DIGITAL MANUFACTURING PLATFORMS FOR CONNECTED SMART FACTORIES

D3.11 Permissioned Blockchain for ZDM

Deliverable Id :	**QU4LITY-D3.11**
Deliverable Name :	**Permissioned Blockchain for ZDM**
Status :	**FINAL**
Dissemination Level :	**PU**
Due date of deliverable :	**31/12/2019**
Actual submission date :	**28/02/2020**
Work Package :	**WP3**
Organization name of lead contractor for this deliverable :	**Engineering Ingegneria Informatica S.p.A. (ENG)**
Author(s):	**Angelo Marguglio (ENG), John Soldatos (AIT), Jan Juerjens (FHG), Javier Diaz de Gracia (ATOS)**
Partner(s) contributing :	**ENG, ATOS, FHG, AIT**

Abstract: This deliverable is devoted to presentation of QU4LITY blockchain enablers that will implement the secure data sharing and state synchronization across multiple systems in the manufacturing value chain. Such enablers can be also used in the platform tier for sharing and synchronizing information across multiple instances of edge nodes.

Co-funded by the Horizon 2020 Programme of the European Union

www.QU4LITY-project.eu

Contents

HISTORY

Version	Date	Modification reason	Modified by
0.1	25/11/2019	First ToC to be shared	Angelo Marguglio (ENG)
0.2	02/12/2019	Added req. analysis for UCs	Angelo Marguglio (ENG)
0.6	28/12/2019	Minor improvements	Angelo Marguglio (ENG)
0.7	08/01/2020	Minor improvements following preliminary peer-review outcomes	Angelo Marguglio (ENG)
0.9	27/01/2020	Further refinements to the deliverable structure and integration of FHG inputs	Angelo Marguglio (ENG), Jan Juerjens (FHG)
0.10	29/01/2020	Enhancements regarding DLT technologies following internal review	Angela-Maria Despotopoulou (AIT)
0.11	01/02/2020	Further refinements and integration of ATOS inputs	Angelo Marguglio (ENG), Javier Diaz De Gracia (ATOS)
0.12	10/02/2020	Further specifications on DLT in QU4LITY (Ch. 4) and infrastructure to be used (Ch. 5)	Angelo Marguglio (ENG)
0.13	11/02/2020	Minor improvements, ready for the peer review	Angelo Marguglio (ENG)
0.14	26/02/2020	First iteration after receiving the peer reviewer comments from TNO	Angelo Marguglio (ENG)
0.15	27/02/2020	Enriched section 3.1 entitled "Business Requirements".	Angela-Maria Despotopoulou (AIT), John Soldatos (AIT), Jan Juerjens (FHG)
0.16	28/02/2020	Pre-Final version	Angelo Marguglio (ENG)
1.0	28/02/2020	Format quality check, final version for submission	Angelo Marguglio (ENG)

1 Executive Summary

The deliverable D3.11 "Permissioned Blockchain for ZDM" will report on the work performed and first results of Task 3.6 (Blockchains for Secure Decentralized State Management). The scope of Task 3.6, and with it the content of this deliverable, is focused on the development of a DLT Infrastructures to enable secure state sharing and management processes and related supply chain interactions.

In this context, DLT Infrastructure will enable secure state sharing and synchronization of distributed industrial processes involved in AQ/ZDM implementation and will support the traceability of the data, improving the way this information is shared across the different stakeholders involved in the process. This double role of DLT Infrastructure will be enabled by the capability of the underlying blockchain platform to keep confidential data secure within separate environments, enforcing specific access policies. This feature will constitute one of the key requirements for the selection of the baseline technology for the QU4LITY DLT Infrastructure and is summarized under the term "multi-tenancy". Other key requirements of the QU4LITY DLT Infrastructure will be: (i) support for permissioned network, (ii) transaction finality and (iii) support for smart contracts.

Task 3.6, in fact, will also provide the means for running autonomous code (smart contracts) at supply chain level. This will improve agreements management between manufacturers, customers and other stakeholders. Moreover, smart contracts will expose generic or specific (per pilot) business logic by the means of Decentralized Application, knowns as DApps, which will be directly implemented into the underlying blockchain infrastructure.

Overall, this deliverable will show an overview of Distributed Ledger Technologies as well benefits derived from its implementation in QU4LITY context, furthermore, blockchains use case scenario will be presented to highlight some of the possibilities for its usage inside QU4LITY.

2 Introduction

2.1 Objectives and Scope

The whole work-package 3 (WP3 in short) is developing and integrating a range of digital enablers, based on background technological developments of the partners and properly customized to the needs of ZDM, to support the QU4LITY Autonomous Quality paradigm as described in D2.3 (and in the following D2.4). Furthermore, these digital enablers will be integrated as part of ZDM solutions so as to emphasizes interoperability and flexibility and will be further exploited (even outside the project boundaries) through the QU4LITY marketplace (as part of the WP8 activities). Last but not least, the term "digital enablers" implied that each digital component will be reusable and accessible via an Open API, which will facilitate their use in ZDM processes and applications.

The challenge faced by QUALITY is the requirement of interoperability among ZDM digital enablers which may deeply differ from each other. QU4LITY-based systems should, in fact, rely on a layer of abstraction, which, to the extent possible, obscures the system from the underlying implementation.

In the context of this deliverable, Task 3.6 will develop a permissioned blockchain infrastructure for quality management processes and related supply chain interactions. DLT inside QU4LITY will enable secure state sharing and synchronization of distributed industrial processes, moreover, it will enable autonomous code execution by the means of smart contract that will open a new world of possibilities in terms of agreement management across manufacturers, customers and other stakeholders. Furthermore, DLT could be exploited to address today's challenge in complex and often internationally spanning supply chains. In this context fall granular evaluation of provenance of physical goods, smart diagnostics and self-service application for machines and cost avoidance impact on supply chain transactions but, many other challenges can be found and solved with distributed ledger technologies, thus, enriching end-users' experience inside QU4LITY platform, contrary to monolithic non-distributed systems.

The following table illustrates the conditions that render blockchains a suitable choice for supply chain management and other industrial applications, but also the cases where blockchains have to be avoided.

When to Use Blockchain In Industrial Applications	When to Avoid Blockchain in Industrial Applications
There is a need for a shared database	There is a lack of any of the five conditions listed on the left (e.g., when a TTT can ensure trustworthiness across the different writers.
There is a need for a database with multiple writers.	When trust and robustness are not an important issue for the use case at hand.
The use case involves with multiple non-trusting writers.	
It is not appropriate or feasible to rely on a trusted intermediary (i.e. Trusted Third Party (TTP).	
There is a need for interactions between transactions in the database.	

Table 1 - Advantages and disadvantages of Blockchain usage in Industrial Applications

The conditions listed in the table provide a good guide for making a proper use of the blockchain and avoid the implication of the hype that surrounds this technology during the past years.

In-line with the conditions that are listed in the table distributed ledger technologies are well suited to zero defect manufacturing use cases where the business processes require:

- Data travelling between many different data stores, some belonging to external stakeholders, along the lifecycle of said processes.
- Data being exchanged between numerous parties who may have conflicting incentives, or do not have complete trust among them. In such an environment DLT assume the role of the third impartial party.
- Data to be consistent across all participating entities, and/or digitization of such a process is desired. DLT greatly improve the speed and overall efficiency of this requirement in comparison to traditional data storing system architectures.
- Data to be mostly append-only in nature (e.g. new sensor measurements are being persisted and are never updated thereafter).
- Uniform rules to be governing all participants in the system, which furthermore change very rarely.
- The existence for an objective, immutable history or log of facts at the disposal of all parties involved.
- Transparency between peers to be even more important than confidentiality.

Distributed ledger technologies are a powerful tool but are not always the proper tool for the job at hand. Therefore, a proper evaluation must be conducted before resorting to them blindly. The following conditions render distributed ledger-based solutions ill-fitted to zero-defect manufacturing regimes:

- Processes contain confidential data of any kind: The biggest advantage and challenge of distributed ledger technologies is radical transparency. Of course, methods to hide confidential data, while sharing it only to relevant parties do exist, but need to be employed carefully.
- Amount of data is excessively large and/or most of the data is static: Because the replication factor of these systems is so high, they are best suited to databases that have many state changes, or store only the minimum necessary amount of information.
- There is no need for multiple organizations to work together to achieve a common goal. Trust within an organization can be achieved through different means.
- The rules around how business processes are conducted change frequently or change in unexpected ways. In the case of Blockchain for instance, the rules of transactions are often pre-set, and smart contracts do not change execution paths once they have been initiated.
- Other options are simply more efficient. When evaluating blockchain technology for a particular use case, one must consider whether regular file storage, a centralized database, or database replication with master/slave relationship between the original and copies is equally adequate for the task.

