Orchestrating product provenance story

Suhail, Sabah; Hussain, Rasheed; Khan, Abid; Hong, Choong Seon

Published in:
Computers in Industry

DOI:
10.1016/j.compind.2020.103334

Publication date:
2020

Citation for published version (APA):
Suhail, S., Hussain, R., Khan, A., & Hong, C. S. (2020). Orchestrating product provenance story: When IOTA ecosystem meets electronics supply chain space. *Computers in Industry*, *123*, [103334]. https://doi.org/10.1016/j.compind.2020.103334

Orchestrating Product Provenance Story: When IOTA Ecosystem Meets Electronics Supply Chain Space

Sabah Suhail[a], Rasheed Hussain[b], Abid Khan[c], Choong Seon Hong[a,*]

[a]*Department of Computer Science and Engineering, Kyung Hee University, South Korea.*
[b]*Institute of Information Security and Cyber-Physical Systems, Innopolis University, Russia.*
[c]*Department of Computer Science, Aberystwyth University, United Kingdom.*

Abstract

"Trustworthy data" is the fuel for ensuring transparent traceability, precise decision-making, and cogent coordination in the Supply Chain (SC) space. However, the disparate data silos act as a trade barrier in orchestrating the provenance of the product lifecycle; starting from the raw materials to end products available for customers. Besides product traceability, the legacy SCs face several other problems including data validation, data accessibility, security, and privacy issues. In this regard, *Blockchain* - an advanced *Distributed Ledger Technology* (DLT) works well to address these challenges by linking fragmented and siloed SC events in an immutable audit trail. However, the underlying challenges with blockchain such as scalability, inability to access off-line data, vulnerability to quantum attacks, and high transaction fees necessitate a new solution to overcome the inefficiencies of the current blockchain design. In this regard, *IOTA* (the third generation of DLT) leverages a Directed Acyclic Graph (DAG)-based data structure in contrast to linear data structure of blockchain to address such challenges and facilitate a scalable, quantum-resistant, and miner-free solution for the Internet of Things (IoT). After realizing the crucial requirement of traceability and considering the limitations of blockchain in SC, in this work, we propose a provenance-enabled framework for the Electronics Supply Chain (ESC) through a permissioned IOTA ledger. To that end, we construct a transparent product ledger based on trade event details along with time-stamped SC processes to identify operational disruptions or counterfeiting issues. We further exploit the *Masked Authenticated Messaging* (MAM) protocol provided by IOTA that allows the SC players to procure distributed information while keeping confidential trade flows, ensuring restrictions on data retrieval, and facilitating the integration of fine-grained or coarse-grained data accessibility. Our experimental results show that the time required to construct secure provenance data aggregated from multiple SC entities takes 3 seconds (on average) for a local node and 4 seconds for a remote node, which is justifiable. Furthermore, we perform experiments on Raspberry Pi 3B to verify that the estimated energy consumption at resource-constrained devices is tolerable while implementing the proposed scheme.

Keywords: Blockchain, Distributed Ledger Technology, Internet of Things, Industrial Internet of Things,, Industry 4.0, IOTA, Masked Authenticated Messaging, Provenance, Supply chain, Trustworthy data.

*Corresponding author
Email addresses: sabah@khu.ac.kr (Sabah Suhail), r.hussain@innopolis.ru (Rasheed Hussain), abk15@aber.ac.uk (Abid Khan), cshong@khu.ac.kr (Choong Seon Hong)

1. Introduction

Electronics Supply Chain (ESC) revolves around an intricate and intensive process during which raw materials or natural resources are transformed into circuit boards and electronic components, integrated and assembled into end products, and ultimately made available to the customers. Such a complex product evolution journey involving collaboration among multiple Supply Chain (SC) participating entities, each performing different operations on a product (or its parts), may raise several questions and issues. For instance, how to identify the granular details of the underlying processes such as who, when, what, where, and how the product was derived. To answer these questions, SCs need a *track and trace* mechanism called *provenance* to construct a complete lineage of data, involving products' origin, production, modification, and custody process [1]. Provenance in SC can enable the enterprises to choreograph their demand-supply circle, perform risk assessment, maximize revenues, investigate reasons for product recalls, and forecast their future goals. Furthermore, provenance ensures the integrity of data during data debugging, reconciliation, replication, decision making, performance tuning, auditing, and forensic analysis [2, 3]. However, procuring product provenance data is an exhaustive task which gives rise to several other challenging issues concerning the collection, distribution, accessibility, and security of data. For instance, (i) how to collate provenance data from disparate data silos, complex data aggregation processes, and on-premise operational practices and procedures, (ii) how to assure integrity, reliability, and resiliency of data, (iii) how to ensure the distributed data accessibility and availability to legitimate participating entities, and many more.

Due to the unavailability of a platform that can provide *one-size-fits-all* solution to orchestrate product provenance, it is hard to differentiate between reliable and counterfeit products. To this end, the proliferation of counterfeit products deteriorates consumer trust and also causes reputational damage to the company's image. For instance, defense system manufacturers face difficulty in detecting counterfeit items, as counterfeiters attempt to imitate materials, part numbers, and serial numbers to simulate authentic parts [4]. Similarly, Integrated Circuits (ICs) counterfeiting has been observed in many industrial sectors, including computers, telecommunications, and automotive electronics [5]. For example, in 2018 Orange County electronics distributor was charged with selling counterfeit integrated circuits for military and commercial use [6]. To effectively mitigate the risk across the SC, *atomistic* sources of risk that involves scrutinizing a restricted part of the SC, must be identified. Identifying such risk is suitable for low-value and less complex components. Alternatively, *holistic* sources of risk that involve a comprehensive analysis of the SC must be identified. This kind of risk is preferable for high-value and complex components [7]. In both of these cases, contingency planning is required to identify the root cause of operational disruption and to identify the fraudulent middleman.

The inception of Distributed Ledger Technology (DLT) solves SC challenges by facilitating distributed, immutable, transparent, and fault-tolerant data aggregation across multiple entities (both physical and digital) [8]. In this regard, a blockchain-based architecture is used as a potential solution to fulfill the digital SC requirements in a plethora of SC use-cases (as discussed in Table 1). Table 1 outlines the current research efforts that use blockchain-based solutions for SC use-cases while considering their security aspects. However, current blockchain solutions lack many striking features such as scalability, offline data accessibility, fee-less transactions, and quantum-immunity that are among the desirable features in digital SC. To adequately address these limitations, IOTA [9] brings a transformation in the third generation of DLT. Following a scalable and quantum-immune approach, it securely accelerates tracking and tracing of multiple trade events in the SC even in the offline mode, and consequently enhance provenance data construction to identify counterfeit

products.

In this paper, we investigate the significance of integrating provenance in the ESC, address the research gaps, and highlight the key factors for adopting IOTA in the SC in comparison to existing blockchain-based solutions. More precisely, we propose an IOTA-based framework for supporting provenance in the ESC. By integrating the Masked Authenticated Messaging (MAM) protocol on top of IOTA (as shown in Fig. 1), our proposed framework provides transparent traceability of data throughout the SC, ensuring trustworthy and quality data.

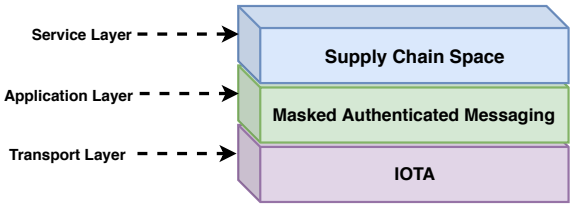


Figure 1: Abstract-level overview of the proposed framework.

The main contributions of this paper are summarized as follows:

- We propose an IOTA-based provenance framework for product traceability that encapsulates the diverse *product story* as *provenance data* at each intermediary process in the ESC. Such a strategy helps to solve the product counterfeiting issue in addition to the problem of fragmented and asymmetric information. To address the security issues, the MAM channel is leveraged to ensure confidential trade flow among competitors, to preserve data integrity, and to provide fine-grained data access to the trusted SC players only.

- We evaluate and show that the proposed scheme is admissible for the ESC in terms of attaching SC data to the IOTA ledger and constructing provenance data by fetching data for varying payload sizes. In doing so, we develop a proof-of-concept for the proposed scheme on the Raspberry Pi 3B hardware platform to mimic the IoT-integrated ESC. Then we analyze the measured average time and energy consumption incurred during attaching and fetching provenance data from the IOTA tangle to validate the efficacy of our proposed scheme.

The rest of the paper is organized as follows. Section 2 surveys related work, provides an overview of IOTA, SC, and discusses the significance of integrating IOTA in SC to support provenance. Section 3 introduces the system model and Section 4 describes the proposed IOTA framework for the ESC. Section 5 presents the simulation results and discusses the security analysis of the proposed approach. Finally, Section 6 concludes the paper with an outlook on future work.

Table 1: Current research efforts pertaining to blockchain-based solutions for SC use-cases and their security aspects.

		SC Technical Challenges											
SC Category	**Scheme**	D	C	I	A	S	AC	Audit	T	OFD	IoT/IIoT	BCID	QI
Food/Agriculture	[10]	✓	✓	✓	✓	⊖	✗	✗	✗	✗	⊖	✗	✗
	[11]	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗
	[12]	✓	✓	✓	✓	⊖	✗	✗	✗	✗	✓	✓	✗
	[13]	✓	✓	✓	✓	✗	✗	✗	✗	✗	⊖	✗	✗
Pharmaceutical/Healthcare	[14]	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	⊖	✗
	[15]	✓	✓	✓	✓	✗	⊖	⊖	✗	✗	✗	✗	✗
	[16]	✓	✓	✓	✓	✗	✗	⊖	✗	✗	✓	✓	✗
Electronics	[17]	✓	✓	✓	✓	⊖	✓	✓	⊖	✗	✗	✓	✗
	[18]	✓	✓	✓	✓	⊖	⊖	✗	⊖	✗	✓	✗	✗
Generic	[19]	✓	✓	✓	✓	✗	✓	✗	⊖	✗	✗	✓	✗
	[20]	✓	✓	✓	✓	✓	✓	⊖	✗	✗	✗	✓	✗
	[21]	✓	✓	✓	✓	✗	⊖	✗	✗	✗	✓	✓	✗

⊖=discussed but details are not provided.
D=Distributed, C=Confidentiality, I=Integrity, A=Availability, S=Scalability, AC=Access Control,
Audit=Auditability, T=Trust, OFD=Off-line data, BCID=Blockchain Implementation Details, QI=Quantum Immune.

2. Related Works

In this section, we survey the related work on DLT-based solutions for SC. We also provide a succinct overview of the current literature that discusses the limitations of the traditional chain-structured blockchains. Moreover, with reference to the limitations of the existing work, we highlight our research contributions. We also provide a quick overview of IOTA, SC, in addition to motivation of using IOTA in SC.

2.1. DLT-Based Solution for SC

Recently, blockchain technology received significant attention to tackle challenging issues (such as traceability and security) in the existing SC legacy system [22]. Blockchain has a very constructive role in SC from different perspectives. For instance, blockchain can provide design decisions and solve most of the challenges related to data management and data security faced by SC. Furthermore, blockchain-based architecture for SC that leverages public or private blockchain, can use different platforms such as Ethereum, Hyperledger Fabric, and Ripple. Many promising blockchain-enabled solutions have been proposed in literature where blockchain is leveraged in SC across different industries, for instance, food, agriculture, pharmaceutical, electronics SCs, to name a few. In Table 1, we summarized technical blockchain-based solutions for various SC categories (application-specific or generalized solutions) and associated shortcomings either in the context of the proposed scheme or the blockchain in particular. In Industry 4.0, blockchain can automate processes among IIoT, cyber-physical systems, and supply partners [23]. For example, [24] discussed the integration of blockchain into the manufacturing industry for data integrity and resilience. Similarly, in [25], the authors proposed a block-chain based platform for small and medium manufacturing enterprises (SMEs) to solve issues such as security, scalability, and big data problems.

