Touching Space: Distributed Ledger Technology for Tracking and Tracing Certificates

Pascal Moriggl
University of Applied Sciences Northwestern Switzerland. FHNW
pascal.moriggl@fhnw.ch

Petra Maria Asprion
University of Applied Sciences Northwestern Switzerland. FHNW
petra.asprion@fhnw.ch

Bettina Schneider
University of Applied Sciences Northwestern Switzerland. FHNW
bettina.schneider@fhnw.ch

Christopher Scherb
University of Applied Sciences Northwestern Switzerland. FHNW
christopher.scherb@fhnw.ch

Abstract

Components built into space vehicles and equipment (space products) must meet different regulatory requirements; in detail, each component must be certified and sustainably traceable at all times. Space engineers have expressed the need for an interoperable system to collect, manage and route certifications for components, parts and materials that go into space products. The lack of a unified approach in the European space industry is a challenge for companies involved in product development. This research proposes an open-source, secure, fast and distributed ledger technology (DLT) based solution that fits into any IT environment and is well adapted to the needs of manufacturing companies in the space sector. The results show that a blockchain-based solution based on 'Hyperledger Fabric' combined with the InterPlanetary File System is viable. The results can guide other researchers and practitioners to consider DLTs when changing their certification management paradigm with suppliers, customers and auditors.

Keywords: Distributed Ledger Technology, Hyperledger Fabric, InterPlanetary File System, Component Certificates, Track and Trace, Space Industry

1. Introduction

Developing products to be used in aerospace is a demanding and time-consuming process followed by a quality management system to ensure that all the requirements for use in space travel are met and can be verified. The reasons for this effort become apparent when the rigorous European space quality management system is seen as part of the broader aerospace industry, based on the aerospace standard AS9100, which relies on ISO 9001 (Țîțu & Ioan, 2019), or equivalent means of military derivation (e.g., ASD-STAN). Compliance with these standards is a challenge, especially for smaller suppliers to the space industry. ISO9001 certification is a must for space industry suppliers, and the industry further requires suppliers to adhere to standards defined in AS9001 and by the European Cooperation for Space Standardization (ECSS). The ECSS is an organization that aims at improving standardization within the European space sector. AS9100 is derived from ISO9001, a company-level certification based on the standard published by the Society of Automotive Engineers (SAE) titled "Quality Systems-Aerospace-Model for Quality Assurance in Design, Development, Production, Installation, and Servicing". This research focuses only on aspects concerned with supplying parts or developing components and their verification obligations. Parts are single items (e.g., screws), whereas components stand for high-tech components (e.g., optical instruments) engineered specifically for the final product (e.g., an aerospace satellite).

In this context, documentation supporting the components is vital to confirm their properties, processes, and operational elements for the other value chain stakeholders, often in the form of certificates. Documentation refers to manuals for guiding the usage and descriptions explaining the components. Besides, documentation that certifies and proves their properties and textures can include project-specific component identification, meta description, and organizational information that should be sticky to the corresponding component. This research focuses on the documentation's traceability, transparency, and completeness, not at least preparing for an automated certificate processing. Traceability is not a space industry demand only. However, it is difficult for large European system integrators that develop space products because they are distributed across countries or split into several profit centers. As a result, their parts and components management processes are

URI: https://hdl.handle.net/10125/103157
978-0-9981331-6-4

already spread and, to a certain degree, fragmented across data silos (Singh et al., 2018).

2. Use Case

A dominant electronic system to track space component certificates in Europe is missing. This research is based on three research questions:

i. How is the space industry organizing its component certificates today?

ii. How could the current approach be modelled in a decentralized manner?

iii. Is it feasible to implement the novel architecture using Hyperledger Fabric?

The contribution is structured as follows. Chapter 2 introduces the underlying use case, starting with a detailed problem description and analysis followed by a market analysis review to retrieve the current state of the art from an industry perspective. Chapter 3 references DLT and its foundational characteristics and discusses recent findings from research publications that apply DLT in a similar context as described in Chapter 2. Chapter 4 describes the prototype and its element as crucial contributions to solving the related problem with a novel approach. Chapter 5 closes with a conclusion and outlook.

2.1. Problem Description

Managing the traceability of parts and component certificates is a time-demanding and resource-consuming duty for involved supply chain participants. Supply chain participants can be raw material suppliers, manufacturers, integrators, OEMs, logistics, and distributors, in the following subsumed under 'Aerospace Product Supply Chain Participants' (APSCP). Traceability in this context means the access and management of parts and component certificates across APSCP borders and compliance with specific industry-specific regulatory requirements. Such requirements are described in AS9100 Rev D. One traceability requirement is the need for 'maintaining configuration', which stands for knowing what parts and processes went into a product or service to be compared to the design configuration (Advisera Expert Solutions, 2017). Another requirement is the 'identification and traceability', defining standards such as serial numbers, batch, or other identification methods to trace the outputs into products. Each processed part or component refers to one but usually several certificates that verify its dimensions, material properties, origin, and other component-specific verifications.