2.2 Relation to other tasks

WP3 aims to develop and integrate a range of digital enablers, which will support QU4LITY Autonomous Quality paradigm. The activities within this WP are organized based on the main technological focus of the expected outcomes, as described in the following:

1. **Task 3.1 Scalable, Reliable High-Speed Connectivity for ZDM**

   This task will provide prototype infrastructure for high-speed connectivity of IT systems, machines and other field devices in the factory. Based on requirements, networking and connectivity solutions for ZDM will be specified and provided, based on 4G/LTE, Wi-Fi and LPWAN protocols.

2. **Task 3.2 Customization of HPC and Cloud Infrastructures for Digital Quality Management**

   This task will customize high performance computing (HPC) capabilities to the needs of autonomous quality management. Thus, an HPC infrastructure for state of the art modeling, simulation and data analysis will be provided to support decision-making as well as testing and validation of new ZDM processes. The task will also deploy private cloud infrastructures for supporting ZDM processes, based on cloud-based deployments of enterprise systems and quality management applications.

3. Task 3.3 AI and BigData Analytics for ZDM

This Task will provide the BigData infrastructures that will be exploited in the scope of the QU4LITY deployments, both in terms of Big Data management systems (e.g., Hadoop, Spark, Storm, Kafka) and in terms of the data analytics algorithms. Moreover, the task will establish infrastructures for executing and evaluating different algorithms in-line with popular data mining methodologies such as CRISP-DM.

4. Task 3.4 Fog/Edge Computing Technologies Adaption and Cyber-Physical Systems Integration

This task will develop the fog nodes and edge gateways required to support the project's autonomous quality paradigm. In particular, fog nodes for interaction with ZDM machinery will be developed, along with edge gateways for running automation and analytics functions close to the field.

5. Task 3.5 QU4LITY Cybersecurity, Privacy and Trust Framework

This task will focus on the development of an SPT framework for digital infrastructures that adhere to QU4LITY RA and implement the project's autonomous quality paradigm. The framework will provide different security solutions for industry, focusing in different aspects for monitoring, data sharing, access control of data, etc.

6. Task 3.6 Blockchains for Secure Decentralized State Management in ZDM

This task will develop a permissioned blockchain infrastructure for quality management processes and related supply chain interactions. The blockchain will enable secure state sharing and synchronization of distributed industrial processes, notably the processes entailed in AQ/ZDM implementation. Moreover, the permissioned blockchain will provide the means for running smart contracts at supply chain, in other to reflect agreements (SLAs) between manufacturers, customers and other stakeholders.

7. Task 3.7 Digital Services Interoperability, Packaging and Integration

This task will deal with packaging and integration of the above-listed digital enablers in the scope of ZDM scenarios, such as: (i) Edge Analytics for fast detection or prediction of defects close to the field; (ii) Cloud/HPC Analytics, which will integrate HPC, cloud and Big Data resources as a means of running large scale simulations with very high performance; (iii) Integration of high-speed connectivity with edge analysis for reliable data acquisition and processing; (iv) Flexible cybersecurity at the connectivity and analytics components of QU4LITY solutions and many more.

This deliverable, representing the first main outcome of Task 3.6, presents a depth analysis of frameworks and technologies which can be used to build a Blockchain Platform for Secure Decentralized State Management capable of supporting ZDM processes. It should be noted that this deliverable may not cover an effective prototype implantation of all the generic enablers that will build QU4LITY Cloud infrastructure, while it may come in a subsequent version of this deliverable (i.e. deliverable D3.12). In the scope of the same deliverable D3.12, any change/updates of the components that build the Blockchain Platform reported in this deliverable will be reported by the QU4LITY partners based on experience coming from the practical use of the enablers in the project's pilots.

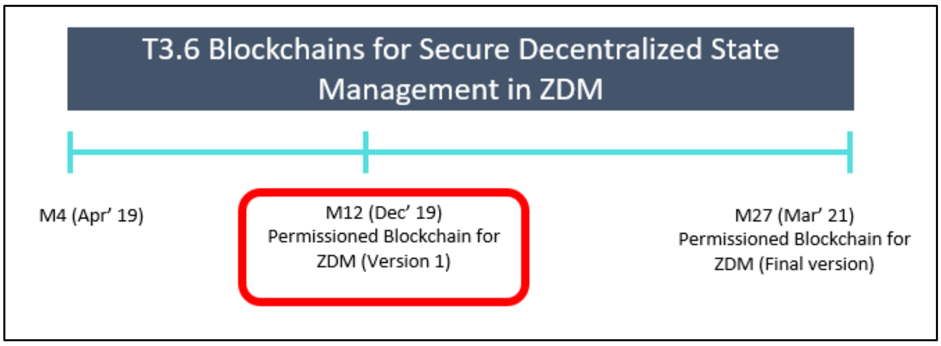

Figure 1 - Task T3.6 timeframe and related deliverables

2.3 Relation to other deliverables

Based on the above-outlined statements it's possible to infer the close linking of the current deliverable with the following documents/deliverables of the project:

- **D2.1 Analysis of User Stories and Stakeholders' Requirements (Version 1)**, which is the main sources for ZDM requirements has been taken into account to properly customize digital enablers to comply with the needs of ZDM specifications.
- **D2.3 Autonomous Quality Vision for ZDM and Quality Management Excellence (Version 1)**, which is another source of requirements that drove the customization of digital enablers for HPC and Cloud infrastructures.
- **D2.11 Reference Architecture and Blueprints (Version 1)**, which defines QU4LITY RA as well as relevant blueprint solutions.
- **D3.7 Fog Nodes and Edge Gateways for ZDM deployments (Version 1)**, since secure data sharing and state synchronization will be also implemented in platform tier across multiple instance of edge nodes.
- **D3.9 QU4LITY SPT Framework (Version 1),** which describes the security policies that will be followed on QU4LITY Cloud.

More links could be found with other deliverables, the one listed above have the most prominent linking.

2.4 Methodology and workplan

The methodology followed for the development and the prototyping of digital enablers for QU4LITY Cloud Platform comprises the following phases which are also shown in Figure 2:

- **Phase 1 – Requirements Analysis**: During this phase, requirements of DLT technologies to bring up QU4LITY Blockchain Private Cloud will be identified to prototype the most suitable platform in accordance with QU4LITY Reference Architecture.
- **Phase 2 – Network deployment**: During this phase, a primer of QU4LITY Private Cloud will be prototyped and implemented.
- **Phase 3 – Smart Contract implementation**: During this phase, will be implemented set of "standard" smart contract which will facilitate secure data sharing and state synchronization across multiple instances of the edge nodes.

2.5 Document Structure

D3.11 is divided in the following main parts:

- **Introduction**: This section identifies the tasks of the project related to the deliverable including information on objectives as well as a short description of the relationship of the current deliverable with the results of other tasks and work-packages.
- **Context and Requirements**: An analysis of other project context and especially the relationships with the QU4LITY Reference Architecture and business requirements, aligned to the overall Autonomous Quality vision pursued by the project.
- **Distribute Ledger Technology**: An analysis of distributed ledger technologies, serving as a reference to build Permissioned Blockchain infrastructures for supporting ZDM processes, adapting these technologies to the project needs and defining our baseline.
- **QU4LITY DLT Infrastructure**: This section will provide insights on the possible adoption of blockchain technologies in a IDS Data Space (proposing several approach to include it as part of an IDS infrastructure), moving then toward the definition of the architecture of the blockchain network to be adopted in QU4LITY, and presenting the deployment and hosting infrastructure.
- **QU4LITY DLT Services**: This section presents the main DLT services (such as orchestration, data publishing and configuration) needed to deploy an operate the QU4LITY DLT infrastructure.
- **Conclusions:** This section provides summarized information on the QU4LITY Permissioned Blockchain Infrastructures to pave the way to the technical developments in WP3, WP4 and WP5, as well as the validation scenario in WP6 and WP7.

An overall view of the document structure can be seen in the figure below.