In the following, we discuss some of the research works in literature that focus on the non-technical challenges of blockchain-based deployed systems in SCs, for example, in [26], the authors highlighted technical, educational, and regulatory challenges and barriers in agriculture and food SCs. In [27], the authors discussed open research challenges in blockchain-based use-cases, including the Internet of Medical Things (IoMT), healthcare data management, and SC management. Furthermore, the authors of [28] also provided an overview of the challenges associated with blockchain adoption and deployment for the health SC with a focus on pharmaceutical, Internet of Healthy Things (IoHT), and public health. In [29], the authors discussed the factors that bring a positive impact on blockchain-based ESC. Similarly, many other use cases discussing the non-technical aspects of blockchains are discussed in [30, 31, 32, 33].

Recently, various worldwide enterprises have played a significant role in providing blockchain-based platforms for supporting friction-less traceability and transparency in SC, for instance, IBM's blockchain framework [34] has been adopted by Walmart, Nestle, Unilever, and other players in the global Food Supply Chain (FSC) [35]. Other notable blockchain-enabled SC frameworks include Hyperledger [36], skuchain [37], Provenance [38], Blockverify [39], etc. However, the proprietary and private blockchain-based solutions are unable to address the specific requirements in the public domain and portray blockchain as a "black-box".

2.2. Limitations of Blockchain in SC

Most of the blockchain-based solutions adopted for SC theoretically cover advantages, potential challenges, and future directions [40, 41, 42, 43]. However, the underlying constraints of blockchain are overlooked by the current solutions. Among other constraints, *quantum-resistance* and *scalability* are noteworthy. Ongoing efforts to address these potential issues are underway, for instance, to meet the challenging requirement of

quantum future, some of the emerging blockchain solutions that already support post-quantum techniques are Quantum Resistant Ledger (QRL) [44], Quantum-secured blockchain [45], etc. Solutions such as sharding and off-chain are expected to solve the scalability problem of the blockchain. However, these solutions have their own drawbacks. For instance, sharding requires synchronizing the running of operations among different processes on different shards. Furthermore, the overheating of a targeted single shard due to many cross-shard transactions is another problem that requires the ranking of these transactions to prevent overloading of block producers on the target shard. Similarly, off-chain solutions suffer from the following limitations: (i) it introduces additional layers of complexity as the protocols are built on the top of the blockchain, (ii) it may face objection by the government and business communities due to their censorship-resistant nature. Directed Acyclic Graph (DAG)-based blockchain design is another effort to overcome the scalability issue caused by the sequential chain-based design of the traditional blockchain [46]. The authors of [47, 48] provide a comparative analysis of DAG-based blockchain schemes.

Many current research works are raising concerns about the practical adoption of blockchain technology in the SC industry. For instance, some of their concerns are as follows: considering the connection between physical and digital world, how to ensure the reliability of data from SC entities and sensors [49], security concerns due to quantum computing and latency issues with the increasing number of nodes in the network [50, 51], lack of privacy and Garbage In Garbage Out (GIGO) problem [8], lack of information leading to existence of gray markets [46], decision paralysis due to information overload, high energy consumption [52], throughput and latency issues [53], lack of standardization and shifting to new infrastructure from legacy systems [54], etc. But paradoxically on the other side, solutions such as [1, 40, 42, 55, 56] focus on the significance of using blockchain in SC. Overall, most of the proposed schemes (discussed in Table 1) failed to address the potential current problem (such as scalability) and most importantly future issues (such as quantum-resistance against cyber attacks) of blockchain. Moreover, other technical requirements of SC such as accessibility and auditability based on roles and access levels, are also overlooked.

The common denominator among DLTs is their reliance on a distributed, decentralized peer-to-peer network, and consensus mechanism. However, DLTs vary substantially in terms of the underlying data structure, fault tolerance, and consensus approaches [57]. In addition to blockchain and its different flavors, other well-known DLTs are tangle, hashgraph, sidechain, and holochains. In [57], the authors provided a comparative analysis of DLTs, whereas, in [48], the authors compared classical blockchain with DAG-based blockchain. Considering the primary challenge, i.e., scalability, faced by blockchain-based solutions in SCs, we consider a DAG-based DLT, i.e., IOTA. In comparison to other DLTs, IOTA exhibits quantum immune nature, provides off-line data accessibility, and supports fee-less microtransactions that are important factors for future SCs.

2.3. Our Research Contributions

This research is aimed to highlight the current research gaps in SCs and propose a state-of-the-art approach to resolve them. Though the existing blockchain-based solutions for SC have solved the primitive problems associated with disjoint data fragments, third party dependency, data security, and many other problems related to legacy systems. Nevertheless, there are still overlooked issues that need to be addressed. In this regard, our contributions include the following key factors that are required to incorporate in a DLT-enabled SC.

Firstly, *Why is the transition from mainstream blockchain to IOTA required?* We adopt IOTA DLT upon realizing the overlooked constraints of blockchain. For instance, scalability issues, particularly in case of

growing participating entities; accessing data from freights in remote areas or off-line mode; dealing with transaction fees, and finally reliance on the security of current cryptographic primitives keeping in view the not-so-far arrival of quantum computers. Secondly, *how to create transparency towards the consumers?* To win consumers' trust, it is important to give them a sheer picture of the product journey. We devise a mechanism that involves reconstructing a trustworthy product provenance story. Thirdly, *how to define customized data access control rights?* We use the MAM protocol to provide fine-grained data access privileges to facilitate the trade secrets of participating entities. Fourthly, *how to identify counterfeit products?* We construct provenance data such that it includes complete information to identify the illegitimate or defective item.

For illustrative purposes, we consider the example of mobile phones in ESC. While keeping the underlying framework intact, the proposed model is suitable for any commodity in ESC. Furthermore, it can be customized to other non-electronics SCs (for example, food-agriculture, pharmaceuticals) keeping in view the diverse requirements driven by their specific business needs and additional information (e.g., expiry dates or any other precautionary measures). For instance, food-agriculture, pharmaceuticals, or any other cold chain differs from ESC as they are subject to sensitive temperature and environmental conditions necessary to maintain the quality of perishable items in terms of temperature, humidity, etc. Similarly, ESC differs from other SCs based on quality testing, such as expiry period in case of cold chains are completely different from the warranty period determined through failure testing/product life testing of electronic components. Other differences include the packaging and assembling of components at various stages. Such requirements of cold SCs can be facilitated through our proposed model by continuous monitoring and reporting of the sensor data at frequent intervals to ensure the quality of products while allowing the integration of any optional information. Therefore, by tweaking the parameters based on the details of the underlying SC case, the proposed framework can be applied to any other SC.

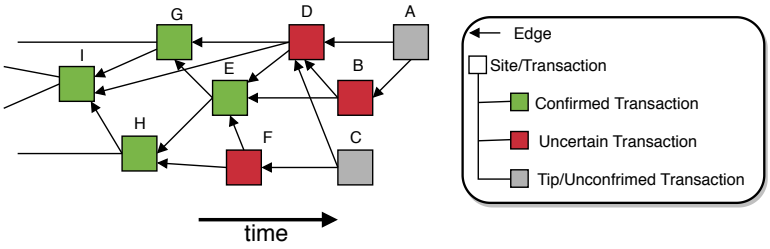


Figure 2: Tangle graph illustrating transactions and edge set connecting transactions.

2.4. IOTA in SC: An Overview

In the following, we provide a quick overview of IOTA and SC. We also emphasize on using IOTA DLT in the SC.

2.4.1. IOTA

IOTA is a public, permissionless, and distributed ledger that leverages directed acyclic graph (DAG) data structure termed as *tangle* for storing interlinked but individual transactions exchanged among peers [9]. Fig. 2 shows a tangle graph where each square-block represents a *transaction/site* which is propagated by a *node*. Every new transaction attached to the tangle graph forms an edge set. To create a transaction, a node

(i) creates and signs a transaction with its private key, (ii) use the Markov Chain Monte Carlo (MCMC) algorithm [58] to choose and validate two other non-conflicting unconfirmed transactions (tips), and (iii) solve a cryptographic puzzle (known as Hashcash) to perform Proof of Work (PoW) for preventing Sybil attacks. Transaction status can be categorized as confirmed transactions (green nodes), uncertain transactions (red nodes), and unconfirmed transactions or tips (grey nodes), as shown in Fig. 2. The revolutionary features of IOTA including scalability, decentralization, zero transaction fee, speedy microtransactions, off-line capability, and quantum security enables it to gain ground not only in Machine-to-Machine (M2M) economy but also in application areas encompassing Industrial IoT (IIoT).

2.4.2. Supply Chain

Supply chain encompasses coordination and collaboration among channel partners (suppliers, intermediaries, third-party service providers, and customers) for planning and managing upstream and downstream process-based activities such as the transformation of natural resources/raw materials, sourcing, procurement, production, conversion, and logistics. Fig. 3 shows the primary entities involved in the production of mobile phones in the ESC.

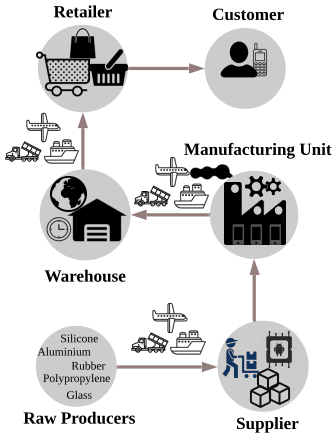


Figure 3: Electronic supply chain showing participating players involved in supply chain processes.

2.4.3. Motivation: Integrating Provenance Support in the Electronics Supply Chain Through IOTA

SCs empower participants for collaborative commerce in a global value chain. A product (for instance, mobile phone) journey from *sand to hand*, comprises numerous chained phases during which components are produced, sourced, refined, integrated, and assembled by multiple entities ubiquitously. Nevertheless, numerous friction points thwart SCs from accomplishing their maximum potential, for instance, opaque mechanics of global commerce, complexity (upstream and downstream), manual processes, and divergent standards. Furthermore, SCs are held back by imperfect and asymmetric information as huge volumes of veracious data are inaccessible to the SC players. This happens particularly during cross-border trading resulting in communication gaps, increased costs, erroneous data aggregation, scattered information, market failures, or absence of markets at all. Therefore, it can be concluded that a sustainable SC stipulates two pivotal features to be incorporated: (i) *Product story*, and (ii) *Orchestrating episodes of product story.*

Provenance: Product Story

To trace the audit trail of data, provenance plays a significant role in constructing a "product story" throughout the SC. The product story (or product traceability) enables the seller-buyer pair to trace the product from its inventory procurement process to its point of sale and hence provides an efficient way for tackling counterfeits or determining liability in the event of faulty records. For instance, upon scanning the Quick Response (QR) code, the consumer can look at the product story.