2.2. Problem Analysis

The main problem is the parts/component certification required by the AS9001 quality management system. Based on AS9100, all components supplied to end products in the space industry need various certifications. All APSCP ensure the adherence to the requirements at their level and can be held liable. The component certifications are usually paper-based and part of the component delivery package.

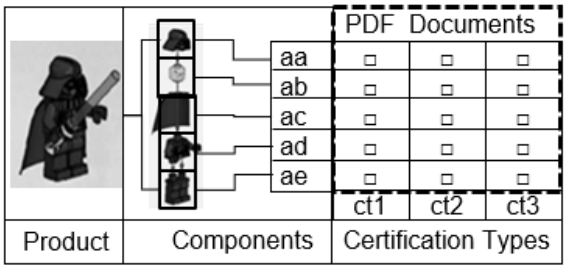

Figure 1 Space components certificate outline illustration

Figure 1 illustrates the preparation work for an integrator when assembling a product. The process requires outlining all certification types needed for each component, often in PDF format. The more parts and components involved in this process, the more time and complexity are demanded by the outlining task. The job absorbs valuable time from the actual value-adding engineering task and represents resource waste for a space engineer.

The certifications must be passed along for each space component supplied from one APSCP to another while maintaining the typical cybersecurity elements confidentiality, integrity, and availability. In the example of an APSCP, a standard system integrator, this supplier must ensure that all components used in the assembly have the required certifications. Figure 2 illustrates a component certification tree with related certifications.

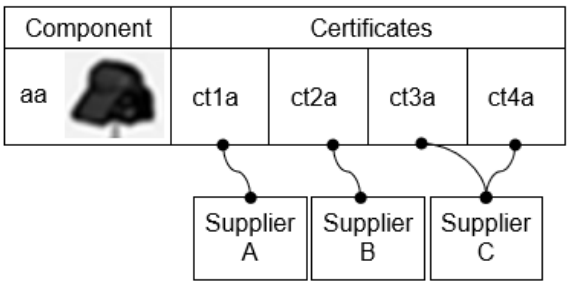

Figure 2 Component certification tree illustration

Suppose the APSCP relies on a database to manage the certifications, and a component has certifications from different suppliers (e.g., subassembly component). Each certificate from an input part or component must be maintained along the supply chain. Sometimes, false certifications are passed along and should be detectable by the processor system.

An APSCP shall be able to reconstruct - in case of need - which component was used on which product and had access to all the related certifications (Figure 2). While some APSCP deliver the certificates as 'pdf files,' most will provide 'printouts' that need to be scanned, catalogued, and revised upon component documentation arrival. Additionally, certifications will later need to be linked to the sub-part used in an assembly. In the case of the system integrator, the associated tasks of collecting, sorting, and checking all this heterogeneously formatted information when using a component consume significant resources and time. The component manufacturer must provide component information (documentation, certificates). The component integrators need to collect and check this information about a component. Example documentation (certification) for a screw is about its foundry lot and its chemical properties reflecting recognized standards, the bare material strength, its power after machining satisfying reference standards, and the surface treatments that the screw needs to receive. This information is collected, maintained, and delivered for screws being part of the space product or sub-product. This documentation requirement applies to any mechanical part (e.g., dimensional checks, materials certificates, coatings certificates, certificates of conformance).

Professional Enterprise Resource Planning (ERP) or Product Lifecycle Management (PLM) systems can help manage the necessary information. Their acceptance and use inside a company require that the systems be classified as part of the (standard) stock management system. Only the most relevant documentation is delivered to the customer in the 'End-Item Data Package' (EIDP). The EIDP is not standardized and includes information about compliance with customer requirements, deviations, and approvals of newly qualified processes. Despite the process of delivering information via the EIDP to an APSCP, there is currently no alternative to manual classification work; this manually runs across APSCPs.

The space industry issues part or component certificates mainly in a portable document format (pdf) and is scanned upon the printed certificate's arrival or sent by mail. Therefore, state-of-the-art focuses on systems that can import/upload pdf documents and transform them into so-called digital objects. Then, the digital objects are the subjects to track and trace certificates that benefit the space industry, automate costly and error-prone manual processes, verify the authenticity, and provide an accredited audit trail. For example, tracking referrals to following the emerging path of the certificate forwards from its starting point to wherever the certificates are and tracing referrals to follow the completed path backwards from its current issue to where the certificate was created.

2.3. Market Analysis

Before a new architecture and software is proposed, a limited market analysis was performed to check for existing software that covers for the problem domain. The goal was to find and review existing certificate tracking software for space companies, the keywords "Tracking', 'Tracing', 'Certificate(s)', 'Documentation', 'Workflow', 'Electronic, Document', 'Certification', 'Space', 'Aerospace', 'ISO9000', 'ISO9001' were used on DuckDuckGo and Google search engine – to complement the results from both. The results in Table 1 show space industry dedicated solutions. We disclosed that the space industry's related products lack a mutually accepted solution in this context, there was no dominant software solution found that tracks space component certificates across company borders.

