Abstract

Blockchain technology has huge potential to decentralize trust in supply chains and bring measurable benefits and value to the public and private sectors. To unlock this potential, the Tspace protocol was designed purposefully to tackle the main challenges which limit the fluent exchange of, and integrity of data in product supply chains. With supply chain data becoming increasingly fragmented, scalability and cost concerns of current decentralized solutions become evident.

Tspace is a unique solution allowing IT providers in supply chains to set up block chain supported data sharing in multi-organizational environment. It helps them build transparency beyond the “one step down, one step up” traceability principle. Furthermore, it improves the integrity of product data and drives efficiencies for stakeholders.

The first version of the Tspace solution is proven and currently deployed in the food industry. The upcoming open source version will be suitable to any product supply chain such as automotive, consumer goods, pharmaceutical etc.

Visit our official website: www.tspace.network

Table of contents

1. Document purpose

This document was created with the goal of positioning Tspace's protocol concept. The protocol was developed based on five years of experience building solutions to enable information transparency in supply chains. It includes our vast practical experience gained during our work on live business cases with new technological possibilities created 1 by the blockchain community.

Despite quick advancement in development of blockchain, we see a gap between the advantages blockchain can bring and the actual implementations in supply chains in a seamless and efficient manner. The positive momentum created by the blockchain community functions as a catalyst to implement the technology for one of the biggest challenges faced by the global economy - opaque, inefficient and untrusted supply chains. Employing the capacity of fast growing blockchain networks, Tspace will bring decentralization, interoperability, data and information integrity and trust to supply chains. This is an open source project and by definition relies on (industry and technical) community feedback to grow stronger.

Tspace protocol, with certain parts currently centralised, is in pilot programs in Europe and China. The results of these pilot programs will be shared in forthcoming documents.

2. Vision

If you take a quick look around your office or home, there is a very high probability that most of the objects surrounding you came through some form of regional, national or global supply chain. The fact that you have very little information with regards to how those products made their way to you is just one of the signs that supply chains are facing more pressure to be transparent... And most of those issues boil down to a very limited ability to share data along the entire supply chain.

Tspace changes that with a decentralised protocol that is tailor made for sharing supply chain data based on blockchain. This brings a profoundly new way of building transparency in supply chains. Tspace uses Blockchain and builds on well established industry standards from GS1 and provides a necessary foundation to build new value - increased trust, optimised supply chain efficiencies, automated compliance and enforce quality assurance processes.

Using Tspace, all stakeholders can securely share their data and keep sensitive data fully encrypted at all times. By supporting global standards for data exchange (GS1, IoT, compliance standards), Tspace assures compatibility with existing ERP systems, making implementation process quick and efficient. Finally, it is fully decentralised. It removes the possibility of collusions and introduces full accountability for the data provided.

Tspace is not a company, it is an ecosystem. It’s based on token economy with direct relations between users and network nodes free of arbitrary fees. Contribution to Tspace ecosystem is a pledge towards more transparent, collaborative, fair and trusted supply chains.

3. Supply chain challenges

With the globalization of trade there is increasing complexity in supply chains. This, in turn, increases the amount of information asymmetry - such that information is unevenly distributed among participating stakeholders within a supply chain.

When participating stakeholders have misaligned incentives, such as the case in which participating stakeholders are different companies, there is no incentive to provide complete information which contributes further to information asymmetry. As a result, end-buyers of products have no economical way of authenticating what they are purchasing, which creates ideal conditions for moral hazard and fraudulent behavior.

Manifestations of such phenomena are the flood of counterfeit goods in the market (e.g., US$200 billion in cost to legitimate businesses in the United States), safety issues, 2 violations of labour standards, just to name few. Stakeholders at greatest risk are end-buyers, consumers, the environment, workers and companies involved in sustainable production and honest practices. Having served our supply chain clients in resolving the challenges above for the past five years, we have identified two key factors impeding data collection and sharing in supply chains: 1. Data is fragmented.

Data siloes and low data interoperability exist across the supply chain in both multi-organisation and single-organisation supply chains. There is a crucial technical challenge for various IT providers for supply chains (software and IOT) that need to be resolved in order to collaborate and establish full supply chain transparency; 2. There is no suitable decentralized solution for supply chain data. There are no solutions that can provide the needed level of performance; scalability and trust for interconnected data in supply chains while at the same time are cost-effective. Current blockchain and decentralized solutions are prohibitively costly, do not provide advanced data relational functionalities, and also have scaling issues.

Nevertheless, all stakeholders have the same goal - being member of the chain and improvement of the whole process regarding volume and efficiency.

3.1 Fragmentation of data in siloes and opacity of supply chains

The current state of supply chain data management solutions involves a number of localized information systems, ERP systems and custom solutions.

In order for them to communicate, custom integrations need to be implemented. Often referred to as "data silos", these centralized systems lack a common technical environment, security, and exchange protocols to facilitate data sharing. Because of this low interoperability of data and other technical hurdles (e.g., different security policies, separate infrastructures and environments), useful real time knowledge on supply chain product context has not been available to interested stakeholders (e.g., consumers, certification and governmental bodies, and operating companies in the supply chain).

