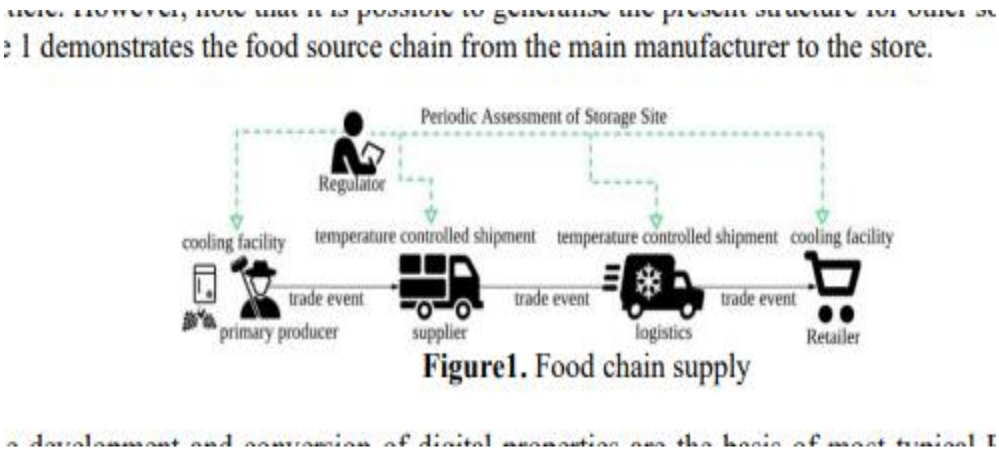
Authentication and Completeness: Ongoing Complexities in Modern Supply Chains The present-day, increasingly diverse supply chains grapple with significant challenges surrounding verification and completeness. Despite the potential of block chain technologies to provide an unaltered trail through manipulation-resistant audits, they fall short in resolving the confidence deficit linked not only to the sequence of chain activities but also the encompassing data related to the entire product life cycle. In this context, the notion of confidence becomes paramount. Existing mechanisms of reputation hold promise as a remedy for this faith predicament. However, these credibility structures prove less than ideal for blockchain-based supply chain applications due to their limitations in granularity, scope, and the absence of an in-depth discussion on overhead and automation. We propose a three-tiered confidence system for addressing these concerns. Our management platform employs a blockchain consortium to meticulously track relationships among supply chain stakeholders. Trust and reputation are dynamically attributed based on these interactions. The crux of innovation lies in our comprehensive model, which evaluates product quality and individual trust through a multitude of observations that emphasize credibility attributes during supply chain events. By tackling the intricate challenges of trust and transparency, we pave the way for a more streamlined, effective, and secure supply chain ecosystem.

Keywords: Blockchain, Confidence protection, food chain supply, Cloud, Privacy.

Introducing

Blockchain Confdence Protection and Cloud Chain Management SupportIn the contemporary landscape of digital transactions and complex supply chains, the challenges of ensuring trust, security, and comprehensive management have reached new heights [1]. As supply chains become increasingly intricate and diverse, the need to verify authenticity and completeness has emerged as a critical concern.

While blockchain technology offers a robust solution through its tamper-resistant audit trail[2] , it falls short in addressing the underlying issue of confidence associated not only with the sequential chain of activities but also with the holistic information encompassing the entire lifecycle of a product [3].In response to these challenges, this study delves into a pioneering approach that converges the power of blockchain technology with confidence protection and cloud chain management support [4]. While blockchain provides the foundation for transparency and immutability, the focus here extends beyond mere data integrity to encompass the vital realm of confidence in supply chain interactions [5].The existing mechanisms for establishing credibility, often reliant on reputation systems, present inherent limitations when integrated with blockchain-based supply chain applications [6]. These limitations include constrained granularity, scope, and an insufficient discussion of overhead and automation. Consequently, a novel three-layer confidence system is proposed, poised to overcome these shortcomings and enhance the ecosystem's efficacy [7]. At its core, our management platform leverages a blockchain consortium to intricately trace relationships among various actors within the supply chain. Through dynamic assignment of trust and prestige based on these interactions, the system tackles the intricate web of credibility associated with every transaction [8].A groundbreaking model is introduced, one that evaluates not only product quality but also individual trust through a multitude of observations, emphasizing credibility attributes throughout the supply chain journey [9]. By disassociating supply chain members from the products themselves, our approach streamlines the integration of brand credibility using smart contracts, ensuring straightforward utilization by the same participant [10].The efficacy, security, and automation of this approach are underscored by an automated credibility scoring mechanism, significantly reducing latency and throughput overhead when compared to conventional blockchain-based supply chain models [11].In essence, this study pioneers an innovative paradigm, bridging the gap between blockchain technology, confidence protection, and cloud chain management support [12]. By tackling the multifaceted challenges of trust and transparency within the supply chain realm, we aim to lay the foundation for a more seamless, secure, and efficient ecosystem that resonates with the demands of the modern digital age [13].