Table 1 documents tracking solutions for the space industry

Product name and vendor
Document Control by Sunday business systems
Nonconformance Tracking System (NCTS) by European Space Agency
Document configuration and change management by Sapienza Consulting Holding bv
Aerospace Supplier Information System by the as9100 store
Nasa technical report server by NASA
Documentation and Compliance Management by Konica
Aerospace documentation suite by Amplexor
SDL Contenta Publishing Suite by SDL
ERP by SAP

The searches returned several documents tracking solutions for general industries and the ones in Table 1 for the space industry. They have in common that none of these solutions relies on DLT, but all rely on standard database (DB) technology. According to our

analysis, the solutions (Table 1) lack 1.) actual separation of power as in central software provider, and 2.) a specific focus on data security features, including confidentiality, integrity, and availability, which DLTs offer by design (Moriggl et al., 2020). The outlined deficiencies could be responsible for the absence of a prominent 'component certificate tracking system' in the space industry.

3. Distributed Ledger Technology

DLT could benefit supply chains in the space industry, particularly component certificate tracking, from digitalization and cybersecurity perspectives. Different systems can be created based on DLT, with individual methods to work. A standard definition for DLT is that it is a form of a digital database that is updated and held by every member independently, without a central authority, in an ample network space (Panwar & Bhatnagar, 2020). Its characteristics can make a difference to a use case compared to other technologies, particularly centralized DBs. DLT encompasses generic distributed ledger principles that result in different concepts when brought together with a varying application focus. Blockchain is a way to implement DTL. A blockchain is a chain of blocks connected by cryptographic signatures which ensure the blocks cannot be changed without breaking the signatures. Blockchain, tangle, and hashgraph are three distinct concepts that constitute approaches to implement DLT. The three concepts differ in their architecture, where tangle and hashgraph are based on a directed acyclic graph (DAG), and a blockchain is its own "blockchain"-technology (Burkhardt et al., 2018).

3.1. Foundational Characteristics

In blockchain, fraud and censorship resistance is achieved through chained hashes and consensus results that can be verified - a malicious party cannot quickly mutate or obfuscate data without a network majority. Decentralization and distribution can also be achieved using a 'Distributed Database' (DDB) solution. However, for the given problem space, a DDB has significant limitations resp. risks when compared to a blockchain-based DLT (Health, 2018): message loss, fluctuating message queuing time, remote node failure or temporary downtime, and disturbed or asynchronous message flow between network and node are potential risks associated with DDBs. Such risks can be mitigated through data conflict capabilities that are part of DLT but not a DDB. DLT inherits conflict resolution, transaction verification, and transaction audibility (i.e., consensus).

A blockchain-based distributed ledger is suitable for several application areas; a so-called 'digital evidence chain' can also be traced. These characteristics are discussed in (Chowdhury et al., 2019) and concluded in the following:

Distributed Consensus: one of the critical characteristics of any distributed ledger is its ability to achieve a distributed consensus on the ledger's state without being dependent on a trusted third party. This ability opens up the possibility of building and using a system where all authorized instances can verify every possible state and interaction.

Immutability and Irreversibility: achieving a distributed consensus involving many nodes ensures that the ledger state becomes practically immutable and irreversible after a certain period. This principle is the basis of all blockchains and also applies to smart contracts that allow the use and execution of immutable computer programs.

Data (Transaction) Persistence: data in a distributed ledger is stored in distributed form, ensuring its persistence as long as nodes participate in the P2P network.

Data Origin: a mechanism that facilitates the data storage process in a distributed ledger called a transaction. Each transaction must be digitally signed using public-key cryptography (PKI), which guarantees the authenticity of the data source. The PKI, in combination with the properties of immutability and irreversibility of a blockchain, provides a powerful instrument of non-repudiation for all data in the ledger.

Distributed Data Control: a distributed ledger ensures that data stored in or retrieved from the ledger can be executed in a distributed manner that does not have a single point of failure.

Accountability and Transparency: since every authorized unit can check the ledger's state and every interaction between the involved groups, it promotes accountability and transparency.

The DSTS purpose is the need for a traceable and secure tracking of documents like certificates that contain information that could be sensitive or succumb to non-disclosure agreements. Hence, cybersecurity is a fundamental positive argument for using DLT, where DLT matches cybersecurity mechanisms like data security and data privacy, digital trust, resilience, and forensics (Moriggl et al., 2020). DLT provides

cybersecurity features that are not easily feasible in DB-based systems (Moriggl et al., 2020). The advantages of DLT are having inherent confidentiality, integrity, availability, accountability, authorization, and client fairness capabilities.