IOTA: Orchestrating Product Story

Relying solely on provenance to record trustworthy data is not sufficient, therefore, to efficiently and proactively systematize the product story in terms of provenance data, we collocate the product story in a tamper-proof product ledger maintained by IOTA. IOTA ledger provides data auditability to identify accountable actors causing data contamination, reasonable confidentiality and privacy of the trade flows, and access control on immutable and trustworthy data. Thus, acquiring real-time provenance data (such as location information, transfer of custody, monitoring environmental conditions during storing and shipping of products through GPS, RFID tags, temperature sensors, humidity sensors, etc.) can help in decision-making and risk mitigation.

Symbol	Description
QC	Quality Control
T_{ID}, B_{ID}, C_{ID}, S_{ID}	Transaction ID, Batch ID, Component ID, Sensor ID
$Payload_a$, $Payload_f$	Attach payload, Fetch payload
D_p	Data publisher or Seller
D_r	Data receiver or Buyer
$\mathcal{K}$	Authorization key
$\mathcal{K}_{pu}$, $\mathcal{K}_{pr}$	Public key pair, Private key pair
T_{Data}, A_{Data}	Transaction data, Auxiliary data
P_{Data}, $P_{collect}$, P_{aggr}	Provenance data, Provenance collect, Provenance aggregate
T_{Data}, A_{Data}, S_{Data}	Transaction data, Auxiliary data, Sensor data
Con_{info}	Consignment information
Reg_{cert}	Certificate by regulatory authority
s_d	data from sensor devices
Src_{ID}, $Prev_{TID}$	Source ID, Previous Transaction ID

Table 2: List of notations

3. System Model of the Proposed IOTA-based SC

In this section, we provide an overview of the design parameters necessary for the SC system. We describe the network model and the data model that we consider for our proposed IOTA-based provenance scheme for SC. We also present the provenance model along with the outline of elemental provenance data components that are utilized in our proposed scheme. Finally, we discuss the security goals that our proposed scheme aims to achieve.

3.1. Design Approach

In this subsection, we highlight the factors that we consider while proposing a provenance-based solution for SC. It is worth mentioning that primarily we focus on addressing technical challenges in the proposed

solution.

The *first* factor (F-I) is to identify the information type and source, for instance, level of information (coarse-grained or fine-grained), data acquiring source such as digital assets or humans (each having different repercussions), etc. Comprehensive data aggregated from multiple data sources play a significant role in solving many problems such as data traceability, risk factors in trade events, etc. Additionally, data retrieval necessitates the evaluation of the proposed scheme with respect to performance and energy constraints, for instance, the time and energy required to construct secure provenance data aggregated from multiple SC entities.

The *second* factor (F-II) is to identify erroneous data in the system to ensure data trustworthiness which in turn can solve many issues such as bullwhip effect, GIGO problem, trust issues between seller-buyer pair, etc. Erroneous data refer to the state of data before it arrives at the ledger, i.e., during data generation and data transit. Erroneous data can be generated (either maliciously or mistakenly) by (i) source/data originator, (ii) intermediate entities, (iii) SC participating entities, and (iv) sensors or other technologies connecting the physical and digital world.

The *third* factor (F-III) is to identify the best practices for Supply Chain Risk Management (SCRM). SCRM involves processes to identify risk events and to activate a plan accordingly to mitigate its effect. Problems such as shrinkage, outage, natural disasters, economic crisis, etc. are covered under this factor.

The *fourth* factor (F-IV) is the integration of state-of-the-art technologies such as IIoT as industrial adaptation of the IoT, Industry 4.0 along with use of cyber-physical systems in the manufacturing industries, DLT, others. Such integration can automate industrial processes with minimal human involvement.

The *fifth* factor (F-V) is the evaluation of non-technical factors such as Ethical, Sustainable, and Responsible (ESR) operations as discussed in [46]. ESR operations deal with issues, such as labor conditions, child labor, responsible usage of natural resources (land, water, energy), etc.

Note that, the above-mentioned factors are tightly inter-linked with each other, i.e., failure to exercise any one of the factors can highly affect the outcome of the other factor.

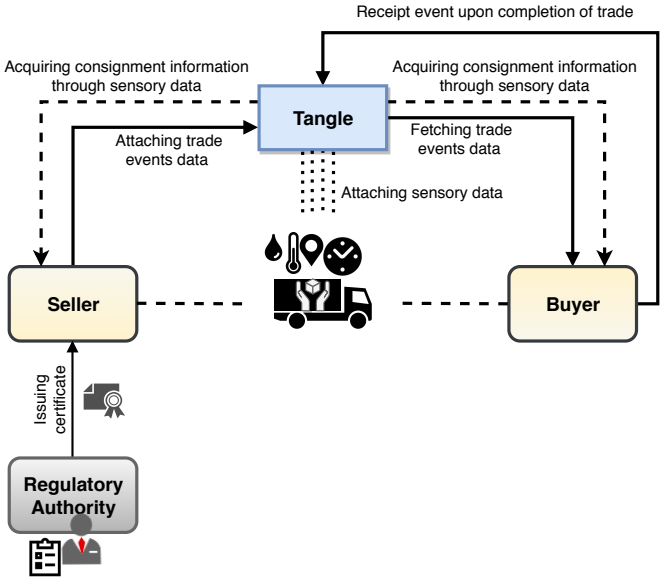


Figure 4: Network model illustrating a trade event between seller-buyer pair.

3.2. Network Model

Our network model consists of SC entities (participating and non-participating) and sensors. In the following, we outline two main data sources in the ESC, i.e., SC players and sensors.

3.2.1. SC Players

The following are the participating players in ESC.

(i) Raw producers, (ii) Suppliers, (iii) Manufacturers, (iv) Warehouses, (v) Logistics, and (vi) Retailers. The raw producers provide raw materials to the supplier to produce chip-sets and other peripherals. Those components are fabricated and assembled at a manufacturing unit. The finished products (for instance, mobile phones) are delivered to the warehouses for distribution. Finally, customers can purchase them from designated retailers.

Additionally, there are non-participating players such as (i) customers, and (ii) researchers/analysts. Non-participating members are not involved in the SC process; however, they may need to fetch the production and manufacturing information about the products. Hence, they are also considered as part of our network model.

3.2.2. Sensors

Sensors are used to connect the physical world to the digital world. Sensors are affixed to batches during logistics and transportation to provide information such as location, temperature, humidity, etc. Due to the resource-constrained nature of sensors, we assume that such devices act as light nodes and may utilize the full nodes for performing computationally expensive tasks of the IOTA framework. For further processing, interpretation, and analysis of data, the sensor data is fetched from the tangle to track and trace SC events (handling of design factor F-IV).

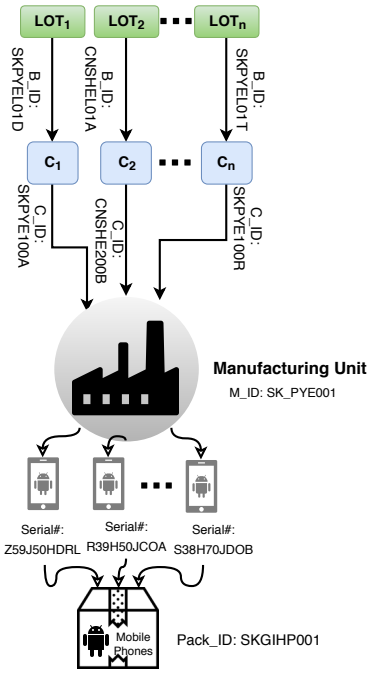


Figure 5: Product manufacturing and assembly at the manufacturing unit.

3.3. Data Model

We assume that each SC entity acts as a *Data Publisher* (D_p) and publishes its data (also referred to as *attaching data*) on its *MAM channel* identified by $Channel_{ID}$. On the other hand, the interested viewers act as a *Data Receiver* (D_r) and subscribe to the desired channel ($\mathcal{C}$) to gain access to the data (also referred to as *fetching data*) by using an authorization key ($\mathcal{K}$). The term $\mathcal{K}$ is collectively used for public $\mathcal{K}_{pu}$ and private $\mathcal{K}_{pr}$ key pairs.

In the context of SC, D_p and D_r can be referred to as *Seller* and *Buyer* respectively. The data (also referred as payload) consists of (i) Transaction data (T_{Data}), (ii) Auxiliary data (A_{Data}), and (iii) Sensor data (S_{Data}) can be represented as:

$$Payload \leftarrow T_{Data}||A_{Data}||S_{Data}, \tag{1a}$$

$$T_{Data} \leftarrow T_{ID}||Seller_{ID}||Buyer_{ID}||Con_{info}, \tag{1b}$$

$$A_{Data} \leftarrow QC||Reg_{cert}||optional\_field, \tag{1c}$$

$$S_{Data} \leftarrow S_{ID}||Channel_{ID}||s\_d||timestamp. \tag{1d}$$

T_{Data} consists of transaction ID (T_{ID}), trade event as $\langle source, destination \rangle$ pair, i.e., seller ID ($Supplier_{ID}$) and buyer ID ($Buyer_{ID}$), and consignment information (Con_{info}). Con_{info} may include batch ID (B_{ID}), component ID (C_{ID}), make and model number (as depicted in Fig. 5 and Fig. 7). Other granular details such as quantity, unit price, vehicle ID, etc., can also be included as a part of Con_{info} (handling of design factor F-I).

A_{Data} consists of Quality Control (QC) parameters (such as ISO certifications/accreditation, warranty, etc.), regulatory endorsements certificates (Reg_{cert}), and optional field ($optional\_field$). We consider $optional\_field$ to store application-specific or user-specific information, for example, pre-defined agreements among trading entities. In our case, we use this field to store packaging information (i.e., traceability information) related to items that may need to be packed together and extracted at a later stage such as during assembling mobile phone parts or during burning software on ICs. Traceability information includes *where* a particular package is reopened by *which* entity due to *what* reason. Besides, it may contain information about shrinkage events in case of loss or damage to physical goods (handling of design factor F-III). Among other quality control parameters, warranty plays an effective role as it provides a marketing strategy to attract customers and also signals product quality [59]. In our case, this factor can also contribute to establishing a trust relationship among buyers (consumers) and sellers (honest or dishonest) in the long run. The regulatory endorsements can help to ascertain that SC processes are abiding by ethical practices and environmentally-responsible operations. The exercising of such ESR operations requires the involvement of regulatory bodies (NGOs, governments, industry self-regulators) to conduct a periodic on-site inspection of the units and provides verifiable certificates (Reg_{cert}) (handling of design factor F-V) as shown in Fig. 4. Note that we have not formally followed any certificate issuing organization's procedures and policies. We consider the inclusion of a certificate (document) as a part of the payload where the certificate holds some basic information about following ESR operations. The fields in the certificate and its revocation criteria can be further customized to fulfill the requirements of such organizations.

S_{Data} consists of sensor ID (S_{ID}) assigned to each sensor, $Channel_{ID}$ of D_p publishing the sensor data (s_d) such as location, temperature, humidity along with timestamp information. During transportation and logistics of goods, s_d is attached to the tangle and can be accessed by seller-buyer pair to acquire Con_{info} as shown in Fig. 4. The granularity level of s_d can be customized depending on the requirements, for instance, coarse-grained data by averaging temperature data or fine-grained data by using channel splitting option.