there. However, note that it is possible to generalise the present structure for other sc

1 demonstrates the food source chain from the main manufacturer to the store.

Figure1. Food chain supply

e development and conversion of digital properties are the basis of most typical I

Methodology

Addressing Verification and Credibility Challenges in Supply Chain Management The challenges of verifying and establishing credibility within supply chain management processes loom large. Ensuring the traceability and integrity of supply chains demands the fulfillment of two distinct imperatives: the formal verification and transparency of source chain activities, and the accurate depiction of commodity data encompassing its attributes, IoT sensor readings, and supplementary data sources like encryption anchors [14]. In addition, the control of authorizations demands that data capture is securely documented, which is admirably fulfilled by a decentralized, tamper-resistant ledger offered by blockchain (BC) technology, addressing the first imperative. Our objective is to effectively tackle the second requirement through the formulation of processes that instill confidence in source information while ensuring the reliability of reported data on the blockchain [15]. This endeavor aims to establish trust at a granular level, meticulously considering various categories of goods, organizations, and their intricate interrelationships within supply chains. Given the multifaceted nature of supply chains, which encompass diverse individuals and a wide array of products, our proposed framework, coined as the "BC United Confidence and Standing Platform," endeavors to achieve this objective. The framework employs intelligent contracts, self-executing software programs triggered upon the fulfillment of predetermined conditions, to automate operations. Structured into three layers as depicted in Figure 2, the system commences with the information layer housing data generated by supply chain events, business processes among organizations, and authorization protocols. While raw data can be stored offline in a database within the application layer, a transaction hash is directed to the BC layer. The interactions are stored on the BC layer's ledger and are subject to processing based on a predefined set of Access Control List rules (ACL), determining permissions for data read and write operations. Intelligent contracts come into play, establishing credibility and trust scores for companies and product quality, further generating alerts based on stipulated conditions, such as temperature thresholds. Within the digital compartments of the BC, credibility and trust attributes of supply chain entities and product quality are preserved. The application layer facilitates communication between stakeholders, regulators, and commissions, inquiring into the reliability and efficiency of organizations and products. As products traverse the supply chain, their consistency is made transparent to end-users. Depending on earned scores, incentives and penalties are administered, rewarding high-value entities with visibility points while penalizing low-value ones through network revocations and user reviews. Assuming the integration of IoT sensors for temperature, position, and moisture measurements across each supply chain node, depicted in Figure 2, these readings serve as critical inputs for food safety measures. Regular recalibration of these sensors ensures measurement accuracy. As an example, we employ temperature sensors, underscoring the necessity for products to consistently remain within specified temperature thresholds, from origin to consumer shelf. Smart commodity contracts define ratings and trigger alerts in case of deviations from specified ranges. In summation, this approach grapples with the intricate complexities of supply chain verification and credibility. By fusing block chain technology with intelligent contracts and IoT sensors, we set the stage for a more transparent, accountable, and secure supply chain ecosystem that resonates with the demands of modern commerce.

ed according to a set of the Access Control List rules (ACL).