3.2. Literature Review

A literature review was conducted to determine the characteristics of systems discussed in the research field that track certificates with DLT and showcase an implementation. The keywords 'Tracking', 'Tracing', 'Certificates', 'Certification', 'Document', 'Documentation', 'Workflow', 'Electronic', 'Space', 'Aerospace', 'ISO9000', 'Blockchain', 'DLT' were used on the databases IEEE, ACM, and Google Scholar. The results include all findings that use DLT for certificates from those databases; non-DLT results were filtered out. In summary, recent research favours blockchain-based systems that track digital credentials or certificates with an underlying permissionless network (Table 2). No solution explicitly for the space industry was found, and none of the findings included a consortium blockchain.

Table 2 Research contributions focusing on certificate tracking systems using DLT

SHORT DESCRIPTION	SOURCE
DigiCert: A Secured Digital Certificate Application using Blockchain through Smart Contracts. The system proposed is built over a public blockchain based on the Ethereum platform.	(Poorni et al., 2019)
Issuing and Verifying Digital Certificates with Blockchain. This study proposes and implements an issuing and verifying model called UniCert based on UniCoin, a digital currency built on blockchain technology.	(Huynh et al., 2018)
Certificate Transparency Using Blockchain. In this paper, leveraging recent progress in blockchain technology, we propose a novel system, called CTB, that makes it impossible for a CA to issue a certificate for a domain without obtaining consent from the domain owner /HL Fabric	(Madala et al., 2019)
SmartCert BlockChain Imperative for Educational Certificates. The electronic authentication system authenticates the documents electronically using blockchain technology, enabling us to implement an integrated system of official documents for the Al-Zaytoonah University of Jordan.	
Robust Crypto-Governance Graduate Document Storage and Fraud Avoidance Certificate in Indonesian Private University In this study, we considered crypto-governance as a solution for critical problems in private university management: fraud avoidance diplomas, transcripts and diploma supplements.	(Taufiq et al., 2019)
A Secure Permissioned Blockchain-Based System for Trademarks. In this study, we have utilized Hyperledger fabric as the permissioned blockchain framework and smart contracts to provide a solution to the current trademark system's financial, procedural, enforcement and protection-related challenges.	(Showkatramani et al., 2019)
CVSS: A Blockchainized Certificate Verifying Support System. In this paper, we propose an approach that utilizes blockchain technology to issue immutable digital certificates and improve the current limitations of the existing certificate verifying systems, such as faster, more trusted, and independent of the central authority.	(Nguyen et al., 2018)
On-block certs: blockchain-based lightweight digital certificates.	(Prado & Henriques, 2019)
Blockcerts is an open standard for creating, issuing, viewing and verifying blockchain-based certificates.	(Santos & Duffy, 2019)

Permissionless systems discussed in these publications lack identity and access management controls suitable for the space industry. The DSTS architecture is different from the current research effort in academia. Instead of relying on purely public blockchains (e.g., Ethereum-based Blockcerts (Santos & Duffy, 2019)) and their limitations regarding identity and ownership, DSTS focuses on strengthening maintenance, guaranteed availability,

access management functionality, and reliable data protection capabilities – properties found in commercial software described in Table 1. The logic of existing systems that track certificates with DLT was studied and adapted to be transformed into a permissioned, consortium-based DLT with an identity-, network-, and storage layer that seamlessly interact with each other. The novelty in the DSTS was the combination of easy-to-use, enterprise-grade, leading, safe and mature, stable DLT combined and applied in a consortium that enables the highly regulated space industry to track the component certificates.

4. Solution

For the first prototypical solution, a decentralized tracking system for component certificates in space titled "Decentralized Certificate Tracking System" (DSTS) was sketched.

Unlike existing alternatives, the DSTS states to be optimized for the space industry, where different digital certificates for different purposes such as documenting a processing step, the part composition, the material properties, or the performance measurement must be obtained and shared. It shall provide conceptual feasibility proof for an open-source, secure, fast and DLT-based solution.

4.1. Methodology

The primary method for developing the prototypical solution and collecting knowledge about DLT and related distributed file systems was adopted from the Design Science Research (DSR), proposed by Hevner and Chatterjee (Hevner & Chatterjee, 2010). The first iteration formalized the business processes and their verification by conducting open interviews with five experts from the European space industry, and in their roles being involved in testing, procurement, or engineering. As a result, 21 user stories grouped in six epics where collected. In a second iteration, wireframes were produced for creating a graphical user interface (GUI)-like visualization of the processes to foster understanding, which was validated by the same five experts. The third iteration resulted in a minimum-viable prototype using Hyperledger Fabric to implement the solution architecture, which was internally tested at a space company and included regular bug fixing.

4.2. Architecture

The architecture visualized in Figure 3 shows an overview of all components that form the DSTS prototype. The front end offers the user interface to interact with the overall system. It is accessible using any modern web browser and provides an application programming interface (API) that interacts with the underlying blockchain (Figure 3).