When a product or its parts are received by the buying entity, the receipt (*Receipt*) is generated to log the completion of the trade event between the seller-buyer pair (as shown in Fig. 4).

$$Receipt \leftarrow T_{ID}||status, \tag{2}$$

where T_{ID} and *status* represent the transaction ID and status of the received item respectively. The purpose of introducing this transaction is threefold: (1) to keep track of the successful transactions to avoid any fake-progressive sub-chains, (2) to indicate any loss or damage event, and (3) to integrate trade finance processes in SC.

3.4. Provenance Model

Deriving the product story primarily involves collecting provenance data (P_{Data}) based on $\langle source, destination \rangle$ pairs while traversing through the SC process. Therefore, to construct and assemble P_{Data}, firstly the payload (holding complete transaction and auxiliary data) is fetched from the ledger, and secondly the required information is acquired from the fetched payload ($Payload_f$). The key factors to devise product provenance are:

$$P_{Data} \leftarrow Channel_{ID}||T_{ID}||Src_{ID}||Prev_{TID}, \tag{3}$$

where $Channel_{ID}$ refers to the current ID of source, Src_{ID} refers to the channel ID of destination (i.e., immediate $Channel_{ID}$ of SC entity), and $Prev_{TID}$ refers to the on-going transaction in the channel of Src_{ID} pertaining to the fact that there can be multiple on-going transactions in that channel. Note that depending on the query, additional information can be obtained from T_{Data}, A_{Data}, and S_{Data} accordingly. Also, P_{Data} can be encoded on a QR code to be used by SC entities.

3.5. Security Goals

Keeping in view the requirements of SC, our proposed scheme aims to achieve the following security properties:

1. **Data confidentiality:** To hide classified trade information among competitors, it is essential to encrypt data communication.
2. **Access control rights:** Defining access control rights is indispensable to conceal classified trade information among competitors. Moreover, sharing only a subset of data at any desired point in time must be allowable by the SC player.
3. **Restrictions on data retrieval:** Upon joining the data stream of the SC process, SC players must only be able to retrieve the information at or after their entry point to the process with no privileges to previous transaction streams.
4. **Data integrity:** Integrity of trade events must also be ensured during data creation and sharing.

5. **Non-repudiation:** Any participating entity must not be able to deny an SC event that has happened or SC data that has been produced.

In the following, we utilize the above-mentioned components in our proposed approach while considering the design factors and security objectives.

4. Proposed Framework: Procuring Provenance in ESC Through IOTA

In this section, we provide a brief overview of the characteristics and working of the MAM protocol provided by IOTA. We also devise the proposed framework for provenance in SC using IOTA with the help of algorithms and flow diagrams.

4.1. Masked Authenticated Messaging (MAM)

To ensure secure, encrypted, and authenticated data streams on the tangle, we leverage a MAM module that provides a channel where data owners who publish the data and data viewers who subscribe, meet. Using the gossip protocol, the message from the data publisher is propagated through the network and can be accessed by the channel subscribers only.

4.1.1. Generating Message Chain

A MAM transaction bundle consists of two sections including (i) *Signature*, and (ii) *MAM*.
Fig. 6 shows the main components of *MAM Transaction Bundle*.

The "MAM section" contains the masked message. To post a masked message, MAM deploys *Merkle tree-based signature scheme* [60] that requires the creation of a root to view the payload. Furthermore, to support forward transaction linking, the MAM section also contains a connecting pointer i.e.,*nextRoot* and other associated entities that are required for fetching the next payload. The approach to access the payload depends on the channel mode used, for instance, restricted channel mode requires authorization key pairs to encode and decode messages.

For the validity check of the MAM section, data publishers add a signature in the MAM bundle and store it in the *signature Message Fragment(sMF)* of the transaction. Such transactions are stored in "Signature section" of the MAM bundle. A comprehensive working of the MAM protocol is explained in [61].

4.1.2. Access Control and Provision of Authenticated Data

To control the data accessibility and visibility in the tangle, MAM provides the following channel modes: (i) *public*: address = root, i.e., by using the address of the message, any random user can decode it, (ii) *private*: address = hash(root), i.e., the hash of the Merkle root is used as the address, thus, preventing random users from deciphering message as they are unable to derive the root from the hash, and (iii) *restricted*: address = *hash(root) + authorization key*, i.e., the hash of the authorization key and the Merkle root is used as address, thereby allowing only authorized parties to read and reconstruct the data stream. Changing the authorization key results in revoking permission to access the data without requiring the data publisher to change its $Channel_{ID}$. It is important to note that considering the confidential trade flow requirements of the SC players, we prefer the use of restricted channel mode of MAM. Furthermore, to enforce the ownership of the channel, signature validation is performed upon message reception to authenticate the source of the message or in other words to validate the ownership of the publisher. Failure to signature verification results in an invalid message.

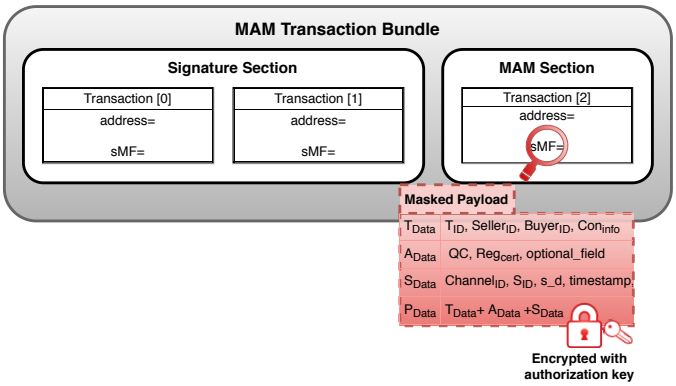


Figure 6: MAM transaction bundle illustrating *signature section* and *MAM section*. MAM section consists of *Masked Payload* encrypted with authorization key (restricted channel mode). Masked Payload consists of transaction data T_{Data}, auxiliary data A_{Data}, and sensor data S_{Data} whereas P_{Data} can be constructed from T_{Data}, A_{Data}, and S_{Data}.

4.2. Provenance in ESC

In this subsection, we provide a detailed description of the proposed provenance-based SC framework.

4.2.1. Seed Generation

To initiate the communication process based on the address and private key requires a seed. A seed is more like a private key and consists of 81 characters including upper case alphabets and digit 9. The seed generation process uses environmental noise (for example, device drivers, network packet timing, etc.) as an input to a Cryptographic Secure Pseudorandom Number Generator (CSPRNG), to produce random seed values.

4.2.2. Setting Security Level, Channel Mode, and Key Generation

IOTA has defined three security levels: 1 (low), 2 (medium), and 3 (high). The default security level is 2; however, we use the recommended security level 3. To keep the communication confidential, we set the channel mode as "*restricted*" so that the authorized parties can access the data based on shared authorization key pairs. The authorization key $\mathcal{K}$ is used to encrypt and decrypt the payload by a sender and receiver entities, respectively. The cryptographic keys can be shared among the participating parties by using any of the existing key exchange techniques, for instance, Elliptic Curve Cryptosystems (ECDSA or ECDH). However, the existing key exchange systems are at risk of being broken due to quantum computing attacks, therefore, a lattice-based public-key cryptosystem N*th* Degree Truncated Polynomial Ring (NTRU) must be adopted as it allows to generate and exchange key pairs in a quantum secure way. In our case, we use the NTRU key exchange protocol.

4.2.3. Data Publishing

Each SC player creates a channel $\mathcal{C}$ to publish its data on the tangle. For further details of the payload and its sub-entities, we refer to Section 3.3. Upon selection of channel mode, security level, and authorization key, finally, the MAM transaction bundle is attached ($Payload_a$) to the tangle. Algorithm 1 illustrates the steps of data publishing.

Algorithm 1 Data publishing

Input: $seed, root$
Output: $Payload_a$
1: mamState ← Mam.init (iotaObject, seed, securityLevel)
2: mamState ← Mam.changeMode (mamState, channelMode, $\mathcal{K}_{pub}$) ▷ Set channelMode as 'restricted' and use public key pair to encrypt the payload.
3: MAMObject ← Mam.create (mamState, payload) ▷ Create MAM payload which consists of transaction and auxiliary data.
4: Mam.attach (MAMObject.payload, MAMObject.address) ▷ Attach the payload to the tangle.

4.2.4. Data Receiving

The interested SC players subscribe to the channel to view the published data. The subscribers are able to receive or fetch payload ($Payload_f$) based on root and decipher the payload based on $\mathcal{K}$, as presented in Algorithm 2.

Algorithm 2 Data receiving

Input: $root$
Output: $Payload_f$
1: mamState ← Mam.init (iotaObject, seed, securityLevel) ▷ Set seed value and securityLevel as used in Algo. 1.
2: mamState ← Mam.changeMode (mamState, channelMode, $\mathcal{K}_{pr}$) ▷ Set channelMode and private key pair to decrypt the payload.
3: Mam.fetch (root, restricted, $\mathcal{K}$) ▷ Fetch message stream from the tangle.

It is important to mention that IOTA enables flexible integration of the sensor data (S_{Data}) in the tangle. Hence, S_{Data} can be published, fetched, and analyzed following a similar approach as that of data publishing and data receiving. For instance, the consignment information can be acquired by the seller or buyer as shown in Fig. 4.

Algorithm 3 Collecting and aggregating provenance data from the fetched payload

Input: $root$
Output: P_{Data}
1: **procedure** FETCH_AGGR(P_{Data})
2: **do**
3: **for** `each subscribed channel` $\mathcal{C}_i$ **do**
4: Mam.fetchSingle (root, restricted, $\mathcal{K}$) ▷ Fetch transaction from the subscribed channel.
5: $Payload_f = T_{Data}||A_{Data}||S_{Data}$ ▷ Fetch and decipher the payload.
6: $P_{collect} \leftarrow Channel_{ID} \,||\, T_{ID} \,||\, Src_{ID} \,||\, Prev_{TID}$ ▷ Collect provenance data from fetched_payload.
7: $P_{aggr} \leftarrow P_{collect} \,||\, A_{Data} \,||\, S_{Data}$ ▷ Aggregate other granular details (if required).
8: $P_{Data} \leftarrow P_{aggr}$
9: goto $\langle Src_{ID} \rangle$ channel ▷ Go to the intermediate source channel.
10: look for $Prev_{TID} == T_{ID}$ ▷ Look up for the transaction ID.
11: **end for**
12: **while** $\langle Src_{ID} \rangle \neq$ NULL
13: **end procedure**

4.2.5. Collecting and Aggregating Provenance Data

Collecting P_{Data} consists of three steps: (i) fetching payload ($Payload_f$), (ii) collecting provenance ($P_{collect}$), and (iii) aggregating provenance (P_{aggr}). Firstly, the payload is fetched from the tangle. Secondly, upon fetching the payload, $P_{collect}$ collects the information using key identifiers as mentioned in eq. 3. Thirdly, the collected provenance information is maintained as P_{aggr} along with other granular details (including consignment information, timestamped sensor data, quality control information, etc.). Finally, P_{aggr} is then stored as P_{Data}. $\langle Src_{ID} \rangle$ refers to the channel address of the SC player who publishes the data through transaction $Prev_{TID}$. Throughout the chain, $\langle Src_{ID} \rangle$ helps in locating back to the intermediaries and ultimately the originator. Hence, moving to the next channel to collect, and aggregate provenance information is based on $\langle Src_{ID} \rangle$ and $Prev_{TID}$ to obtain the respective transaction. The process of fetching and aggregating provenance continues until the supplier is found. The steps for collecting and aggregating provenance data from the payload are illustrated in Algorithm 3.