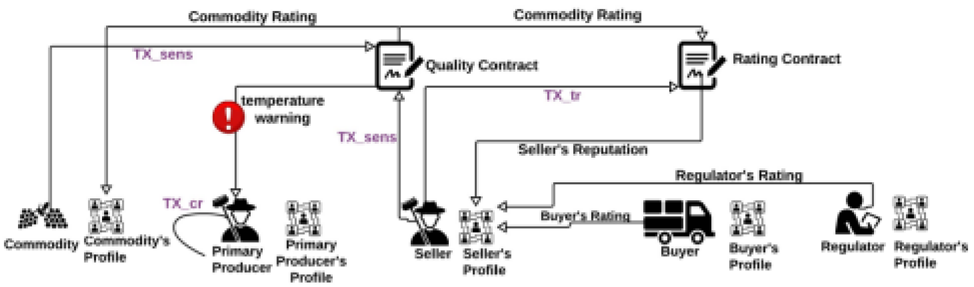


Figure 2: Overview of the proposed system

Results

In this section, we delve into the subject of trust-related attacks and the efficacy of Block-level protection against them. Our analysis encompasses controllers, corporate system operators, and associates within the Hyperledger network. These entities are evaluated to be both credible and immune to vulnerabilities. Notably, Hyperledger endorsers are excluded from the scope of our threat model due to a safeguard mechanism: transactions supported maliciously by any partner undergo comprehensive validation by all validators before final commitment. Consequently, the potential for a manipulative peer to succeed is highly improbable due to the robust support policies and consensus processes inherent in blockchain (BC) technology. It's crucial to reiterate that our system's fundamental objective is to address confidence issues within the supply chain domain, encompassing product standards and the tracking of organizational activities using blockchain. Consequently, adversaries in our threat model encompass elements within the supply chain capable of independently or collaboratively falsifying source information. This spans a range of potential attacks, including manipulation of sensor data, counterfeit goods production, registration of multiple fake IDs, fabrication of fictitious scores for other supply chain entities, impersonation, and the act of disavowing commercial activities. Figure 3 visually illustrates the throughput analysis of trade transactions. It's pertinent to note that our focus lies primarily on reputation device attacks, with network attacks typically excluded from consideration. Our evaluation involves assessing the likelihood of these attacks transpiring and their potential impact, based on guidelines outlined by the European Telecommunication Standards Institute (ETSI) for threat assessment. One illustrative scenario involves a seller issuing a "flag of dissatisfaction" to an underperforming buyer, substantiated by evidence related to performance. Our system exhibits substantial resistance to eight of the nine attacks tested and a moderate resilience against the remaining one. The matter of unequal assessments is briefly addressed, and the process of flag communication is channeled through a validator belonging to the reseller.However, an important consideration emerges—the possibility of an infinite loop wherein a seller intentionally flags a reputable buyer as unsatisfactory. This can be mitigated by the validator through the adjustment of the buyer's ranking weight (w2) and a reassessment of resellers. Further checks are implemented when dissatisfaction flags from the same buyer are lifted by multiple sellers, and the increase in consecutive dissatisfaction flags from the buyer by the seller remains below the number of commercial connections between them. These criteria validate the authenticity of the seller's dissatisfaction flags.For validation and assessment, we employ Caliper3, a benchmarking tool designed for evaluating Hyperledger performance. It empowers users to gauge the output of a BC model, taking parameters like latency and strength into account. It's important to note that Caliper's predefined network models have limitations.Our evaluation centers on a basic model comprising a solitary ordering node and two assisting participants with a shared communication platform from different organizations. The entire enterprise network is modeled using Hyperledger Composer, with Caliper tests conducted on a Dell notebook (Intel Core i7, 2.21 GHz, 8 GB memory). Transactions are considered not only typical but also with higher computational overhead to simulate success assessments.Within the context of trust management, we compare our proposed Trust Management system's output with a basic BC scheme that merely stores ownership details of supply chain events. Our assessment encompasses both performance and latency, spanning transaction frequencies from ten to 100 connections per second over a replication interval of 100 seconds. These assessments are based on the results of multiple test runs, averaging across various sending rates and transaction types.In summation, this segment provides a comprehensive analysis of trust-related attacks, the resilience of Block-level protection, and the empirical assessment of our Trust Management system's performance within the context of a simulated supply chain scenario.

15.