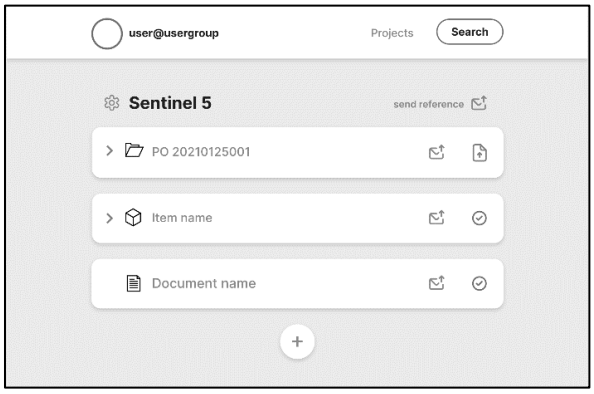

Figure 3 DSTS GUI project view

The design incorporates an authentication service and a custom backend consisting of several participant nodes. Each system participant has a Fabric and an InterPlanetary File System (IPFS) node, controlled by the ordered and orchestrated by the Fabric Gateway. All components are containerized using Docker, which is current practice in web development.

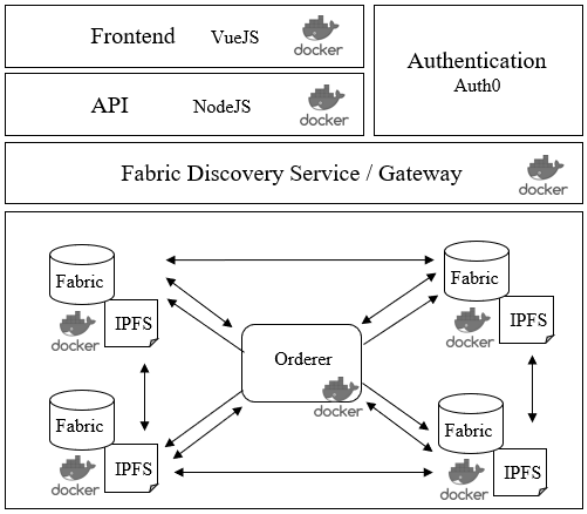

Figure 4 Prototype architecture components

The software prototype consists of Authentication, Hyperledger Fabric chaincode, API, Private IPFS, and the Frontend (Figure 4).

The prototype is designed to run in Docker containers as a scalable concept. The blockchain, the IPFS, the API, and the Frontend are provided using containerized servers. This abstraction layer allows for adding additional nodes to scale and increase decentralization. Hyperledger Fabric requires an orderer node that provides consensus and creates new blocks added to the blockchain by all peers.

To ensure proper access rights and encryption, a Certificate Authority, run as its container, manages all the certificate handling within the network. This setup can be scaled up to use more nodes and allow participants to run their nodes. The file storage uses a private IPFS network, enabling the storage to be decentralized. User experience is a crucial success factor in market adoption. Blockchain, in contrast, relies on certificate files which are cumbersome to use on one device and even worse on multiple devices. To enable a smooth user experience, Auth0 was used as an authentication provider, allowing users to either have their account or use other systems, such as Google, to authenticate their users within the application. The prototype provides an API that can interact with the web-based Frontend and is used by ERPs or other systems reading or delivering data. The prototype was developed using the popular, JavaScript-based, NodeJS, creating a highly efficient way of interacting with the Authorization, the blockchain, and the IPFS service. The user-friendly web interface was based on VueJS, a lightweight, reactive JavaScript framework.

The DSTS frontend application is communicating with both networks, IPFS and Fabric. The Hyperledger Fabric allows for ruling access to various organizations within a more extensive set by creating a Fabric channel. A channel allows the private data to be stored on a ledger while sharing it with an arbitrary number of organizations organized in a set, which Hyperledger Fabric's equivalent refers to as collections. Therefore, on the IPFS network, the access to file data should be determined based on whether a node from an organization is permitted to see the file's hash code on the ledger. A process where the files are encrypted using a symmetric key stored on the ledger and the file hash-code is required. After successfully uploading a file, the IPFS API will respond with the hash code of the file and encryption key. Both data are delivered to the Hyperledger Fabric API, invoking the chain code and storing it on the ledger. The logic allows only sharing or inheriting access to the certification. The document itself does not move outside the initial storage location.

Chain code runs on multiple peers, and in production, an endorsement policy that requires multiple peers to endorse a transaction proposal should be in place. This means several peers will receive the client's request and make requests to the IPFS storage. However, suppose a successful upload to IPFS is required for an endorsement proposal to be successful. In that case, the network will either end up with multiple uploads to IPFS or failed transactions since the same file/descriptor is trying to be written to the storage. As such, the chaincode workflow shall look like the following: 'client -> chaincode -> client -> ordering service -> client -> IPFS storage'