With each stakeholder in the supply chain receiving and sending data about product attributes “one step back, one step forward” , trust is easily broken and value chains 3 integrity compromised. Many organizations today aim to bring more order and integrity to complex supply chains, including global standard providers in supply chains (e.g., GS1), certification organizations (e.g. Global GAP, ISEAL, Rainforest Alliance, Bureau Veritas) and information systems providers (e.g. IBM). Yet, none of these organizations can ensure entire chain integrity by creating a stand-alone solution due to centralized logic of data collection and sharing.

Typically, only parts of global supply chains get audited and involved which leads to partial data collection, poor verifiability of collected data, and eventually diminished trust

4. Tspace - First purpose built protocol for supply chains based on blockchain

Tspace is a protocol solution allowing IT providers to easily set up blockchain supported data sharing in supply chains. It enables building transparency and tracking beyond the “one step down, one step up” principle, protecting brands from fraudulent behaviour and driving efficiencies for all stakeholders.

Tspace brings the following :

1. Seamless and automatic data connection and interoperability between IT systems of different stakeholders in multi-organisation supply chains, with consensus mechanisms for ensuring integrity of data;

2. A public decentralized solution for performance, cost and scalability issues by providing a tailored decentralized system for supply chain data based on blockchain.

Direct users of the Tspace are therefore developers creating various supply chain applications using the described protocol. Users can be third party technology providers (supply chain software companies, ERP providers, IoT providers, software development companies) or in-house supply chain technology teams. Applications where Tspace’s protocol delivers value are:

- Product authentication,
- Product journey visibility,
- Product recall efficiency,
- Product freshness for perishables,
- Chain of custody with accountability,
- CSR activities support,
- Supply chain mapping and optimization,
- Inventory management,

- Alert systems (exception management),
- supply chain compliance assurance,
- Customs, audit and regulations process optimization,
- And any other supply chain application that requires transparent supply chain as a starting point.

4.1 Automatic data connection and interoperability beyond the “one step back, one step forward” principle

Tspace protocol enables exchange of different data sets between multi-organisation supply chains no matter its complexity while ensuring the data quality and integrity. Input and sharing data with Tspace is based on a common set of data standards which allow multiple organizations (companies involved in production, distribution or retail of goods) to exchange data beyond the “one step back, one step forward” principle

4.1.1. Data interoperability format

In order to provide for a uniform data flow, all information must be standardized within the ecosystem. While the XML is a widely adopted file format for data exchange, content within the file must be also standardized. Supply chain can span across the globe, where each member has its own local standards. For example, date and time formats are very different even in neighbouring countries. Date 01/10 can be the first of October in one system, and the 10th of January in another. This defines the challenge that data sent to Tspace must be standardized, and vice versa. This requires standardization not only the attributes and nodes within attributes of XML file, but the content also.

Tspace adopts widely used GS1 standards. GS1 standards support the information needs of end users interacting with each other in supply chains, specifically the information required to support the business processes through which supply chain participants interact.

Tspace supports data such as, but not limited to:

● Master Data: data shared by one trading partner to many trading partners, that provides descriptive attributes of real-world entities identified by GS1 Identification Keys, including trade items, parties and physical locations.

● Transaction Data: trade transactions triggering or confirming the execution of a function within a business process as defined by an explicit business agreement (e.g., a supply contract) or an implicit one (e.g., customs processing), from the

start of the business process (e.g., ordering the product) to the end of it (e.g., final settlement), also making use of GS1 Identification Keys.

● Visibility Data: details about physical or digital activity in the supply chain of products and other assets, identified by keys, detailing where these objects are in time, and why; not just within one organisation's four walls, but across organisations.

Tspace is focused on the EPCIS framework [1] because it suits the protocol in its core foundations. The framework is designed to be:

● Layered: In particular, the structure and meaning of data in an abstract sense is specified separately from the concrete details of data access services and bindings to particular interface protocols. This allows for variation in the concrete details over time and across enterprises while preserving a common meaning of the data itself. It also permits EPCIS data specifications to be reused in approaches other than the service-oriented approach of the present specification. For example, data definitions could be reused in an EDI framework.

● Extensible: The core specifications provide a core set of data types and operations, but also provide several means whereby the core set may be extended for purposes specific to a given industry or application area. Extensions not only provide for proprietary requirements to be addressed in a way that leverages as much of the standard framework as possible, but also provides a natural path for the standards to evolve and grow over time.

● Modular: The layering and extensibility mechanisms allow different parts of the complete EPCIS framework to be specified by different documents, while promoting coherence across the entire framework. This allows the process of standardization (as well as of implementation) to scale.

Other data sets will include Iot and compliance data. This allows for exchanging and tamper-proof recording of product properties, which leads to accountability and data integrity in product supply chains.

4.1.2. Data consensus check as a tool for trustworthiness

When receiving information from stakeholders, Tspace protocol performs a "consensus check" that verifies there are no discrepancies between data provided by different stakeholders. The check is performed in several steps:

Step 1. Each stakeholder has to be approved by the previous and the following supply chain stakeholder, creating a chain of accountability.