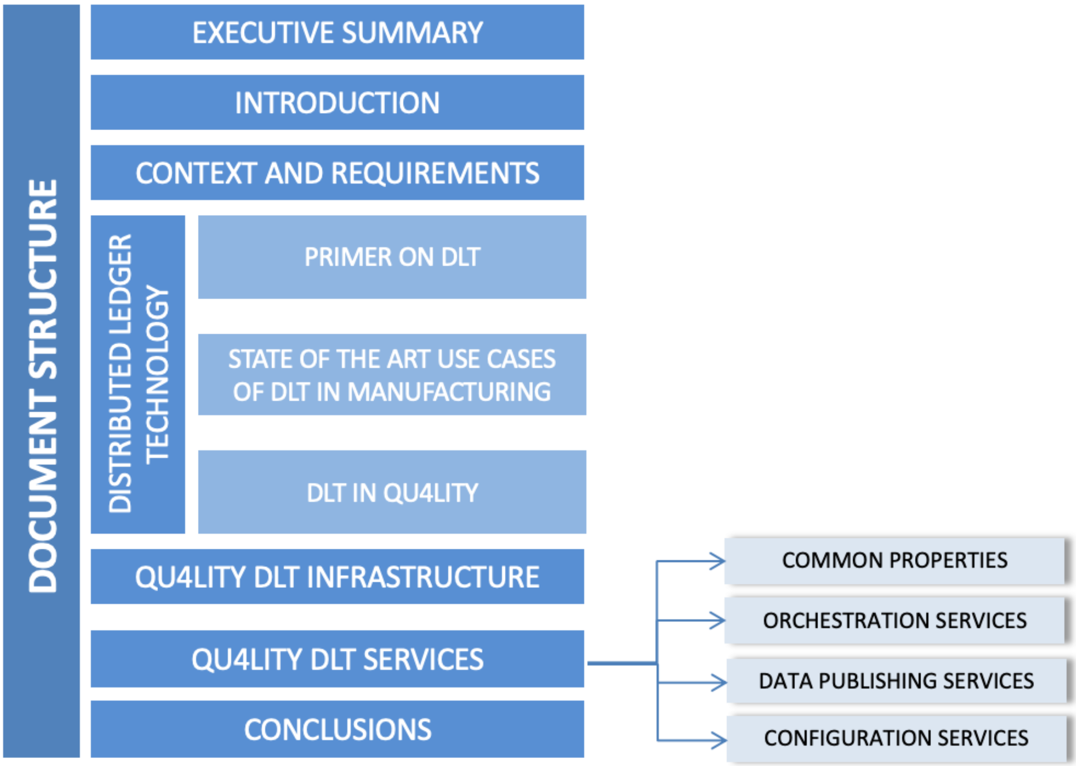

Figure 2 - D3.11 document structure

3 Context and Requirements

QU4LITY Value Chain Ledger and Private Ledger for ZDM are core part of the QU4LITY RA. This is depicted in Figure 3, which illustrates different components and views of the RA.

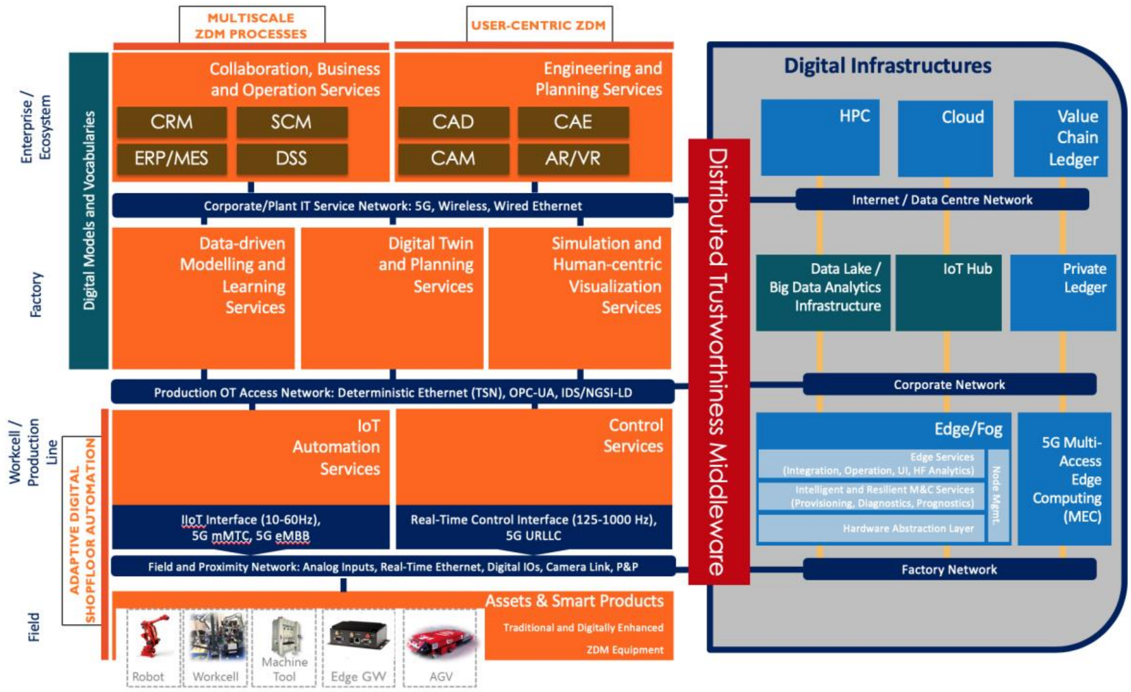

Figure 3 - Initial version of the QU4LITY RA

In-line with deliverable D2.11, the Value Chain Ledger and Private Ledger are part of the **Digital Infrastructure Pillar.** This pillar is intended for the Fog/Cloud/HPC infrastructure required for the operation of the digital services pillar as well as communication and data distribution enablers to create direct interaction between the different layers. This layer is therefore focused on the enablers for (big) data ingestion, processing and management both data in motion and data at rest.

The physical deployment of QU4LITY should benefit, in fact, from DLT Infrastructure to keep confidential data in separate sandboxes with specific access rights. Moreover, DLT Infrastructure will address data integrity and non-repudiation of data enforcing and ensuring critical security policies across peers of QU4LITY Platform.

Components presented in this deliverable adhere to these specifications of the RA and interoperate with the remaining architectural components to realize the QU4LITY Cloud Platform.

3.1 Business Requirements

Today's manufacturing companies struggle to establish interoperability between various organizations and systems. The need of interoperability has led to the hiring of specialized intermediate companies to take care of end-to-end integration. This has typically caused high integration costs while keeping the diffusion relatively low. For this reason, companies have been collaborating to accelerate the integration of a digital supply chain (DSC) as a means of creating a multi-stakeholder environment in which, even competing companies, are collaborating to pursue integration of the entire supply network.

The benefits of digitalizing supply chains are numerous:

- Efficiency increase associated to reduction of governance costs and costs related to transactions with participants of other ecosystems.
- Reduction of human error due to the automatization of data flows.
- More flexible supply chains design.
- Reduction of product and/or service costs.
- Reduction of supply chain lead times.

The concept of businesses electronically sharing information that was traditionally communicated on paper, such as purchase orders and invoices, is often referred using the term **Electronic Data Interchange** (EDI)[1]. The EDI approach specifies and uses standards for the communication between the trading partners, specifically:

- EDI standards are used for the interaction between trading partners business information systems (such as ERP and MRP systems). The use of relevant standards (such as X12, GS1 XML, EDIFACT, etc.) is agreed between the trading partner.
- EDI standards based information is transmitted over secure protocols like sFTP (Secure File Transfer Protocol), AS2 (Applicability Statement 2) or VAN (Value Added Network).

Despite the fact that the strategic choice of digitalizing supply chains constitutes a no-brainer for modern organizations, operations still suffer from certain insufficiencies. Those reach the peak of their noticeability when business processes require documents to travel across organizations who do not share common Enterprise Resource Planning (ERP) systems. Data often do not flow smoothly through the handshakes or interface points between systems. Those defects are accentuated during transference of ownership (that in a paper-dominated world takes place at the point in time when legal documents are exchanged). Visibility is limited at the hand-off points of funds, raw materials, tools, spare parts, or finished products. This lack of transparency is often intentional, as companies avoid exposing their competitive advantages (e.g., an inexpensive supplier who delivers quality products on time). Finally, even in a digitized business process flow, exchange of ownership still may require more than a business day to be completed, validated and communicated to all involved parties. Common scenarios still involve people hand-typing paper documents into an ERP, electronic exchange of documents massively between ERPs through ETL (extract, transform, load) automatic routines outside business hours, intermediate repositories between ERPs to achieve interoperability that add steps to the processes, etc.

[1] https://www.arcesb.com/resources/edi/?ref=rssbus

Recent developments in the fields of Blockchain and Distributed Ledgers, have provided interesting and innovative proposals on how to tackle the abovementioned challenges, improving greatly the processes currently accepted as best practices. Blockchains are being used to solve problems in supply chain management by eliminating the need for a trusted third party to certify raw materials, components, or finished products, as they travel through a supply chain. Every participant, or node, contains a copy of all transactions, on whom updates require few minutes maximum (the time depends on how quickly the participants reach consensus on the global state). This provides an audit trail of every transaction that has occurred in the system. Since all participants have a copy of all past transactions in the network, any participant can detect if a transaction has been falsified. Instead of examining raw materials, components, or finished products at several points in the supply chain, a record of the inspection would be available and bound to the item as it moves through the supply chain. Although a record of the transaction is public and tied to the movement of physical items across the network, specifics such as the quantity of goods, or the identity of the parties transacting, can be done pseudo-anonymously in a blockchain. Such a granular view of movement through supply chains furthermore improves resource allocation.