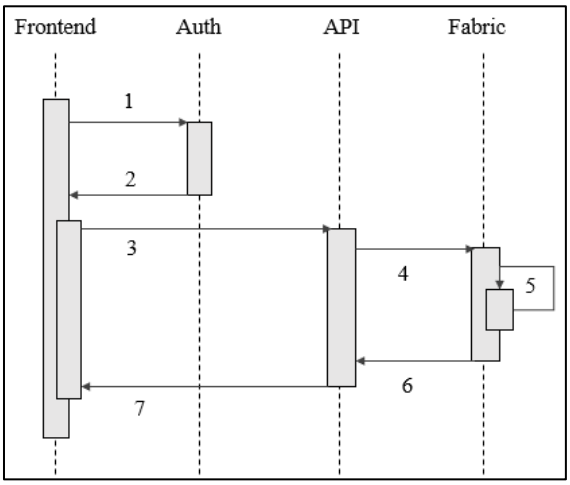

Figure 5 DSTS Login Sequence

When describing the working of IPFS from the user's perspective, it is the location where the hashed document is stored. Accessing the document could be audited by triggering transactions. However, altering the document requires the generation of a new hash. In Figure 5, the workflow between the components is illustrated in the example of a login. The login request (1) happens between the Frontend and the 0Auth service, issuing a token (2). In the next step, the Frontend fetches for the user its project list (3), for which the API sends a 'get projects' (4) to the Fabric. For Hyperledger Fabric to deliver the projects to the API (6) and eventually to the user (7), the blockchain network has to check the permissions of the particular user (5). The permissions are stored on the blockchain in the form of transactions. When storing a certification, the sequence looks slightly different as there is also the IPFS involved (Figure 6).

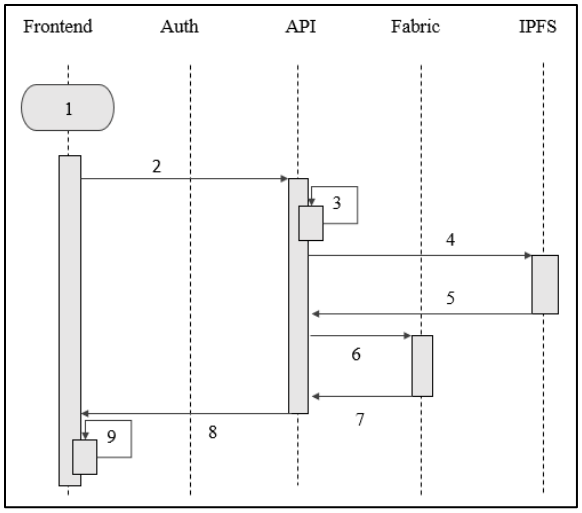

Figure 6 DSTS Storage Sequence

The user is logged in (1), and the project list with its permissions was already fetched/updated. The user uploads a certificate (2) via Frontend, the API encrypts the document (3) using the user's private key, stores the file on IPFS (4) and returns its file hash (5). Secondly, the Hyperledger Fabric creates or updates the record in a transaction (6) and returns the status to the API (7). Finally, the API reports the status to the Frontend (8), where notification is shown to the user (9).

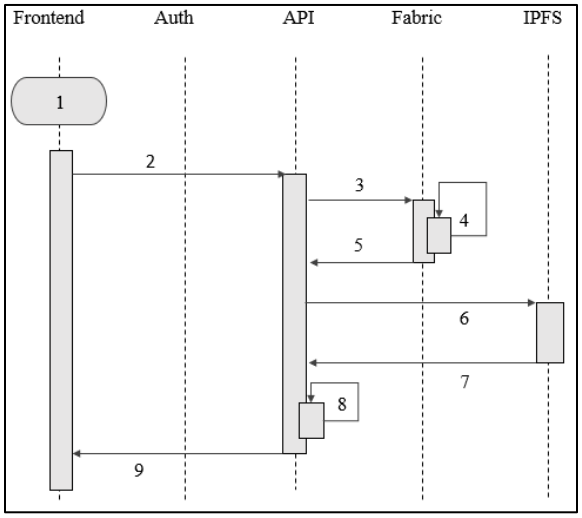

Figure 7 DSTS Retrieval Sequence

The retrieval process for a certificate or a document is shown in Figure 7. Unlike the previous upload, the API has to retrieve the file location the logged-in user (1) is requesting (2). Before the file location is provided, the API pings the Fabric network (3), the network checks for permission (4), and returns the document location (5) to the API. The API can then get the encrypted document from IPFS directly (6), as it now knows the location (7). As the last step, the document is decrypted (8) using the user's private key and returned to the frontend user (9).

4.3. Logical Structure

We propose conceptualizing and developing a space industry ecosystem with a comprehensive, decentralized certificate management service for APSCPs. The service should be globally accessible and support the interface between APSCPs to ensure that the required quality documentation is available, reliable, and transparent across the chain. Such an ecosystem allows each APSCP (obliged to contribute a component certification) to upload and manage access to his component's certificate. Visually speaking, the network resembles a beehive that consists of hives and combs (Figure 8). Each hive contains information about the available and delivered stock items (combs). Each comb contains information generated for specific components, either internally (e.g., lot number of a given metal casting) or externally (e.g., chemical analysis, proof load). The idea is that this hive is interfaceable with standard stock management systems. The information contained in a comb is propagated upon procurement from supplier to integrator, which can embed this information into its stock management system.