Step 2. Matching of dynamic batch information is verified, including the critical information of batch identifiers, appropriate timestamps and transactional data. As this step involves company private data (e.g. quantities of sales), a Zero Knowledge Proof 6 mechanism implementation will provide a way to check that private information matching is provable without revealing the information itself. Other dynamic data may include data collected from sensors and compliance data.

Step 3. As an additional layer of credibility, auditing and compliance organisations can validate data by supplying their confirmations.

4.2 Tspace Decentralized Network

In order to provide the optimal solution we implement the Tspace protocol that runs on an off-chain decentralized peer to peer network, called the Tspace Decentralised Network (ODN). It enables peers on the network to negotiate services, transfer, and process and retrieve data, verify its integrity and availability and reimburse the provider nodes. This solution minimizes the amount of data stored on the blockchain in order to reduce cost and inefficiency

Tspace incorporates blockchain as the platform to ensure data integrity.

For all the information that gets included in the system, a tamper proof "fingerprint" (a cryptographic hash) is generated and stored on the blockchain at the time of arrival. The cryptographic hash is commonly used to prove the received data has not been modified in any way, and having the hash immutable in blockchain as a reference to the original input completes this mechanism. If there is a need to check if data was tampered with, a simple hash comparison between the stored hash in the blockchain and the newly generated hash from the same data in ODN shows if changes have been made.

Tspace supports many different blockchain implementations. The current version of Tspace utilizes Ethereum blockchain to provide proof of concept and initial implementation, the fully developed solution will provide interfaces to many different blockchains. There are multiple reasons for adopting this principle:

● Competing blockchain solutions will evolve in unexpected ways, which will influence the pricing of blockchain usage,

● more advanced blockchain solutions in the future could be integrated,

● Supply chain stakeholders already using blockchain solutions for various purposes will be able to use the same blockchain for Tspace.

On top of the blockchain layer are two system layers - the network and data layers, which combined form the ODN system. Because of computational and

storage efficiency, the ODN is able to deliver a cost-efficient solution for data integration and manipulation in for supply chain stakeholders.

4.5 Possible system attacks Sybil & Outsourcing

Attacks creating multiple (Sybil) identities would theoretically allow for malicious nodes to pretend storing more copies of the same data, but having them stored only once and quickly fetched from the storing location when required to prove they are providing the service. This issue is addressed by establishing a similar mechanism to the Proof-of-Replication [7] introduced in the Filecoin whitepaper [8] applied to graphs, with the consideration that the data in Tspace is public by design. With these preconditions in place, encryption is used to prove replication and not used to obscure data - it is up to the data creator to encrypt the input information they require to be obscured before inputting data into the system.

The 51% Attack

A 51% attack is usually defined as an ability to control an overwhelmingly large amount (at least 51%) of power in a decentralized system (i.e. hashing power in Ethereum), which then grants the ability to manipulate data. In terms of data integrity in Tspace that is fully safe from 51% Attack.

Possible Eclipse Attacks

Isolating a node or a multitude of them from the network by having all outbound connections reach malicious nodes is called the eclipse attack. This is addressed by using public key hashes as node IDs in Kademlia.

To eclipse a node on the network the attacker has to generate key pairs that position themselves closer in Kademlia to the targeted node than its nearest non-malicious neighbor, as well as maintaining that position when new nodes join with closer IDs. This problem grows in complexity as more nodes are introduced

to the network and essentially presents a form of proof-of-work problem.

Hostage data attacks

A malicious node might refuse to deliver certain graph data in order to extort data owners for additional tokens. This possibility is mitigated by replicating graph data across a multitude of node.

Tspace Token Economics

Therefore, Tspace nodes are incentivised to do two groups of tasks:

● Data processing - Supply chain consensus checks, data quality and replication checks

● Storing, managing and delivering the data in graph form Write (introducing new supply chain information to Tspace) and storing operations are performed by nodes for which they receive the compensation in Trace tokens based on the agreement reached, in regards to the data distribution protocol mechanism described in this document. It is important to note that Tspace uses a blockchain layer which presents an independent system and thus adds additional cost depending on the chosen underlying blockchain for some OriginTrail functionalities.

In case of Ethereum being the underlying blockchain, this means that a small amount of gas (Ether) is also needed to store the necessary hashes on Ethereum for the storage operation. Read operations are also compensated with Trace tokens. An exception where read operations can be free of cost is if certain conditions are met: if one has access to i.e. an Ethereum node for free reads from Ethereum (or another chosen blockchain from the blockchain layer), and if they hold a local Tspace node which contains the necessary graphs.

The amount of tokens to be awarded for the nodes providing the service is a function of supply and demand between nodes and users. Data creators will not be required to pay any additional arbitrary fees apart from what they agree to pay to the nodes. On the other side, nodes will receive full payment of what they have

agreed with and provided to the user. The Trace token is implemented as an ERC20 compatible token on Ethereum. This ensures 8 interoperability with wallets and other tokens on Ethereum. The Trace token smart contract handles all transactions and balances in a secure and trusted manner.