In order to explain the fetching and aggregating of P_{Data}, let us consider Fig. 7. Suppose that a SC player (customer or analyst) wants to trace back the product journey. Firstly, key identifiers are fetched, i.e., T_{ID}=SM-G8846, $Product_{ID}$=R39H50JCOA, and $Channel_{ID}$=R_ID: SK_SEL679 from the *Retailer*

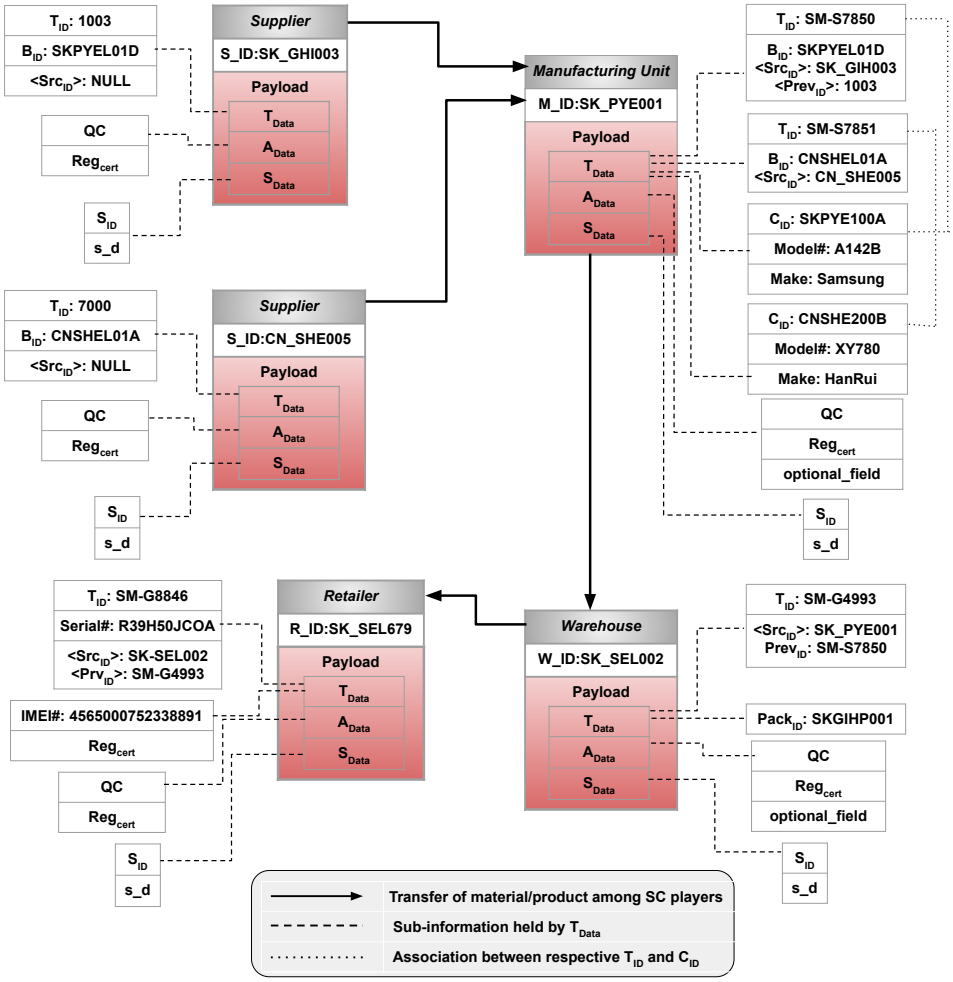


Figure 7: Product ledger: an example scenario illustrating the process of collection and aggregation of *provenance data* throughout the ESC.

channel. Secondly, fetched data and auxiliary data are aggregated and collected in P_{Data}. Thirdly, based on the $\langle Src_{ID} \rangle$=SK_SEL002 and $Prev_{TID}$=SM-G4993, the provenance information (for instance, $Pack_{ID}$= SKGIHP001), is then fetched from next *Warehouse* channel such that $Prev_{TID}$ equals T_{ID}. Similarly, following $Prev_{TID}$=SM-S7850 and $\langle Src_{ID} \rangle$=M_ID: SK_PYE001 the information related to batch B_{ID}, model# and make is obtained from *Manufacturing Unit* channel. Here we can see that the batches holding components may arrive from different suppliers located in different countries. Hence, based on T_{ID}=SM-S7850, B_{ID}=SKPYEL01D and C_{ID}=SKPYE100A information are obtained. Also $\langle Src_{ID} \rangle$=S_ID: SK_GIH003 is used to reach the respective *Supplier* channel. Since $\langle Src_{ID} \rangle$=NULL, therefore, no further $channel_{ID}$ is required to fetch more information. It is important to note that the additional information can be collected and aggregated from T_{Data}, A_{Data}, and S_{Data} based on the user's query (Step 7). The query results also depend on access privileges defined by the SC players. Furthermore, the data can be fetched from any channel by any of the participating entities at any instant of time by using provenance key identifiers.

Platform name	CPU	CPU core	Number of cores
Desktop machine	Intel Core i5-3330	-	4 (per socket)
Raspberry Pi 3B [62]	BCM2837	Cortex-A53	4

Table 3: Specifications for hardware platforms.

5. Performance Evaluation

In this section, we evaluate the proposed IOTA-based provenance scheme for SC. Overall, we consider 4 IOTA operations including (i) create, (ii) PoW, (iii) attach the payload to the tangle, and (iv) fetch payload from the tangle. Among these operations, we focus on attaching and fetching latency metrics. We also analyze the security of the proposed scheme with respect to SC requirements.

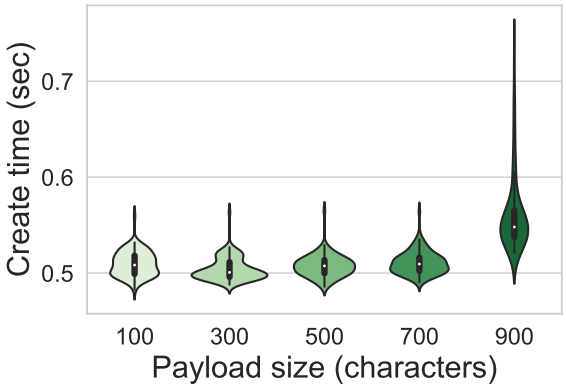


Figure 8: Estimated time (sec) required to create payload.

5.1. Simulation Setup

5.1.1. Hardware

To evaluate the performance of the proposed scheme, we use a desktop machine and a Raspberry Pi 3B. The summary of hardware specifications for the test environment is shown in Table 3.

5.1.2. Software

To evaluate IOTA operations, we use JavaScript and compile it for the considered target platforms. Both target platforms are running Linux operating system (Ubuntu 16.04 LTS). For operations including creating payload, attaching payload to the tangle, and fetching payload from the tangle, we use the current implementation of MAM protocol. We evaluate the proposed scheme for security level 3. For local PoW, we use a PoW proxy server that acts as a dedicated proxy server to perform PoW for the targeted node. To carry out this operation, we use CCurl[1] library developed and maintained by the IOTA Foundation. We also use a remote node selected from the available IOTA nodes list which is responsible for carrying out PoW on behalf of the targeted node.

5.2. Evaluation Metrics

We put emphasis on the latency metric for the evaluation of IOTA operations. Each experiment is evaluated 100 times for security level 3. To represent the data distribution, we choose violin graph that befits our representation requirements of the results. The violin graph indicates median (a white dot), quartiles (thick black bar) with whiskers reaching up to 1.5 times the inter-quartile range (thin black bar), and kernel probability density (colored area) that shows the distribution shape of data. With reference to the proposed scheme, parameters of the violin graph can be interpreted as follows: median represents the central value for performing IOTA operations (including creating, attaching, and fetching), whereas quartiles represent the overall range of data while performing IOTA operations. Starting with payload creation, Fig. 8 shows that the time required to create the payload is almost negligible. However, it is observed that for payload size 900 the distribution of data is different in comparison to others. The reason for such different behavior is particularly because of the creation of the bundle. In addition, if the payload size increases more than 2187 trytes (1300 characters) additional transactions in the bundle are required.

Next, we analyze the process of attaching payload to the tangle, fetching payload from the tangle, and PoW (local and remote) due to the fact that such IOTA operations have significant time delays in comparison to creating payload.

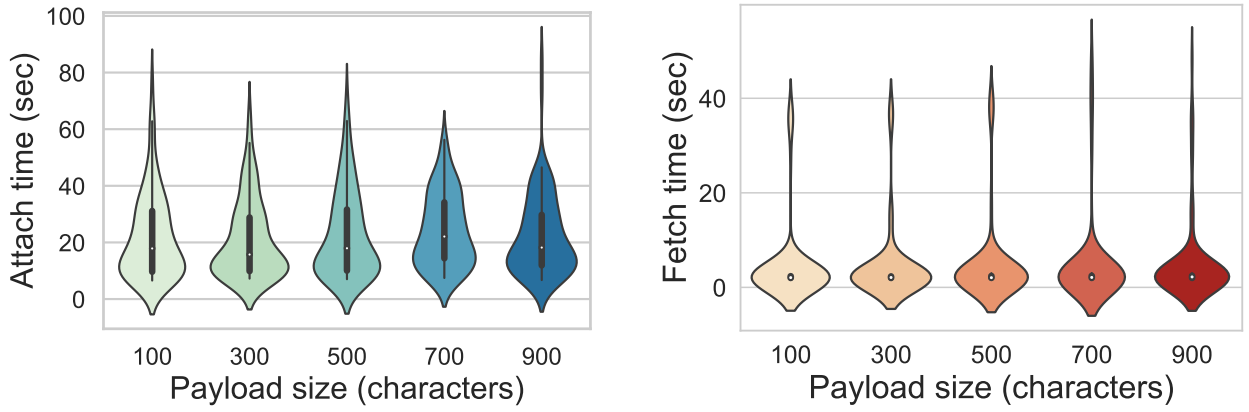
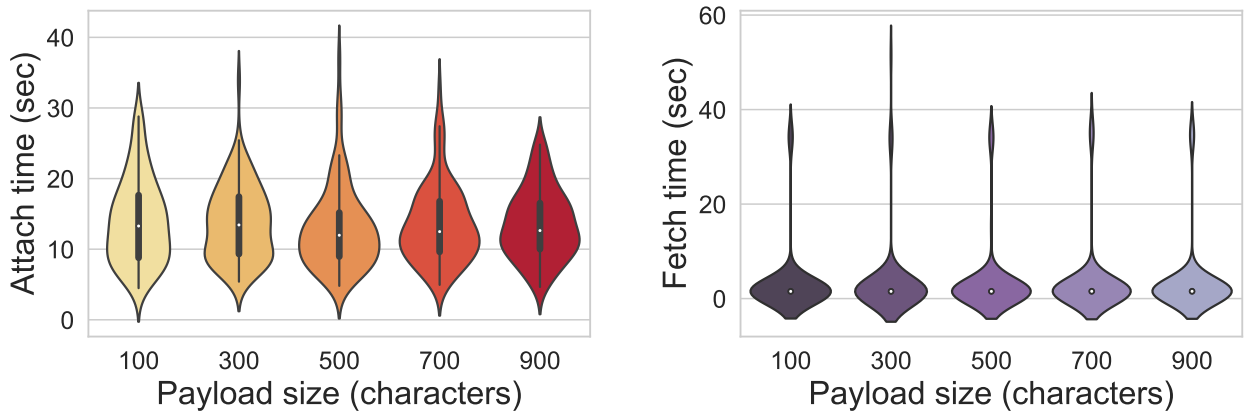


Figure 9: Estimated time (in sec) required to (a) attach data to the tangle, (b) fetch data from the tangle by using remote node.