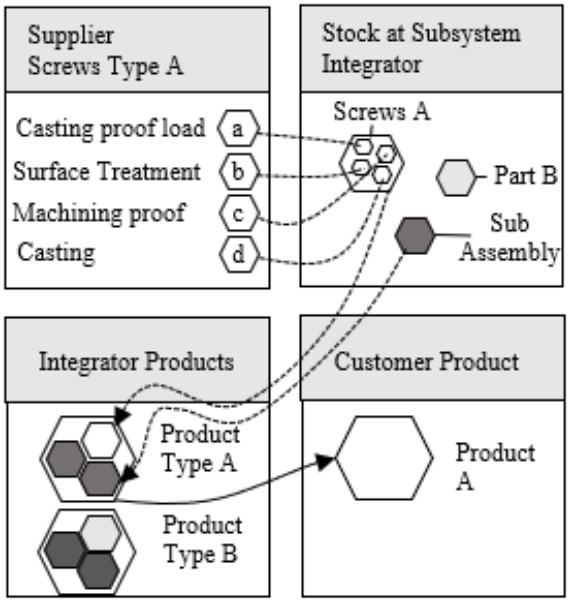

Figure 8 Beehive Structure using Combs

Once the integration of components starts, the so-called 'kitting of the device' calls for the collective information required to define a new product. The

action shapes a new cell into the integrator hive. Figure 8 aims to evidence the nested and recursive nature of the parts and the documentation attached. Different end-products can require documentation related to many screws. Each product comprises components on the other end of the chain, demanding organized, visible, and transparent documentation. Integrity, availability, completeness, and transparency of the documentation from the bottom up of the supply chain enable (1) assessment of the supplier and (2) the overall supply chain quality.

4.4. Backend Workflow

Paper certificates were shipped with parts and materials and then scanned and filed by the recipient (e.g., from supplier A to integrator B). When an assembly containing those parts or materials was shipped (e.g., from integrator B to customer C), all documentation and certification received and created by integrator B had to be gathered manually and included in the shipping. The diagram (Figure 9) shows the new document flow supported by the DSTS prototype and the example roles.

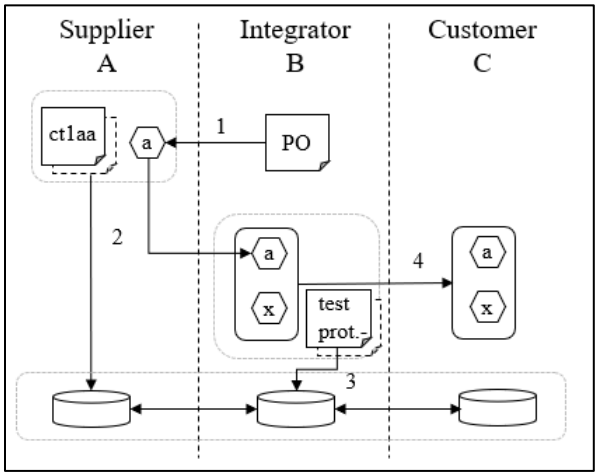

Figure 9 DSTS Documentation Flow

An example process starts with the integrator issuing a purchase order (PO) to the supplier for part A (1). The supplier uploads the respective certificates and documentation to the distributed storage using DSTS (2). In parallel, the supplier ships part A to integrator B. The integrator assembles a device from part A and another part X. After testing the device, a test protocol is uploaded to DSTS (3). The device is shipped to customer C (4). Customer C has access to both - certificates and documentation from supplier A and the test protocol from integrator B. A single source is created by uploading certificates and other documentation into a distributed but shared system. Documentation and certification are only handled once. All subsequent recipients across the supply chain work on a single file. These files can be uploaded by an item (e.g., a certificate) or collection owner (e.g., several files within a project) or by a different participant who receives a shared collection from an owner. Prototype users and roles foresee the same rights for all participants in the network. Accordingly, the prototype was set up. All users of a company can see company projects.

5. Conclusions

The introduction set up the scene for the space component certificate tracking. Chapter 2 discussed the current practices on how the space industry is organizing its component certificates today and answered RQ1. After a market analysis and literature review in chapter 3, a blockchain-based, decentralized architecture was iteratively developed and documented in chapter 4, responding to RQ2 and RQ3. Different to the existing permissionless solutions, the DSTS contributes new knowledge as it is the first verified, permissioned and blockchain-based solution to the challenge of tracking space component certificates in a decentralized manner. The DSTS was designed to be compliant with current space industry requirements. It has the potential to improve current business processes in the space industry when being widely adopted, and its functionalities were validated through interviews with industry experts. A key differentiator to the existing solution is its architecture that allows an integrated Auth0 authentication service for user identification and user login.

There are identified limitations in the presented setup. First, the orderer service regarding Hyperledger Fabric stores the network logic, and the orderer manages the different network interactions in the channel. The prototype had all participants in only one channel and did not have an automated node-adding algorithm, creating a centralized dependence on the API developer. Second, the API stored all user keys in encrypted form for key management convenience, which presents a potential security risk, and is a common challenge for permissioned blockchain-based solutions. Furthermore, apart from the development feasibility demonstrated using Hyperledger Fabric, neither reliable performance benchmarking nor automation through smart contracts was prioritized.