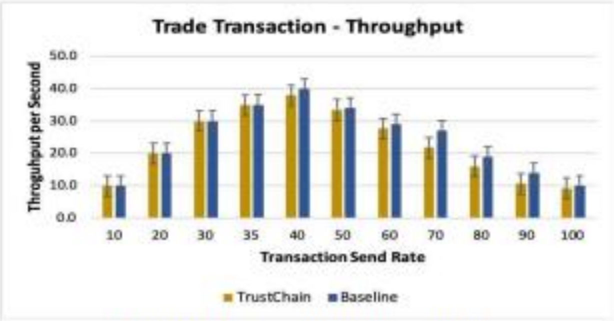


Figure 3. Throughput analysis

Conclusion

This article proposes a comprehensive system for managing confidence within blockchain-enabled supply chain processes, aiming to address the overarching challenge of ensuring trust in both product consistency and the classification of blockchain data by various participants. The underlying architectural framework harnesses the potential of a blockchain consortium, seamlessly mapping and dynamically attributing trust and credibility scores based on interactions among supply chain entities. This approach encompasses an agent-based and asset-oriented model, enabling the assignment of product-specific standings within the same member entities. The integration of automation and reliability is achieved through the utilization of intelligent contracts.Furthermore, a qualitative analysis has been conducted to scrutinize the security aspects, focusing particularly on the integrity of the device. The findings indicate a robust safeguarding mechanism against potential risks. By further investigating these aspects, we aim to refine and enhance the efficacy of our proposed system, ultimately contributing to the advancement of trust management in blockchain-driven supply chain applications.

References

1. Khaqqi, K. N., Sikorski, J. J., Hadinoto, K., & Kraft, M. (2018). Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Applied Energy, 209, 8-19.

2. Schaub, A., Bazin, R., Hasan, O., & Brunie, L. (2016, May). A trustless privacy-preserving reputation system. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 398-411). Springer, Cham.

3. Moinet, A., Darties, B., & Baril, J. L. (2017). Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.

4. Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers (Vol. 310, No. 4).

5. Starbird, S. A. (1997). Acceptance sampling, imperfect production, and the optimality of zero defects. Naval Research Logistics (NRL), 44(6), 515-530.

6. Food standards australia new zealand. [Online]. Available: http://www.foodstandards.gov.au/Pages/default.aspx

7. Commerce, B. E., Jøsang, A., & Ismail, R. (2002). The beta reputation system. In In Proceedings of the 15th Bled Electronic Commerce Conference.Gambetta, D. (1988). Trust: Making and breaking cooperative relations.

8. T. ETSI, "102 165-1 v4. 2.3 (2011-03)," Technical Specification Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), p. 75, 2011.

9. Diallo, M. H., Panwar, N., Mehrotra, S., & Sani, A. A. (2018, March). Trustworthy sensing in an untrusted iot environment. In 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 468-471). IEEE.

10. Radhika, K., Babu, Y. M. M., & Shahina, S. K. M. Classification of RISAT MRS Data with BM3D algorithm. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8, 104-106.

11. Hemalatha, M., Varadarajan, S., & Babu, Y. M. M. (2017, February). Comparison of DWT, DWT-SWT, and DT-CWT for low resolution satellite images enhancement. In 2017 ICACSE 2020 Journal of Physics: Conference Series 1964 (2021) 042068 IOP Publishing doi:10.1088/1742-6596/1964/4/042068 7 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (pp. 1-5). IEEE.

12. Saravanan, T. R., Uma, K., & Khaja, M. B. Encryption and Decryption of Gray Scale Images Using Scalable Coding Mechanism.

13. Periasamy, K., & Latha, B. The Enhancement of Storage and Bandwidth Optimization Using Data De-Duplication. International Journal of Applied Engineering Research, 9(20), 2014.

[14] Pandey, A., & Prakash, G. (2019). Deduplication with Attribute Based Encryption in EHealth Care Systems. International Journal of MC Square Scientific Research, 11(4), 16-24.

[15] Prakash, G. and Nagesh Y., (2019).Secure and Efficient Block Chain Based Protocol For Food Beverages. International Journal of MC Square Scientific Research,10(3):19-3