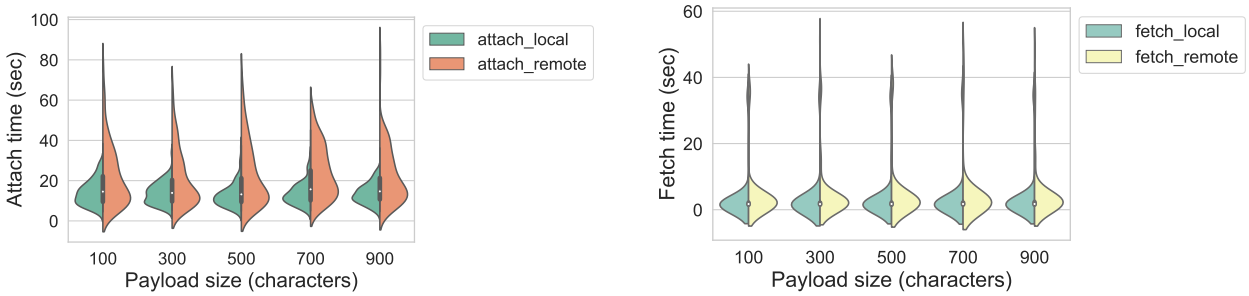
[1]https://github.com/iotaledger/ccurl



(a) **(b)**

Figure 10: Estimated time (in sec) required to (a) attach data to the tangle, (b) fetch data from the tangle by using local node.

It is important to note that the *attach phase* corresponds to $Payload_a$ (attaching payload (consisting of T_{Data} and A_{Data})) while the *fetch phase* corresponds to $Payload_f$ (fetching payload) from which P_{Data} can be constructed. Depending on the query criteria and access privileges defined on the basis of channel splitting, P_{Data} can be constructed. For simplicity, we consider that the query acquires every possible detail (i.e., entire payload) during the fetch phase based on which the provenance information can be derived upon the request of participating and non-participating entities.



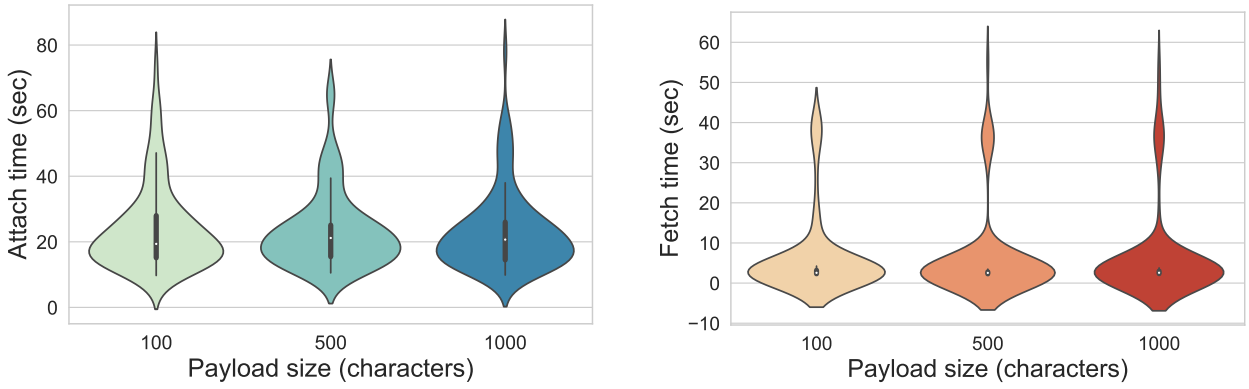
(a) **(b)**

Figure 11: Comparison between processing time required by local and remote nodes: estimated time (in sec) required to (a) attach data to the tangle, (b) fetch data from the tangle.

Keeping in view the above-mentioned definitions of attaching and fetching data, firstly, we perform the attaching and fetching of payload (shown in Fig. 9) by relying on a remote node and secondly, we perform the attaching and fetching of payload (shown in Fig. 10) by using a local node. In either of the cases, it is observed that the attaching process consumes more time in comparison to the fetching process. Both the attaching and fetching phases are independent of the payload size ranging from 100 to 900 characters. Similarly, we compare the attach and fetch process with respect to remote and local nodes. Figure 11 shows that relying on a remote node to perform PoW incurs time delays and hence consumes time, whereas local PoW does not incur much delays. In particular, Fig. 11 represents the distribution of data for performing IOTA operations remotely and locally such that the median value for attaching payload is around 17 sec and 12 sec respectively, while the median value for fetching data is around 2 sec and 1 sec respectively.

Operation	Average Time (sec)	Energy Consumption (J)
Attach	23.1	5.1
Fetch	6.4	1.4

Table 4: Average time measured and energy consumption estimated for attaching and fetching data from the tangle through Raspberry Pi 3B.



(a) **(b)**

Figure 12: Raspberry Pi 3B: Estimated time (in sec) required to (a) attach data to the tangle, (b) fetch data from the tangle.

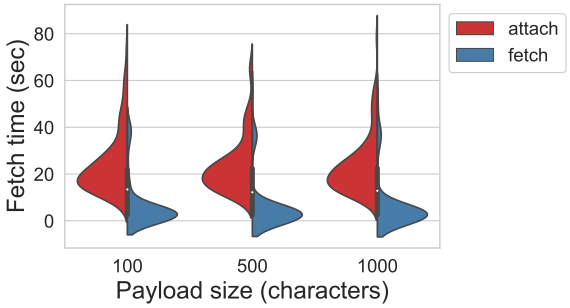


Figure 13: Comparison between estimated time (in sec) required by Raspberry Pi 3B to (a) attach data to the tangle, (b) fetch data from the tangle.

Similarly, to simulate the proposed scheme on an IoT platform, we use Raspberry Pi 3B. On this platform, we consider the attaching and fetching process in terms of time and energy constraints. To include sensor data, we use the Digital Humidity Temperature sensor (DHT11). We assume that any other sensor data can be integrated in a similar way to attach and fetch sensor data to/from the tangle, respectively. Firstly, we compute the average time required to attach and fetch payload (including sensor data) to and from the tangle, respectively (shown in Fig. 12). In particular, Fig. 13 represents the distribution of data for performing IOTA operations remotely such that the median value for attaching payload is around 20 sec while the median value for fetching data is around 2 sec. Secondly, we compute the energy consumption by CPU. Out of 4 cores of Raspberry Pi 3B, a single core (power consumption= 221.0 mW per core) is utilized for attaching and fetching data. The measured average time and energy consumption (evaluated 100 times for security level 3) are given in Table 4. It is important to mention that we only consider Raspberry Pi 3B as a *light node* with the Minimum Weight Magnitude (MWM) parameter set to 14, where MWM is the PoW

complexity currently used in the IOTA mainnnet. Thirdly, we compute the CPU and memory consumption during attaching and fetching phases. Irrespective of payload size, the fetching process consumes more CPU and memory (as shown in Fig. 14). Since during fetching operation, tasks are carried out by Raspberry Pi 3B itself rather than the remote node, hence, it consumes more CPU and memory.

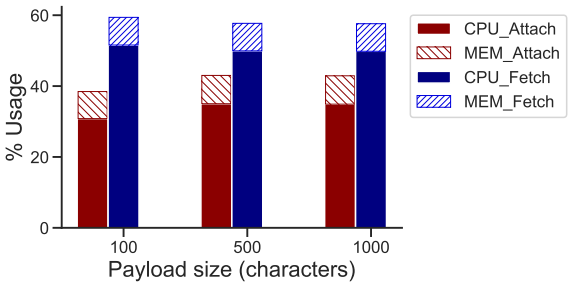


Figure 14: Comparison: CPU and memory usage during attaching and fetching data to the tangle.

5.3. Informal Security Analysis

In this subsection, we revisit the security claims mentioned in Section 3.5 and justify them to evaluate the performance of our proposed provenance-based scheme for ESC.

Claim 1: Data confidentiality.

Justification: The data is stored on the channel in encrypted form. Hence, only those D_r having access to the $Channel_{ID}$ and authorization key ($\mathcal{K}$) can obtain and decrypt the payload.

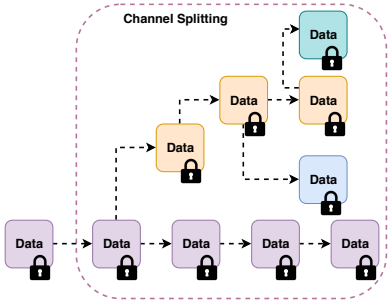


Figure 15: Channel splitting: sharing only a subset of data.

Claim 2: Access control rights.

Justification: MAM channel enables the off-shooting channel (as shown in Fig. 15) particularly when the entirety of data is not intended to be shared. Such fine-grained access to data is desired in many scenarios in ESC. For example, the retailer may share the sales data or customer buying pattern data with the marketing companies while preserving the customer Personally Identifiable Information (PII). Similarly, the idea of channel splitting can also be used to limit access to a company's trade secrets from joint ventures, suppliers, distributors, or customers. Another significant use-case example scenario is when a company is buying some of its product's components from its competitor company. Defining access rights (i.e., grant and revoke) on data is based on an authorization key ($\mathcal{K}$) used in the restricted mode. The key is exchanged with the legitimate SC players only and can be changed to revoke access rights without any need to change the $Channel_{ID}$. The other modes provided by MAM channel includes *public* and *private*. Further details related to the MAM channel are provided in Section 4.1.

To illustrate the process of fine-grained access through channel splitting, let us consider a scenario. Suppose, a seller S_1 (SID: SK_GIH003) is selling components (for instance, DRAM chips) to a buyer B_3. S_1, also outsources its components to one of its partner sub-seller S_{sub} (SID: CN_SHE005) who further sells components to other buyers B_1 and B_2. S_1 and S_{sub} define access control rights for their buyers so that they are able to retrieve the required information from them. The information, in particular, can be generalized as T_{Data}, A_{Data}, $Sales_{info}$ (showing sales pattern), $Client_{info}$ (list of clients), $Manufacturing_{info}$ (manufacturing process), $Advertising_{info}$ (advertising strategies). The defined policies and a few example queries are discussed in Table 5. The query results can be retrieved on the basis of provenance key elements.

Channel ID	**Policies**	**Queries**	**Result**
SID: SK_GIH003	Allow B_3 to access: T_{Data}, A_{Data}	Fetch: $Sales_{info}$ from S_1	Access Denied
	Allow S_{sub} to access: T_{Data}, A_{Data}, $Sales_{info}$, $Client_{info}$, $Advertising_{info}$	Fetch: $Manufacturing_{info}$from S_1	Access Denied
		Fetch: $Sales_{info}$ from S_1	Access Granted
SID: CN_SHE005	Allow B_1 to access: T_{Data}, A_{Data}, $Client_{info}$	Fetch: $Client_{info}$ from S_{sub}	Access Granted
	Allow B_2 to access: T_{Data}, A_{Data}, $Sales_{info}$	Fetch: $Client_{info}$ from S_{sub}	Access Denied

Table 5: Channel splitting example scenario: fine-grained access rights.