A suitable governance framework that supports the DSTS' adoption in the space industry is a future research area. Second, secure key management should be prioritized to find the right balance between user

convenience and security. Additional load tests to reveal performance boundaries are recommended. Together, they shall help the DSTS' to increase its maturity and, therefore, its chances of being adopted by the space industry.

This research received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI) and was supported by the Swiss Space Center (SSO) and the European Space Agency (ESA).

6. References

Advisera Expert Solutions. (2017). *Clause-by-clause explanation of AS9100 Rev D*. https://info.advisera.com/hubfs/9100Academy/9100Academy_Free_Downloads/Clause_by_clause_explanation_of_AS9100_Rev_D_EN.pdf

Burkhardt, D., Werling, M., & Lasi, H. (2018). Distributed Ledger. *2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings*, 1–9. https://doi.org/10.1109/ICE.2018.8436299

Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. *IEEE Access*, *7*, 167930–167943. https://doi.org/10.1109/ACCESS.2019.2953729

Health, C. (2018). *Why Blockchains Don't Suck, and the Perils of Distributed Databases*. Medium. https://medium.com/@mycoralhealth/why-blockchains-dont-suck-and-the-perils-of-distributed-databases-1a522cc7cfe1

Hevner, A. R., & Chatterjee, S. (2010). *Design Science Research in Information Systems*.

Huynh, T. T., Tru Huynh, T., Pham, D. K., & Khoa Ngo, A. (2018). Issuing and Verifying Digital Certificates with Blockchain. *International Conference on Advanced Technologies for Communications*, *2018-Octob*, 332–336. https://doi.org/10.1109/ATC.2018.8587428

Kanan, T., Obaidat, A. T., & Al-Lahham, M. (2019). SmartCert BlockChain Imperative for Educational Certificates. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 - Proceedings*, 629–633. https://doi.org/10.1109/JEEIT.2019.8717505

Madala, D. S. V., Jhanwar, M. P., & Chattopadhyay, A. (2019). Certificate transparency using blockchain. *IEEE International Conference on Data Mining Workshops, ICDMW*, *2018-Novem*, 71–80. https://doi.org/10.1109/ICDMW.2018.00018

Moriggl, P., Asprion, P. M., & Kramer, F. (2020). Blockchain as an enabler for cybersecurity use case: Electronic health records in Switzerland. *CEUR Workshop Proceedings*, *2749*, 80–91.

Nguyen, D. H., Nguyen-Duc, D. N., Huynh-Tuong, N., & Pham, H. A. (2018). CVSS: A blockchainized certificate verifying support system. *ACM International Conference Proceeding Series*, 436–442. https://doi.org/10.1145/3287921.3287968

Panwar, A., & Bhatnagar, V. (2020). Distributed ledger technology (DLT): The beginning of a technological revolution for blockchain. *2nd International Conference on Data, Engineering and Applications, IDEA 2020*, 1–5. https://doi.org/10.1109/IDEA49133.2020.9170699

Poorni, R., Lakshmanan, M., & Bhuvaneswari, S. (2019). DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts. *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*, *Icces*, 215–219. https://doi.org/10.1109/ICCES45898.2019.9002576

Prado, N. F. R. A., & Henriques, M. A. A. (2019). On-block certs: Blockchain-based lightweight digital certificates. *Revista Dos Trabalhos de Iniciação Científica Da UNICAMP*, *26*, 20396.

Santos, J., & Duffy, K. H. (2019). *A Decentralized Approach to Blockcerts Credential Revocation*. 1–8. https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/final-documents/blockcerts-revocation.md

Showkatramani, G., Khatri, N., Landicho, A., & Layog, D. (2019). A secure permissioned blockchain based system for trademarks. *Proceedings - 2019 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPCON 2019*, 135–139. https://doi.org/10.1109/DAPPCON.2019.00026

Singh, V. B., Benoit, T., & Braibant, V. (2018). Breaking down silos with contract based design for industrial software development : illustrated through an aerospace case study. *Embedded Real-Time Software and Systems Conference*. https://www.erts2018.org/authors_detail_inverted_Benoit Tuur.html

Taufiq, R., Trisetyarso, A., Meyliana, Kosala, R., Ranti, B., Supangkat, S., & Abdurachman, E. (2019). Robust Crypto-Governance Graduate Document Storage and Fraud Avoidance Certificate in Indonesian Private University. *Proceedings of 2019 International Conference on Information Management and Technology, ICIMTech 2019*, *August*, 339–344. https://doi.org/10.1109/ICIMTech.2019.8843784

Țîțu, A. M., & Ioan, P. G. (2019). Regarding quality management system in aerospace industry organizations. *Materials Science Forum*, *957 MSF*, 221–230. https://doi.org/10.4028/www.scientific.net/MSF.957.221