Furthermore, companies are interested in enhancing closed loop autonomous control systems providing them with DSS functionalities. In this context, ZDM paradigm could be fully followed starting a revolution of industrial manufacturing processes that will bring to a more respectful and conscious environmental impact by big enterprises. On this matter, the reduced wastes and smarter energy consumption policies could represent a real deal to environmental concern which today represents the most discussed topic between researchers and scientists.

Overall, a blockchain approach to recording transactions and events across the supply chain, offers the following business benefits over conventional EDI transactions:

- A transparent, validated single version of the truth, which is ensured by the anti-tampering properties and the distributed consensus mechanisms of the blockchain network.
- Real-time visibility on the entire network, as the blockchain records all transactions and breaks the information silos across the various trading partners. By removing the "silos" that are created by EDI point to point transfers, blockchain approaches enable the calculation of appropriate KPIs.

4 Distributed Ledger Technology

4.1 Primer on DLT

Distributed Ledger Technology, or DLT in brief, is a generic term defining any OLTP[2] distributed system that maintains a synchronized copy of the transaction log on all nodes and has no central point of control. In a DLT system, all nodes are equal (*peers*) and no "master" copy of the ledger exists, as they are all updated simultaneously. The term Blockchain is used for a specific implementation approach where a group of transactions is committed to the ledger as a *block*, blocks are chained together in a linear sequence and cryptographic techniques are used to seal individual blocks – and the chain itself – in such a way that no transaction can be changed or removed without detection.

A very generic model of how transaction processing works in a blockchain system is given below. Note however that this *typical* sequence of steps may significantly differ in actual implementations.

1. A client creates a new transaction – i.e., a *proposed* change in system state.
2. The new transaction is broadcasted to all the peer nodes of the system via a P2P network protocol.
3. The new transaction is added to the pool of pending transaction waiting to be confirmed.
4. Peer nodes collectively validate the pool of pending transactions, following some implementation-dependent protocol and algorithm; the result is a new block *containing only the approved transactions*, which appear in chronological ordered[3]. This step is called "distributed consensus".
5. The new block is broadcasted to all the peer nodes via a P2P network protocol.
6. All peer nodes update their copy of the ledger, appending the new block at the end of the chain of blocks.

It is worth noting that the timing and specifics of the distributed consensus protocol (step #4) are the core issues that affect the performance, scalability, reliability and sustainability (i.e., the cost of resources spent for the processing of each single transaction) of all the different blockchain implementations on the market.

From a technical perspective, a blockchain can be thought as an LTS (labelled transition system) constituted by a State, which records the state of each peers of the network, and a State Transition Function (STF) which takes a State and a transaction as inputs and returns a new State as output.

[2] OnLine Transaction Processing
[3] The order of appearance of transactions within a block is part of the decision process.

Figure 4 - LTS example

Formally we can define STF as:

APPLY (S, TX) -> S' or ERROR

where S represents the old State, TX a transaction and S' the new State in case of success. STF is executed continuously from the peers of the Network to accomplish the decentralized consensus of the blockchain technology. Depending on the type of blockchain architecture, STF can be computationally burdensome, leading to a high per-transaction cost. We can distinguish two basic architectures: *permissionless* – also known as *public* - and *permissioned*.

- In a permissionless / public blockchain system, anyone can join the network at any time and everyone is anonymous, to the effect to no peer node can be trusted to behave according to the given business rules. We call this a *trustless environment*. The key to effectively enforce business rules in a trustless environment is the consensus protocol, which is backed by an incentivization scheme, designed to reward rule-abiding members and penalize rule-breakers, to the point that any advantage gained by breaking the rules would be outweighed by the costs sustained to do so. The key ingredient for rewards is an internal digital currency – also called a cryptocurrency[4] - that has an economic value and can be exchanged within the system. On the other hand, the cost component is usually an artificially-difficult computation problem that peer nodes must solve in order to participate to the consensus process – a method called Proof-of-Work (PoW). The problem with PoW is that it puts a heavy burden on the system, making individual transactions very expensive and slow to process[5].
- In permissioned blockchain systems, only a known set of participants can join the network, which implies that permissions are granted / revoked by a trusted authority[6]. In this context, there is no need to enforce the rules by means of

[4] Some DLT platforms of the latest generation are trying to solve the problem of trust in a trustless environment without the use of a cryptocurrency (or even of a blockchain) but the effectiveness of their approach is, to date, questionable at best.
[5] Other distributed consensus protocols, like Proof-of-Stake (PoS), are being actively experimented these days and will probably make public networks more efficient in the future.
[6] Which might be a consortium composed by all participants, a single organization trusted by all participants, or anything in between: the actual level of "decentralization" achieved by the system is a matter of contractual agreements.

some decentralized – and inherently inefficient – algorithm: emphasis is put on transaction throughput and fault tolerance.

That said, both architectures are focused on rules: their main point is making all stakeholders confident that no violation of the common rules of transactions (i.e., those agreed to by all participants) is possible. When it comes to the definition of rules, however, two approaches are possible: having them hard-coded in the system vs. letting participants define them as they see fit. Systems of the former type are clearly very specialized – in fact, all those in existence are cryptocurrency platforms – and cannot be extended by their users. The latter kind are much more flexible: sub-systems having their specific rules and "state" (and data model) can be defined by users as application-specific code, which is "deployed" on the system at large and thus becomes a software asset that may be executed on any – or every – peer node. In blockchain jargon, such asset is called "smart contract". Smart contracts are the biggest innovation in blockchain technology, introduced by the Ethereum platform in 2015. Thanks to them, a blockchain platform can play the role of a fully-fledged distributed computing infrastructure: smart contract applications are immaterial, as they run "anywhere on the network", but at the same time are safe to execute as their code is stored on the immutable ledger. In business scenarios, smart contracts are often created as self-enforcing agreements between two or more parties: the rules describe what will happen if and when some conditions are met; when the trigger goes off, changes are applies to the application's state, to the effect that the agreement is automatically enforced.

To summarize, DLT eliminates the need – and the cost – of a trusted third party as the middleman in transactions having economic value. At a lower level, DLT systems are inherently more robust and resilient than traditional ones, as they don't have any single-point-of-failure and can work without disruption when multiple nodes become unavailable. The immutable ledger means trackability, accountability and non-repudiation. However, all these advantages come at a cost: DLT systems have weaknesses that are sometimes mitigated by permissioned platforms, but not to the point of being on par with "classic" application architectures, like Cloud computing. These weaknesses stem from the need of a distributed consensus protocol (performance and scalability penalty) and of massive and permanent data replication (storage inefficiency). Moreover, as the key point of distributed ledgers is transparency (all stakeholders should be able to verify that what is written on the ledger is correct), data privacy may be difficult or impossible to achieve. Last but not least, the immutable nature of the ledger means that DLT systems are at odds with the European regulation on personal data (GDPR), whenever personal data is involved. All these weaknesses may represent a serious concern, but DLT still opens a world of new opportunities in terms of addressing new markets and of complexity reduction in many contexts, such as IoT and ZDM.

4.2 State of the Art Use Cases of DLT in Manufacturing

4.2.1 Overview

Despite the fact the DLT technologies in industrial environments are in their infancy, several uses of blockchain technologies for quality management have been proposed and outlined in the research literature [Andrews17], [Wang17]. Following paragraphs outline the most prominent use cases. These use cases can serve as a reference for designing QU4LITY open calls in order to attract proper quality management use cases / pilots to be deployed over the QU4LITY platforms.

4.2.2 Monitoring of Raw Materials and Spare Parts in the Supply Chain

The variation of raw materials is a primary cause of defects and hence the focus of quality control. However, granular evaluation of provenance of physical goods, i.e. tracking their composing parts back to their first source thus demonstrating their authenticity, often proves a challenge in today's complex and often internationally spanning supply chains.

Stocking the right amount of raw materials and spare parts over time is another key component in just-in-time lean manufacturing and distribution. Companies want to ensure that those elements are available when needed but overstocking them can prove costly. Furthermore, their visibility is limited at the distribution points where transference of ownership between parties occurs.

In this context, distributed ledger technologies can be used to offer highly secure and immutable access to supply chain data [Kim18]. For raw materials and spare parts indispensable to manufacturing processes, they are able to provide a digital platform enabling their physical traceability. In combination with Internet of Things-enabled sensors, they can monitor the journey of a good from raw material to finished product. First, the sensors capture finely granular real-time data about environment characteristics as well as location and timestamps throughout the supply chain. Then the DLT platforms manage the chain of custody for said goods, enabling ownership to be transferred and traded on a network using smart contracts. What is more, governance and validation of the logs for those activities is equally distributed between the peer nodes of the system, making their tampering an expensive therefore uneconomical effort for malevolent actors.