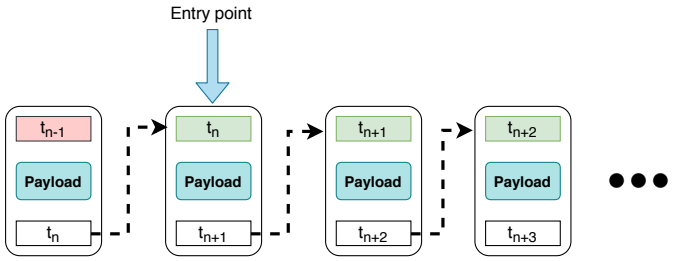


Figure 16: Message chain showing *transaction linking* among transactions and *forward secrecy* enforced at and after the point of entry.

Claim 3: Restrictions on data retrieval.

Justification: To enforce a restriction on previous data in the message chain, we exploit forward secrecy, i.e., the subscriber can only locate and retrieve transactions at or after their point of entry in the channel, but not before their point of entry (as shown in Fig. 16). Upon locating the transaction t_n, the subscriber can retrieve the address of the next transaction t_{n+1} (as shown in Fig. 16). When the masked message of one

generation is decrypted, unmasked message contains *nextRoot* that is used by viewers to find the message of the next generation of the channel.

Claim 4: Preserving data integrity during trade events.

Justification: Sensor tampering or data modification may occur during data creation or data transit phase thereby causing the GIGO problem. For example, in our SC case, the sensor can be tampered to change the readings leading to false data creation or the sensor data can be maliciously altered during communication. To address the former problem, we can rely on any of the existing solutions such as the use of Physical Unclonable Functions (PUF) provided in [63]. For the latter problem, we employed the MAM channel restricted mode for secure communication. Furthermore, it is assumed that IoT sensors are calibrated periodically. Another concern is how to ensure that a rogue participating entity is not corrupting the data. Some of the following solutions in the literature can be leveraged to solve this issue. A rating system for buyers and sellers based on previous trade events can be used. For instance, in [64], the authors used a reputation-based trading system which allows high reputations sellers to access better offers from the buyers. Another similar solution is proposed in [65] to enable monetary punishment mechanism to discourage any malicious changes in data or revoking trader's participation in the SC based on trust evaluation. Though all of the above solutions are proposed in combination with the blockchain ledger; however, they can be incorporated into the IOTA through oracles on the top (i.e., the concept of smart contracts in IOTA is underway [66]).

To eliminate the GIGO problem (handling of design factor F-II) in our proposed scheme, we adopted a combination of the below-mentioned solutions to mitigate the effect of data adulteration. Firstly, we include product traceability through provenance data at each intermediate step in SC processes (handling of design factor F-I). Secondly, the inclusion of the warranty parameter can also help in establishing trust among entities in the long run. Thirdly, the verification of the transactions by both buyer and supplier can also confirm any fraudulent activity, for instance, *Receipt* transaction in our proposed solution. Finally, the attacker can not repudiate once found guilty (claim 5). It is also worth noting that the adversary in a permissioned ledger requires consideration of many other possible security scenarios (for instance, attacks by an internal or external adversary, colluding users, etc.) and is out of the scope of this paper.

Claim 5: Non-repudiation.

Justification: To handle repudiation of trade events by any of the participating entities, transactions on the IOTA ledger ensure the immutability of data, the existence of SC events, and associated data carried out by the particular entity.

5.4. Outstanding Issues and Challenges in IOTA Ledger

Analogous to the blockchain, IOTA also faces security and stability issues. Currently, IOTA is relying on a coordinator (COO) for consensus that is responsible for the continuous generation of trust-able transactions to help to secure the infant tangle network from a double-spending attack. There are two main problems that arise due to the presence of COO: (i) single point of attack that can paralyze the whole tangle if COO stops working or taken over, and (ii) curtailing scalability of IOTA. However, to optimize the designed system, *Coo-less IRI* (CLIRI) [67] is recently introduced which is considered to be an important step towards the maturity of IOTA protocol. *znet* is also launched as the first iteration of the coordinator-less testnet [68]. Hence, research is still ongoing in key areas that would allow the desired decentralization. Keeping in mind the compatibility requirements, we assume that the proposed scheme will be compatible with any up-gradation in the IOTA or the application layer MAM protocol.

Similar to the *forking* problem in blockchain, tangle also suffers from *parasite chains* in which an attacker makes a side tangle to double-spend the money. This problem can also be referred to as *double-spending* attack discussed in [9]. According to IOTA paper, parasite chain attack can be prevented when nodes use the MCMC tip selection strategy under the assumption that the main tangle has more hashing power than the attacker. However, as opposed to the assumption, attack analysis is still under discussion by the community [69]. In the literature, [70] suggested a solution against parasite attack by proposing the matrix model for the MCMC tip selection algorithm.

For highly energy-constrained IoT devices (such as battery-powered) performing computationally expensive tasks is not practically possible without hardware-accelerated cryptography. Nevertheless, powerful devices such as Raspberry Pi are still capable of doing IOTA operations as light nodes [71]. Another important issue is the staggering amount of transactions received by IOTA nodes which of course results in ever-increasing memory and CPU requirements. To combat this situation, a snapshot is performed to either reduce the size of the tangle or to reduce the burden on memory-constrained nodes. A snapshot essentially throws away all the transaction history and resets the IOTA ledger to a list of all the addresses that have a nonzero balance. Therefore, such a global snapshot prunes the database to create room for newer transactions. It is hard for node owners with limited storage (IoT devices), to store full transaction history. To handle such situations, a local snapshot feature can be used that allows node owners to delete old transactions and keep their tangle database small. This option facilitates faster synchronization, lower resource requirements, and eliminates the need to wait for global snapshots [72]. For many scenarios, data needs to be stored for an extensive period of time. To deal with such use cases, the IOTA Foundation provides a permanode solution called Chronicles [73]. This solution enables node owners to have unbounded storage of the tangle's entire history and makes it accessible at scale. In the context of SC, both permanode solution and local snapshot can be used depending on the situation and requirements. For instance, in the case of resource-constrained devices, local snapshot can be adopted, however, in the case of the SC process, permanode solution can be adopted. Such features can be incorporated into our proposed work upon finalizing these features by IOTA Foundation.

In this proposed framework, we adopt a 2-tier approach to orchestrate provenance in the ESC. In the first tier, we collect SC data flowing across each SC participant, store securely in a distributed IOTA ledger, and manage data access rights. In the second tier, we construct provenance data to trace and track the product journey at each intermediate step in the SC cycle. Such a 2-tier approach provides an optimal strategy to carry out SC processes. For example, the first tier resolves the problems of fragmented data repositories and enables the SC participants to hide their trade secrets by defining data access rights while the second tier resolves the problems of counterfeit products and helps in achieving customer's trust.

6. Conclusion and Future Research Directions

In this paper, we have targeted two key challenges in the ESC, i.e., disparate data repositories and untrustworthy data dissemination. To address these issues, we have proposed an IOTA-based provenance framework that encapsulates the diverse product story as provenance data at each intermediary process in the ESC. Our provenance-enabled framework helps in reducing counterfeiting issues in addition to the problem of fragmented and asymmetric information. Furthermore, to ensure the construction of secure provenance information, we have leveraged the MAM channel that provides confidential trade flow among competitors, preserve data integrity, and provide fine-grained data access to the trusted SC players. We have also validated

the efficacy of our proposed scheme in terms of energy consumption and the time required to attach and fetch data from the ledger on the Raspberry Pi 3B hardware platform. It is worth mentioning that the DLT-based solutions have unique features such as no-fee, scalability, and quantum resilience that make them favorite candidates for ESC. We also note that currently ESC is struggling with the integration of blockchain with SC; however, after addressing the outstanding problems, it is anticipated that DLT-based ESC will prove to be a viable futuristic solution. Our proposed IOTA-based solution is one such effort in this direction.

For future work, we plan to survey other existing DLTs and compare them with IOTA in terms of performance (scalability, latency, and throughput) and device resource usage (CPU, memory, and energy consumption). Depending on the infrastructure, different types of sensors are deployed in different SC application areas. Therefore, we also plan to extend the proposed provenance-enabled SC system to other ARM-based devices to evaluate their compatibility across different platforms. As discussed in Subsection 5.3 (Claim 4), evaluating traders in the SC based on the mechanism of trust scores to facilitate honest buyers and sellers is also part of future work. From the perspective of SC management, introducing trade finance process to replace traditional finance procedures and risk management (for example, environmental risks) are other potential extensions of our proposed scheme. Regarding the applicability of the proposed approach, SC data can be monetized to allow other business communities to learn and analyze the current industry trends and traits. This involves the integration of the current hyped technologies such as Artificial Intelligence (AI) and Machine Learning (ML). For this purpose, querying data can be customized based on access privileges or anonymization techniques. Such information can also help to study forecasting future events to avoid inaccuracies and ultimately take possible measures against the bullwhip effect. Lastly, addressing challenges such as real-time performance, coexistence, and interoperability, associated with IIoT in the SC system are among other interesting areas that are required to be explored.

References

[1] M. Montecchi, K. Plangger, M. Etter, It's real, trust me! establishing supply chain provenance using blockchain, Business Horizons 62 (3) (2019) 283–293. doi:10.1016/j.bushor.2019.01.008.

[2] J. Cheney, S. Chong, N. Foster, M. Seltzer, S. Vansummeren, Provenance: a future history, in: Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, ACM, 2009, pp. 957–964.

[3] S. Suhail, R. Hussain, M. Abdellatif, S. R. Pandey, A. Khan, C. S. Hong, Provenance-enabled packet path tracing in the RPL-based internet of things, Computer Networks 173 (2020) 107189. doi:10.1016/j.comnet.2020.107189.

[4] J. Stradley, D. Karraker, The electronic part supply chain and risks of counterfeit parts in defense applications, IEEE Transactions on Components and Packaging Technologies 29 (3) (2006) 703–705. doi:10.1109/tcapt.2006.882451.

[5] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, Y. Makris, Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain, Proceedings of the IEEE 102 (8) (2014) 1207–1228. doi:10.1109/jproc.2014.2332291.

[6] Orange county electronics distributor charged with selling counterfeit integrated circuits with military and commercial uses, Available at: https://www.justice.gov/usao-cdca/pr/orange-county-

electronics-distributor-charged-selling-counterfeit-integrated-circuits (Accessed on December 29, 2019).

[7] G. Svensson, Key areas, causes and contingency planning of corporate vulnerability in supply chains, International Journal of Physical Distribution & Logistics Management 34 (9) (2004) 728–748. doi:10.1108/09600030410567496.

[8] V. Babich, G. Hilary, OM forum - distributed ledgers and operations: What operations management researchers should know about blockchain technology, Manufacturing & Service Operations Management 22 (2) (2020) 223–240. doi:10.1287/msom.2018.0752.

[9] S. Popov, The tangle. White paper., Available at: https://iota.org/IOTA_Whitepaper.pdf, 2016.

[10] F. Tian, A supply chain traceability system for food safety based on HACCP, blockchain & internet of things, in: 2017 International Conference on Service Systems and Service Management, IEEE, 2017. doi:10.1109/icsssm.2017.7996119.

[11] S. Malik, S. S. Kanhere, R. Jurdak, Productchain: Scalable blockchain framework to support provenance in supply chains, in: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), IEEE, 2018, pp. 1–10.

[12] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, H. Y. Lam, Blockchain-driven IoT for food traceability with an integrated consensus mechanism, IEEE Access 7 (2019) 129000–129017. doi:10.1109/access.2019.2940227.