4.2.3 Smart Diagnostics

DLT platforms can be used for developing smart diagnostics and self-service applications for machines, where the machines themselves will be able to monitor their state, diagnose problems, and autonomously place service, consumables replenishment, or part replacement requests to the machine maintenance vendors. DLT technologies further expand the possibilities for using an innovative pay-per-use model for those services. The rationale is that a Ledger Service is responsible of evaluating the service received (to the satisfaction of both the owner and the user), while the Ledger itself ensures that the relevant log recordings cannot be falsified in any way.

Following that, payments can automatically be extracted through cryptocurrency micro-transactions between digital wallets. Pricing may also be flexible; the final fee paid by the receiver of the maintenance service can be automatically calculated by a smart contract, depending on which and to what extent the agreed terms have been realized [Andrews17], as evidenced by the relevant data.

4.2.4 Monitoring conformity to Service Level Agreements (SLAs), Standards and Regulation

The advantages of translating Service Level Agreements to self-imposed smart contracts are noteworthy [Uriarte18]. First and foremost, this process automates their lifecycle stages: discovery and negotiation, deployment, monitoring, billing/penalty and termination. Furthermore, it introduces clarity, since all rules are univocally defined, and transparency, since all interactions between physical and non-physical parties are recorded in a definitive manner. Lastly, DLT technologies are by definition suitable for environments where parties do not need to cultivate and maintain relationships of trust among them [Zhang19].

In a real-world application, a “master” smart contract can be designed to enforce legal standards and agreements of any kind. By cross-examining the data uploaded by different stakeholders all parties can verify to what extent the process meets the predefined regulatory conditions. Once all the requirements are met, the regulatory approval may be automatically granted through a smart contract with no further need for on-site inspections or in-person verification.

4.2.5 Equipment identity management

DLT technologies are well-suited to provide an effective mechanism that enables equipment management, and more specifically identity authentication and authorization. Quality control requires strict supervision over which equipment has clearance to modify which subsets of data collections. What is more, the logs assembled during the procedure ought to be immutable. By assigning a digital identifier to each piece of equipment, allowing it to univocally “sign” its interactions with data, transparency and, therefore, an uncontested single source of truth are formulated step by step.

In practice, various blockchains and other DLTs provide the possibility of creating unique accounts, fitted with a pair of cryptographic keys; a public one to be universally authenticated and a private one to “sign” transactions. In such a configuration, any interaction with data is signed with the equipment's private key and can be verified by anyone who has access to the latter's public key. This verification proves that the equipment had access to the private key, and therefore is likely to be the one associated with the public key. This also ensures that the digital signature has not been tampered with, as it is mathematically bound to the key it originally was made with. From their part, smart contracts can be employed for both handling authorization requests and translating authorization policies into machine-readable self-executing code.

Overall, the use of DLT for equipment identify management, provides the following benefits:

- Security risks related to password authentication are mitigated. For example, there is no possibility for the third party to use a simple/frequent password or to share it unintentionally.
- Authentication of mobile devices, such as phones, tablets and AR glasses, is less prone to risk. No cookies or other retrievable objects remain on the device.
- Storage and logs are immutable per DLT specifications.
- Weak authentication protocols and human negligence do not pose a threat.
- Security regulations are more severe and privately manageable as opposed to cloud repositories.
- There is no centralized data honeypot for hackers to target.
- There is no need for action if the external user for some reason needs to be un-certified in the future.

4.2.6 Maintenance Equipment Leasing

In complex and large-scale manufacturing projects, purchasing heavy equipment that will be used only periodically is often uneconomical. Equipment used for maintenance tasks entails besides its own storing and repairing costs. As a consequence, leasing this type of machinery can be a lucrative option to cut down expenses. However, the conventional leasing process tends to be an effort-consuming endeavor, pertaining to time-consuming negotiation cycles and inflexible bureaucracy. Smart contracts can provide a framework to largely automate the subprocesses that compose the leasing procedure, such as two-part negotiation, payment accomplishment and insurance agreement.

To start, the owner of a machine needs to state its availability for leasing by recording the fact in the DLT system. Then a prospective contractor declares their intention of acquiring the machine, after having evaluated that it fits their needs. The two parties' identities as well as that of the machine are subsequently registered on the leasing ledger, a fact that is confirmable by all network participants. Afterwards, the transaction on the DLT may be updated with a particular lease option (i.e. short-term, long-term etc.) and insurance option. For the final stage, the DLT may orchestrate payment for the lease and insurance using a cryptocurrency, after the related smart contract has been triggered. It is noteworthy that the monetary transaction and its terms are again publicly recorded in a tamperproof way.

4.2.7 Knowledge dissemination with built-in protection of Intellectual Property

It is not uncommon for dissimilar projects albeit utilizing common sub-systems to encounter comparable challenges when attempting quality monitoring. The existence of a common data warehouse, searchable for encountered issues and tested countermeasures would evidently be an asset for all interested parties. In practice, a scenario like this would raise demands for assurances that the interests of the original knowledge owner are being protected. Intellectual property may also extend to include copyright, trademark, and patents.

DLTs are an instinctive answer to property rights issues arising in trustless environments [Li18]. A blockchain may record a hash of a document (or an image or their location etc.) and then control and track its distribution. A smart contract initiated by the owner of a piece of knowledge can act as an intermediate for confirmation or rejection of sharing requests. The establishment of a signed connection between the two parties can additionally be a solid base for further collaboration between them.

4.2.8 Circular economy

The term "*circular economy*" refers to an economic system aimed at employing reuse, sharing, repair, refurbishment, remanufacturing and recycling to minimize the use of resource inputs and the creation of waste. From a manufacturers' perspective it is an attractive option for social, financial, environmental and legal reasons. However, a key success factor in any such a production chain is the condition and quality status of the returned items to be pushed into the remanufacturing process.

A distributed ledger that constantly monitors the lifecycle of a product arms a remanufacturer with substantial advantages towards this direction. First, it provides an accurate and unchangeable account of the item's provenance and journey, filtering out counterfeit and misused products. Second, it asserts quite transparently that the item enters remanufacturing being on a status that complies with some minimum quality criteria and desirable specifications. And, finally, it provides a guarantee of the item's status after the finalization of the remanufacturing process, useful, for instance, to compose warranty documents.

4.3 DLT in QU4LITY

In QU4LITY we aim at creating one single DLT Infrastructure for both the "value chain ledger" (one single instance shared between multiple participants) and the "private ledgers" (instances dedicated to a single factory), as defined in the RA. The enabler for this double role is the capability of the underlying blockchain platform to keep confidential data secure within separate environments, enforcing specific access policies: such capability is therefore one of the key requirements for the selection of the baseline technology for the QU4LITY DLT Infrastructure, and is summarized under the term "**multi-tenancy**"[7]. In QU4LITY context, multiple scenarios of aforementioned use cases are getting assessed. Smart diagnostics, monitoring of raw materials and spare parts in the supply chain, translating of SLAs into self-imposed smart contracts and circular economy define the milestones that DLT usage in QU4LITY has set. In this matter, several requirements need to be respected to accomplish QU4LITY goal of building an autonomous quality model to meet the Industry 4.0 ZDM challenges. Such requirements can be summarized as: assuring

[7] In the ICT industry, multi-tenancy means that a single instance of the software serves multiple customers.

immutability of transactions, assuring trust where not taken for granted (which is intrinsic in DLTs), support for automated transactions.

Formally, the main key requirements are:

- Support for **smart contracts**: the business logic of the system *must* be customizable by means of application-specific code that is executed as part of the transaction validation process.
- Support for **permissioned networks**: the system *must* be suitable for running as a private infrastructure, subject to access restrictions. In particular, the "distributed consensus" process (the core of transaction validation) *should not* be based on economic incentives.
- **Transaction finality**: once a valid transaction is committed to the ledger, it must not be subject to post-commit invalidation.

4.3.1 Selection of baseline platform

We have analyzed the state-of-the-art of blockchain platforms in order to find the most suitable one for QU4LITY's needs. Our pre-selection criteria where: open source software, wide and active community of developers and code maturity (i.e., validated in several demanding real-world scenarios). Five platforms have been identified as the initial candidates:

1. **Bitcoin**: the archetypal blockchain invented by the pseudonymous Satoshi Nakamoto as a cryptocurrency system (i.e., decentralized digital money).
2. **Ethereum**: the first "2.0" blockchain, which adds smart contracts to the original Bitcoin concept and thus extends the applicability of DLT to distributed computing.
3. **Quorum**: a variant of the Ethereum blockchain, redesigned for use on permissioned networks only and with a strong focus on security and data protection.
4. **Hyperledger Fabric (HLF)**: an industrial-strength, original design of a 2.0 blockchain that is focused on performance, reliability and flexibility.
5. **Corda**: another industrial-strength, original design of a DLT platform (it doesn't actually use blockchain technology) which targets the financial sector.

In the following table, we match the five candidates with the four above-mentioned high-level requirements:

	Transaction Finality	Smart Contracts	Permissioned Networks	Multi-tenancy
Bitcoin	No	No	No	No
Ethereum	No	**Yes**	Limited	Limited
Quorum	Limited[8]	**Yes**	**Yes**	**Yes**
HLF	**Yes**	**Yes**	**Yes**	**Yes**
Corda	**Yes**	**Yes**	**Yes**	**Yes**

Table 2 - DLT Comparison in QU4LITY

According to above comparison, only two candidates are a full match against requirements: HLF and Corda. Given that both are roughly equivalent in terms of performance, scalability and robustness, we have examined in more detail their features as development platforms and their proven reputation as commercial products. The clear winner with respect to these aspects is HLF: it provides a nearly unrestricted development environment for several programming languages (Go, NodeJS and Java) and has a convincing success record in the industry at large[9].

For the above reasons, and also thanks to the extensive experience acquired by some technical partners in a previous research project with similar requirements (FAR-EDGE, H2020-FOF11-2016), HLF has been selected as the baseline blockchain platform of choice for QU4LITY. The role of HLF in the FAR-EDGE architecture was that of a peer-to-peer network that enabled seamless collaboration between Edge Computing nodes without any central service acting as the coordinator.

4.3.2 Hyperledger Fabric Overview

HLF is a permissioned blockchain developed by IBM and currently owned by the Linux Foundation, which released it under the business-friendly Apache 2.0 license.

Peer nodes are the fundamental elements of the blockchain, and where the blockchain is stored. Peer nodes and clients of an HLF network enroll through a trusted Membership Service Provider (MSP). MSP component provides an abstraction of cryptographic protocols needed to issue and validate a certificate, providing modularity of membership operations and interoperability across different membership standards and architectures. The HLF platform comes with its own Certificate Authority (CA) implementation, but any third-party tool capable of generating standard digital certificates will do.

[8] Strictly speaking, it's not supported; however, it is extremely unlikely to occur in real-life scenarios.
[9] See https://wiki.hyperledger.org/display/LMDWG/Use+Cases for a partial portfolio of use cases.

With respect to permissionless blockchains, HLF simplifies the distributed consensus mechanism by removing the concept of economic incentives for trustworthiness and introducing *trusted* validation peers (VP). The transaction validation mechanism in HLF therefore becomes:

1. A transaction is sent by a client to one trusted VP of choice.
2. The VP validates the transaction against the rules, as coded in the relevant smart contract (*chaincode* in HLF jargon); it does that by *simulating* the execution of the code, so that application state changes are identified and collected, but not yet applied.
3. The VP signs the output of the transaction (new version of the application state) and returns it to the calling client; this process is called *endorsement*.
4. Optionally, the client can get multiple endorsements by involving other VPs.
5. The client sends the endorsed transaction to the ordering service, so that it will be committed to the ledger and become effective. Depending on configuration, the ordering service may be a cluster of dedicated nodes[10] or the whole network[11].
6. The ordering service is in charge of putting all incoming transactions, which are generated concurrently by all the active clients, in the "correct" order, by assigning them a sequential identifier; this means, for instance, that a transaction depending on previous transactions must appear in the ledger after them.
7. The ordering service broadcasts the confirmed transactions, in the correct order, to the entire network – including the originating client.
8. All peer nodes update their copy of the ledger accordingly.

This mechanism is graphically represented in Figure 5 below[12]:

[10] In HLF versions <= 1.4, this will typically be as an Apache Kafka cluster; see https://kafka.apache.org/
[11] In HLF versions >= 2.0, the network will use the RAFT consensus protocol; see https://raft.github.io/
[12] From the HLF documentation: https://fabrictestdocs.readthedocs.io/en/latest/arch-deep-dive.html

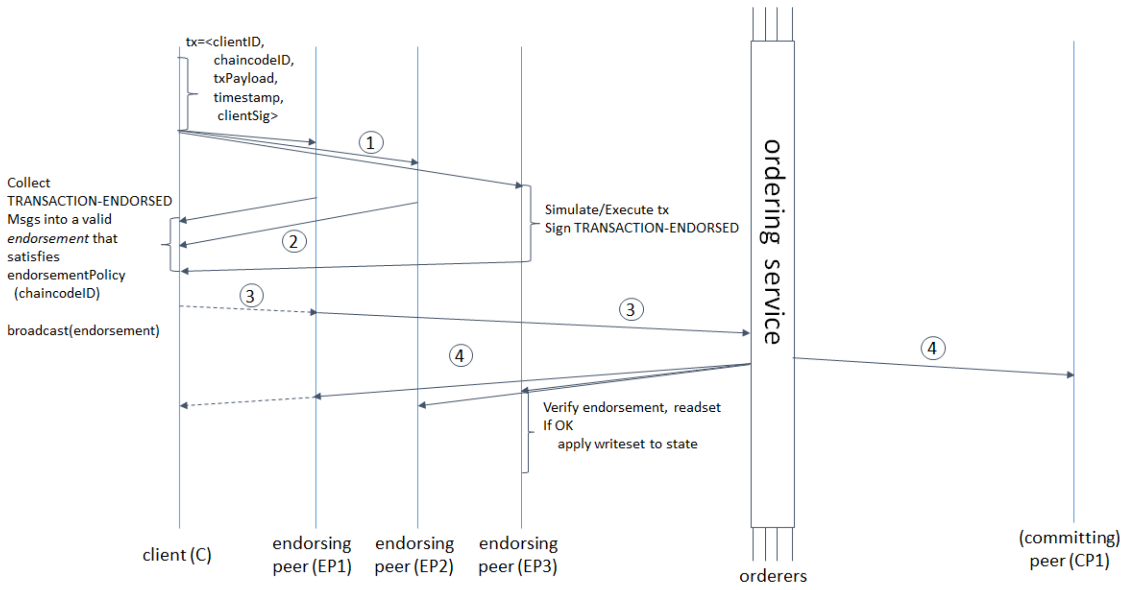

Figure 5 - Transaction validation process in Hyperledger Fabric

HLF supports multi-tenancy through *channels*, an abstraction that groups participants into segregated sub-ledgers that are only visible and accessible to authorized nodes. For example, if two nodes join the same channel, they will be the only ones having a copy of the ledger for that channel. A node can participate in multiple channels at the same time. Also, HLF has built-in support for *private data collections*, which is a finer-grained data privacy abstraction that does not require to define an entire channel just for the purpose of maintaining a subset of data private.

HLF features of a well-documented series of case studies and success stories:

- **Walmart** thought that blockchain technology might be a good fit for the decentralized food supply ecosystem. To test this hypothesis, the company – in partnership with IBM – created a food traceability system based on HLF. Walmart can now trace the origin of over 25 products from 5 different suppliers using a system powered by HLF. The company plans to roll out the system to more products and categories in the near future.
- **Maersk** needed an open and neutral platform for managing sea freight and supply chains, enabling automated exchange of information between all participants. Using TradeLens[13], a HLF-based commercial product developed in partnership with IBM, they were able to achieve their objectives and also provide a valuable service to all the stakeholders of their ecosystem, namely cargo owners, terminal operators, sea/land carriers, governments agencies and financial institutions. The advantages are in terms of automation of complex multi-party processes (re-implemented as smart contracts), transparency and standardization, which overall mean a significant reduction in time, cost and risk.

[13] See https://www.tradelens.com/

- **Honeywell Aerospace** wanted to create a marketplace for used aircraft parts and cut purchasing time from days or weeks down to seconds as well as connect each physical part to its digital infrastructure. Thanks to HLF, Honeywell Aerospace can now enjoy purchase time reduction from days to minutes and more than 50 storefronts in the marketplace with an average sale of $4 million in less than a year.
- **Sony Global Education** wanted to develop with a consortium of government agencies and organizations, a next-generation credentials platform to record education and training credentials of Japanese citizens. With HLF, Sony Global Education succeeded on achieving his goals and identified the worldwide need of such platform.

5 QU4LITY DLT Infrastructure

QU4LITY DLT Infrastructure is the result of previous partners' experiences in distributed ledger technologies and analysis of different business and governance models to best fit QU4LITY needs. QU4LITY DLT Infrastructure, therefore, will provide the capabilities of exploiting supply chains and closed loop control systems, bringing added value to ZDM solutions adopted in QU4LITY.

Moreover, during the development of DLT Infrastructure there will be found examples and insights from QU4LITY project to feed into a next version of the International Data Space Association (IDSA) position on blockchain technologies. Therefore, the same core aspects of IDSA will be kept in mind while developing QU4LITY DLT Infrastructure to ensure trust between participant and ensure data sovereignty.

This chapter is structured as follows. We begin with a short overview of the IDS ecosystem as a basis for the QU4LITY DLT infrastructure, followed by a key concept of the IDS as a whole and an IDS connector, IDS broker and IDS app store as a main component, including information about the conformity requirements. Then we sketch the relationship between the IDS and Blockchain in order to illustrate how transactions inside the ecosystem recorded securely, followed by a discussion on deployment issues.