[13] M. P. Caro, M. S. Ali, M. Vecchio, R. Giaffreda, Blockchain-based traceability in agri-food supply chain management: A practical implementation, in: 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), IEEE, 2018, pp. 1–4.

[14] R. Raj, N. Rai, S. Agarwal, Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 1572–1577.

[15] P. Sylim, F. Liu, A. Marcelo, P. Fontelo, Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention, JMIR Research Protocols 7 (9) (2018) e10163. doi:10.2196/10163.

[16] T. Bocek, B. B. Rodrigues, T. Strasser, B. Stiller, Blockchains everywhere - a use-case of blockchains in the pharma supply-chain, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), IEEE, 2017. doi:10.23919/inm.2017.7987376.

[17] P. Cui, J. Dixon, U. Guin, D. Dimase, A blockchain-based framework for supply chain provenance, IEEE Access 7 (2019) 157113–157125.

[18] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, M. Tehranipoor, Electronics supply chain integrity enabled by blockchain, ACM Trans. Design Autom. Electr. Syst. 24 (3) (2019) 31:1–31:25. doi:10.1145/3315571.

[19] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, J. H. Khor, Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains, IEEE Access 7 (2019) 7273–7285. doi:10.1109/access.2018.2890389.

[20] M. Westerkamp, F. Victor, A. Kupper, Tracing manufacturing processes using blockchain-based token compositions, Digital Communications and Networks.

[21] H. Wu, Z. Li, B. King, Z. B. Miled, J. Wassick, J. Tazelaar, A distributed ledger for supply chain physical distribution visibility, Information 8 (4) (2017) 137. doi:10.3390/info8040137.

[22] C. Mandolla, A. M. Petruzzelli, G. Percoco, A. Urbinati, Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry, Computers in industry 109 (2019) 134–152.

[23] M. Ghobakhloo, The future of manufacturing industry: a strategic roadmap toward industry 4.0, Journal of Manufacturing Technology Management 29 (6) (2018) 910–936. doi:10.1108/jmtm-02-2018-0057.

[24] Z. Li, A. V. Barenji, G. Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, Robotics and computer-integrated manufacturing 54 (2018) 133–144.

[25] A. Vatankhah Barenji, Z. Li, W. Wang, G. Q. Huang, D. A. Guerra-Zubiaga, Blockchain-based ubiquitous manufacturing: a secure and reliable cyber-physical system, International Journal of Production Research (2019) 1–22.

[26] A. Kamilaris, A. Fonts, F. X. Prenafeta-Bold$\acute{v}$, The rise of blockchain technology in agriculture and food supply chains, Trends in Food Science & Technology 91 (2019) 640–652. doi:10.1016/j.tifs.2019.07.034.

[27] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: A comprehensive review and directions for future research, Applied Sciences 9 (9) (2019) 1736. doi:10.3390/app9091736.

[28] K. A. Clauson, E. A. Breeden, C. Davidson, T. K. Mackey, Leveraging blockchain technology to enhance supply chain management in healthcare:, Blockchain in Healthcare Todaydoi:10.30953/bhty.v1.20.

[29] J.-H. Lee, M. Pilkington, How the blockchain revolution will reshape the consumer electronics industry [future directions], IEEE Consumer Electronics Magazine 6 (3) (2017) 19–23.

[30] N. Kshetri, 1 blockchain's roles in meeting key supply chain management objectives, International Journal of Information Management 39 (2018) 80–89. doi:10.1016/j.ijinfomgt.2017.12.005.

[31] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. challenges and opportunities, Future Generation Computer Systems 88 (2018) 173–190. doi:10.1016/j.future.2018.05.046.

[32] A. Hughes, A. Park, J. Kietzmann, C. Archer-Brown, Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms, Business Horizons 62 (3) (2019) 273–281. doi:10.1016/j.bushor.2019.01.002.

[33] V. J. Morkunas, J. Paschen, E. Boon, How blockchain technologies impact your business model, Business Horizons 62 (3) (2019) 295–306. doi:10.1016/j.bushor.2019.01.009.

[34] IBM blockchain, Available at: https://www.ibm.com/blockchain (Accessed on July 8, 2018).

[35] A. Barbaschow, IBM blockchain to help prevent contamination in the global food supply chain, Available at: https://www.zdnet.com/article/ibm-blockchain-to-help-prevent-contamination-in-global-food-supply-chain/ (Accessed on February 26, 2018).

[36] T. Blummer, M. Sean, C. Cachin, An introduction to hyperledger, Tech. rep., Tech. rep. 2018. url: https://www. hyperledger. org/wp-content/uploads/2018 (2018).

[37] skuchain, Available at: http://www.skuchain.com/ (Accessed on July 10, 2018).

[38] Provenance: every product has a story, Available at: https://www.provenance.org/ (Accessed on July 9, 2018).

[39] Blockverify, Available at: http://www.blockverify.io/ (Accessed on July 9, 2018).

[40] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management, International Journal of Production Research 57 (7) (2018) 2117–2135. doi:10.1080/00207543.2018.1533261.

[41] N. Hackius, M. Petersen, Blockchain in logistics and supply chain: trick or treat?, in: Proceedings of the Hamburg International Conference of Logistics (HICL), epubli, 2017, pp. 3–18.

[42] Y. Wang, M. Singgih, J. Wang, M. Rit, Making sense of blockchain technology: How will it transform supply chains?, International Journal of Production Economics 211 (2019) 221–236. doi:10.1016/j.ijpe.2019.02.002.

[43] K. Francisco, D. Swanson, The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency, Logistics 2 (1) (2018) 2. doi:10.3390/logistics2010002.

[44] P. Waterland, Quantum resistant ledger (qrl)., Available at: https://theqrl.org/ (Accessed on December 29, 2019).

[45] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, A. K. Fedorov, Quantum-secured blockchain, Quantum Science and Technology 3 (3) (2018) 035004. doi:10.1088/2058-9565/aabc6b.

[46] V. Babich, G. Hilary, Blockchain and other distributed ledger technologies in operations, Foundations and Trends in Technology, Information and Operations Management 12 (2-3) (2019) 152–172. doi:10.1561/0200000084.

[47] F. M. Bencic, I. P. Zarko, Distributed ledger technology: Blockchain compared to directed acyclic graph, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2018. doi:10.1109/icdcs.2018.00171.

[48] H. Pervez, M. Muneeb, M. U. Irfan, I. U. Haq, A comparative analysis of DAG-based blockchain architectures, in: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), IEEE, 2018. doi:10.1109/icosst.2018.8632193.

[49] K. Wüst, A. Gervais, Do you need a blockchain?, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018. doi:10.1109/cvcbt.2018.00011.

[50] M. Higginson, M.-C. Nadeau, K. Rajgopal., Blockchain's occam problem, Available at: https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem# (Accessed on December 29, 2019).

[51] K. W. Prewett, G. L. Prescott, K. Phillips, Blockchain adoption is inevitable—barriers and risks remain, Journal of Corporate Accounting & Finance 31 (2) (2020) 21–28. doi:10.1002/jcaf.22415.

[52] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, B. M. Boshkoska, Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions, Computers in Industry 109 (2019) 83–99.

[53] M. Lezoche, J. E. Hernandez, M. d. M. E. A. Díaz, H. Panetto, J. Kacprzyk, Agri-food 4.0: a survey of the supply chains and technologies for the future agriculture, Computers in Industry 117 (2020) 103187.

[54] H. S. Sternberg, E. Hofmann, D. Roeck, The struggle is real: Insights from a supply chain blockchain case, Journal of Business Logistics.doi:10.1111/jbl.12240.

[55] D. Roeck, H. Sternberg, E. Hofmann, Distributed ledger technology in supply chains: a transaction cost perspective, International Journal of Production Research 58 (7) (2019) 2124–2141. doi:10.1080/00207543.2019.1657247.

[56] R. Azzi, R. K. Chamoun, M. Sokhn, The power of a blockchain-based supply chain, Computers & Industrial Engineering 135 (2019) 582–592. doi:10.1016/j.cie.2019.06.042.

[57] N. E. Ioini, C. Pahl, A review of distributed ledger technologies, in: H. Panetto, C. Debruyne, H. A. Proper, C. A. Ardagna, D. Roman, R. Meersman (Eds.), On the Move to Meaningful Internet Systems. OTM 2018 Conferences - Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II, Vol. 11230 of Lecture Notes in Computer Science, Springer, 2018, pp. 277–288. doi:10.1007/978-3-030-02671-4_16.

[58] W. Gilks, S. Richardson, D. Spiegelhalter (Eds.), Markov Chain Monte Carlo in Practice, Chapman and Hall/CRC, 1995. doi:10.1201/b14835.

[59] X. Chen, L. Li, M. Zhou, Manufacturer's pricing strategy for supply chain with warranty period-dependent demand, Omega 40 (6) (2012) 807–816. doi:10.1016/j.omega.2011.12.010.

[60] R. C. Merkle, A digital signature based on a conventional encryption function, in: C. Pomerance (Ed.), Advances in Cryptology — CRYPTO '87, Springer Berlin Heidelberg, 1988, pp. 369–378.

[61] ABmushi, IOTA: MAM eloquently explained, Available at: https://medium.com/coinmonks/iota-mam-eloquently-explained-d7505863b413 (Accessed on February 26, 2018).

[62] Raspberry pi (trading) ltd. 2016. compute module datasheet, Available at: https://www.raspberrypi.org/documentation/hardware/computemodule/datasheet.md (Accessed on June 9, 2018).

[63] U. Javaid, M. N. Aman, B. Sikdar, BlockPro, in: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems - BlockSys'18, ACM Press, 2018. doi:10.1145/3282278.3282281.

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

[65] A. Ramachandran, M. Kantarcioglu, Using blockchain and smart contracts for secure data provenance management, arXiv:1709.10000. [Online]. Available at: https://arxiv.org/abs/1709.10000 (2017).

[66] Smart contracts and IOTA, Available at: https://medium.com/coinmonks/smart-contracts-and-iota-f8a59c355084 (Accessed on December 30, 2019).

[67] I. F. Coordicide Team, The coordicide, Available at: https://coordicide.iota.org/ (Accessed on May 20, 2019).

[68] A testnet with no coordinator, Available at: https://blog.iota.org/a-coo-less-testnet-879ad17ca1af (Accessed on June 18, 2019).

[69] B. Kuśmierz, Attack analysis - the simple parasite chain, Available at: https://blog.iota.org/attack-analysis-the-simple-parasite-chain-42a34bfeaf23 (Accessed on December 25, 2019).

[70] A. Cullen, P. Ferraro, C. King, R. Shorten, Distributed ledger technology for IoT: Parasite chain attacks, arXiv: 1904.00996. [Online]. Available at: https://arxiv.org/abs/1904.00996 (2019).

[71] A. Elsts, E. Mitskas, G. Oikonomou, Distributed ledger technology and the internet of things: A feasibility study, in: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, ACM, 2018, pp. 7–12.

[72] IRI 1.6.0 with local snapshots out now!, Available at: https://blog.iota.org/iri-1-6-0-with-local-snapshots-out-now-fc4d991faba8 (Accessed on September 23, 2019).

[73] Introducing chronicle — a permanode solution, Available at: https://blog.iota.org/introducing-chronicle-a-permanode-solution-8e506a2e0813 (Accessed on September 23, 2019).