5.1 Relationships with IDSA developments

The International Data Space Association (IDSA) is an industry and user driven initiative that aims to develop a global International Data Spaces (IDS) standard and reference architecture which ensures data sovereignty for the creator of the data. Digital Transformation and Innovation in today's business world has increased the intrinsic value of data which get usually exploited by companies in exchange of services. IDS address the new need for vendor independent data ecosystems by specifying an architecture, interfaces and sample code for an open and secure data ecosystem of trusted partners. IDS reference architecture focuses on the concept of "data sovereignty" allowing organizations to share datasets in a secure and controlled way using the International Data Spaces Connector concept. In QU4LITY context, the same aspects can be found in DLT Infrastructure which features among many, the absence of a single trusted party and a decentralized nature. Some of the features of blockchain are, in fact, consistent with features of the IDS architecture while many others are complementary, such as data immutability.

Blockchain technology can boast of three core features which make it very appealing to researchers, entrepreneurs and the IDSA itself:

1. P2P based distributed database.
2. Distributed computing by the means of smart contracts.
3. Data sovereignty under restricted governance (permissioned blockchain).

IDSA emphasizes the creation of data-driven business-ecosystems and marketplaces based on trust between participants and data sovereignty for which Blockchain technology has proven to be enough mature and suitable for the purpose. IDSA has, thus, identified three scenarios where DLT could be applied:

1. Blockchain Based Data Assets Sharing, in which data is shared to feed new data driven services or for business process synchronization. In this context, an IDS Connector is used to share data with other participants within the ecosystem, whereby the owner of the data can control with whom the data is being shared. This way the blockchain is used to store and exchange the actual payload data.
2. Blockchain Based Clearing House, in which the trust authority that act as middleman is replaced by the public consensus given by blockchain technology. Moreover, the clearing process gets empowered and overcomes the limits of complex chain of transaction as well as patching the issue of a single point of failure. Here the blockchain only contains the clearing data.
3. Blockchain Based Identity Management, in which blockchain acts as identity management database and enables reliable and secure identity credentials exchange and thus only contains the identity management related data.

In QU4LITY context, DLT usage falls into the first scenario, a private blockchain will be implemented to empower closed loop control systems and a permissioned one will be used to enrich supply chain exploiting data tracking possibilities.

Moreover, QU4LITY experience could highlight new insights to feed IDSA developments and stimulate new discussions and publications on blockchain technology usage in data-driven business ecosystems.

The International Data Spaces (IDS) has been developed as an implementation basis for the industrial ecosystems to ensure a secure and trustworthy data exchange environment.

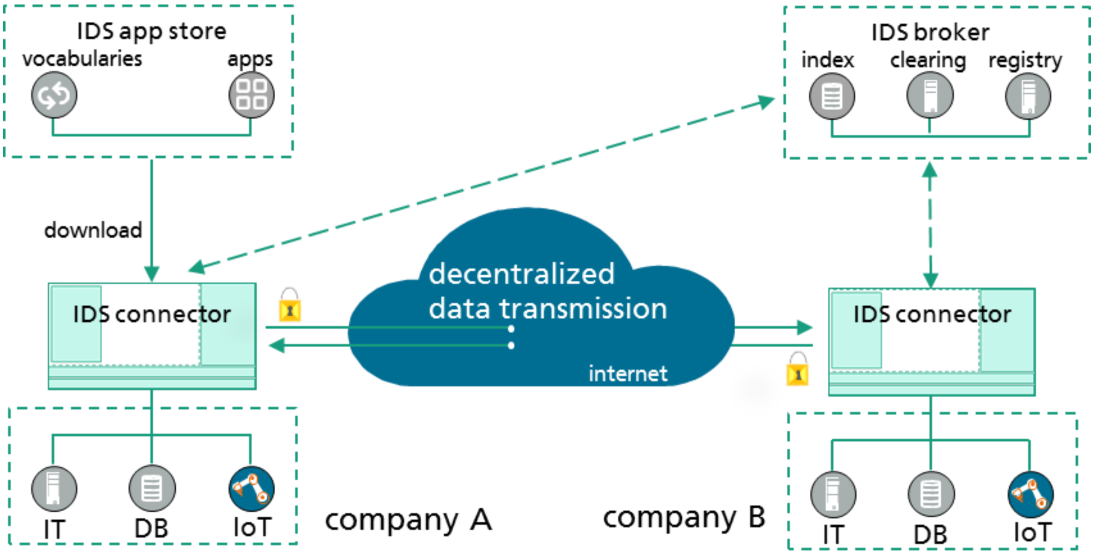

Figure 6 - IDS Reference Architecture [Ott19]

Here we discuss the information the stakeholders need to take part in the ecosystem. The main focus is on connecting manufacturing service providers and service users via the IDS infrastructure.

5.1.1 Platform components

The IDS provides the registration of ecosystem members, service offers in the industrial ecosystem and the negotiation of contracts between service users and service providers. Every ecosystem member receives their ID from a IDS identity provider. The IDS maintains a list of available services and supports the completion of contracts between service provider and service user as well as the billing and accounting.

The IDS app store provides app that can be connected to an IDS connector [Ott19]. A special app is the blockchain app which allows the recording of transactions within the IDS Hyperledger Fabric-Subsystem.

Manufacturing service providers connect their services via IDS connectors to the IDS platform [Ott19]. User of manufacturing services also connect to the IDS platform via IDS connectors.

The IDS storage is a service component where IDS users can save their project data on. A good reason to use this service is the possibility of a user's internet connection with a low bandwidth which makes the exchange of big files laboriously.

5.1.2 Service provision via the IDS

As shown in fig 6 the IDS communication backbone is being used between service users and service providers. For a better understanding we will briefly sketch out the IDS architecture. The IDS1 has been conceptualized as a tool for data exchange between data provider and consumers to ensure the data sovereignty of the data provider. To achieve this function the IDS does not save data but ensures a secure exchange connection between the communication partners who use certified stack connection components.

5.1.3 IDS gross architecture

The IDS contributes to the design of company architectures with regard to digital transformation. A detailed description of the IDS architecture can be found in [Ott19].

The following figure demonstrates the positioning of the IDS in a typical architecture stack of a digital industrial business.

From a technical perspective the IDS connects data providers with data consumers via standardized connectors. To ease the search of data sources, the IDS broker manages a registration of data sources. The following figure provides a overview of the IDS architecture.

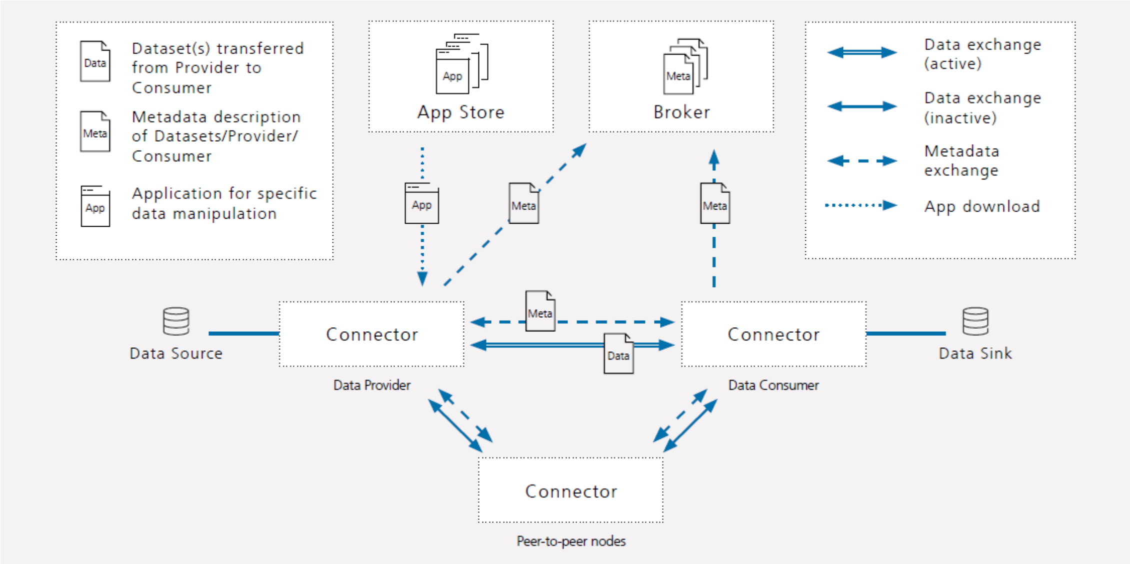

Figure 7 - IDS system architecture [Ott19]

5.2 Architecture of the blockchain network

The DLT Architecture foreseen in QU4LITY consists of two building blocks, mainly a private blockchain (restricted within a single organization) and a permissioned one (encompassing multiple organizations). The underlying idea is to enforce pilot's experience in QU4LITY exploiting two different scenarios:

1. Enforcing closed loop control systems (M2M integration)
2. Empowering supply chains (B2B integration)

Today's growing complexity of products and process and growing consumers' whishes are increasing the pressure of manufacturing industries which struggle to keep up with global demand. In this context, speed, flexibility, quality and efficiency represent the key factors to boost manufacturing industries growth. A significant milestone has been achieved thanks to the digitalization of industrial process and the birth of closed-loop manufacturing (CLM).

CLM reintegrates components and/or materials, that would have been wasted otherwise, into a new cycle of life to produce new products. CLM, thus, continuously improves the cost, time and quality of the manufacturing process to accelerate the delivery of products at the optimal level of quality and cost. Moreover, CLM can vastly improve ecological sustainability of industrial processes by enabling predictive analysis and maintenance.

In QU4LITY context, CLM is achieved by implementing a private blockchain network and, more precisely, a smart contract based autonomous control system. In this scenario, autonomous smart objects could act as peers under a private blockchain network, based on Hyperledger Fabric, and handle machinery workloads based on peers' consensus, thus enabling plug-and-produce pattern model. For this scope, custom "generic" smart contracts will be developed and deployed on QU4LITY onpremises blockchain to enable autonomous control and to some extent, increase overall manufacturing production chain performances.

Speaking about supply chains, QU4LITY could inject DLT into the business. Today's companies are facing the challenge of tracking, in an effective way, service deliveries, so to provide visibility in the supply chain and to promptly meet customers' demand. The current solution adopted by companies operating in supply chains has been to rely on specialized intermediate companies, whose role is to establish interoperability by mapping and integrating company-specific data for various organizations and systems. High integration costs and relatively slow diffusion on the market makes this approach unsustainable in the long run, thus, new solutions based on cloud integration are getting explored, nowadays, to identify a cost-effective business model for interoperable digital supply chains (DSC). QU4LITY explores the advantages of DLT in B2B contexts while developing a cost-effective solution to boost growth and cooperation between companies, even when competing to each other.

In this context, a permissioned blockchain, based on Hyperledger Fabric, will be implemented to achieve a cost-effective business model for interoperable DSC based on smart contracts. According to Szabo's definition: "smart contract is computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality and even enforcement), minimize exceptions, both malicious and accidental, and minimize the need for trusted intermediaries [...]". QU4LITY, therefore, may become a service provider offering blockchain network access to trusted members. This solution will address many of the limits that keeps occurring in today's finance transactions such as securities threats, the need of a middle-man and the lack of support for documents trading; moreover, QU4LITY permissioned ledger will be able to provide security and flexibility at same time and at lower cost than traditional transactions. It's important to note that extremely vertical supply chains won't be able to benefit from DLT usage in QU4LITY as decentralization aspect will be suppressed implicitly.

5.2.1 Architectural description of how Blockchain can be integrated in the IDS

Originally, the blockchain concept has been developed as a decentralized and distributed digital ledger. The basic idea behind this is to make the ledger verifiable and audit-proof through distribution, so that it is unlikely that recorded transactions can be changed synchronously. It became popular with the digital cryptocurrency Bitcoin, which uses blockchain to record Bitcoin transactions.

As such, a combination of IDS and blockchain would be very beneficial, as visualized in the following picture:

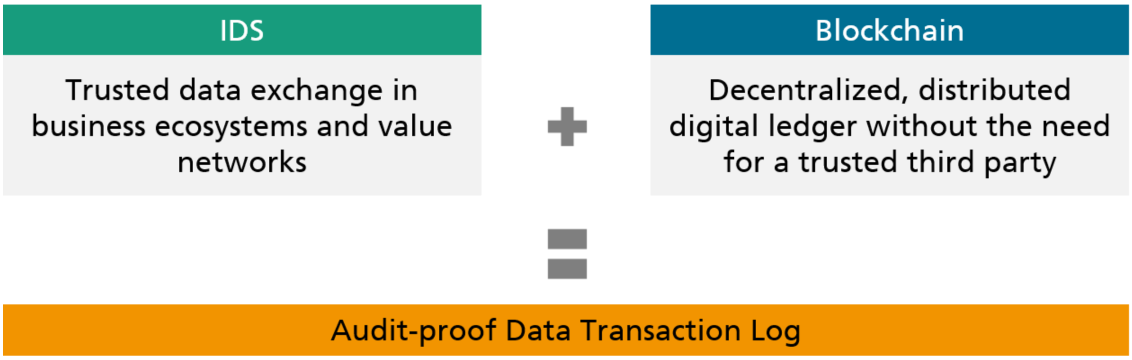

Figure 8 – Benefits of combining IDS and blockchain

We use Hyperledger Fabric for blockchaining transactions within the IDS ecosystem. A distributed ledger is installed in trusted locations. Every IDS connector can contain the IDS blockchain app which records the transmission or receipt of data in the general ledger.

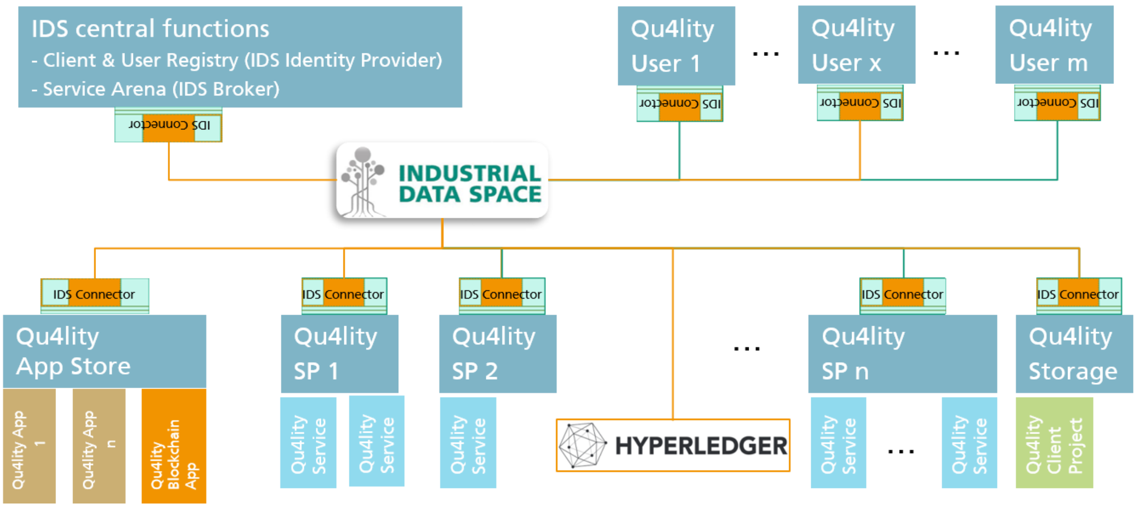

Figure 9 - Gross system architecture

To ensure a reviewable transmission of data between the participants of the ecosystem, the IDS connectors will be linked to a Hyperledger Fabric Blockchain Subsystem in order to protocol every transmission. Manufacturing service provider connect their services via the IDS connectors to the IDS platform [Ott19]. Your connectors may have connected a blockchain app for audit-proof transaction recording, but this is not mandatory. Users of manufacturing services also connect to the IDS platform via IDS connectors. They can also use their connector's blockchain app. From the point of view of the IDS the blockchain implementation can be regarded as a service.

There are multiple possibilities to integrate a service in the IDS infrastructure, as visualized in the following picture:

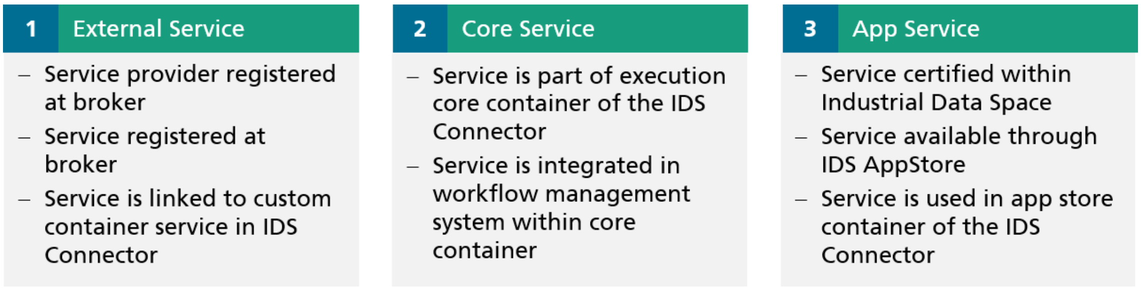

Figure 10 – Services integrated in the IDS infrastructure

One such possibility is to integrate blockchain as an external service via an IDS connector, as shown in the following picture:

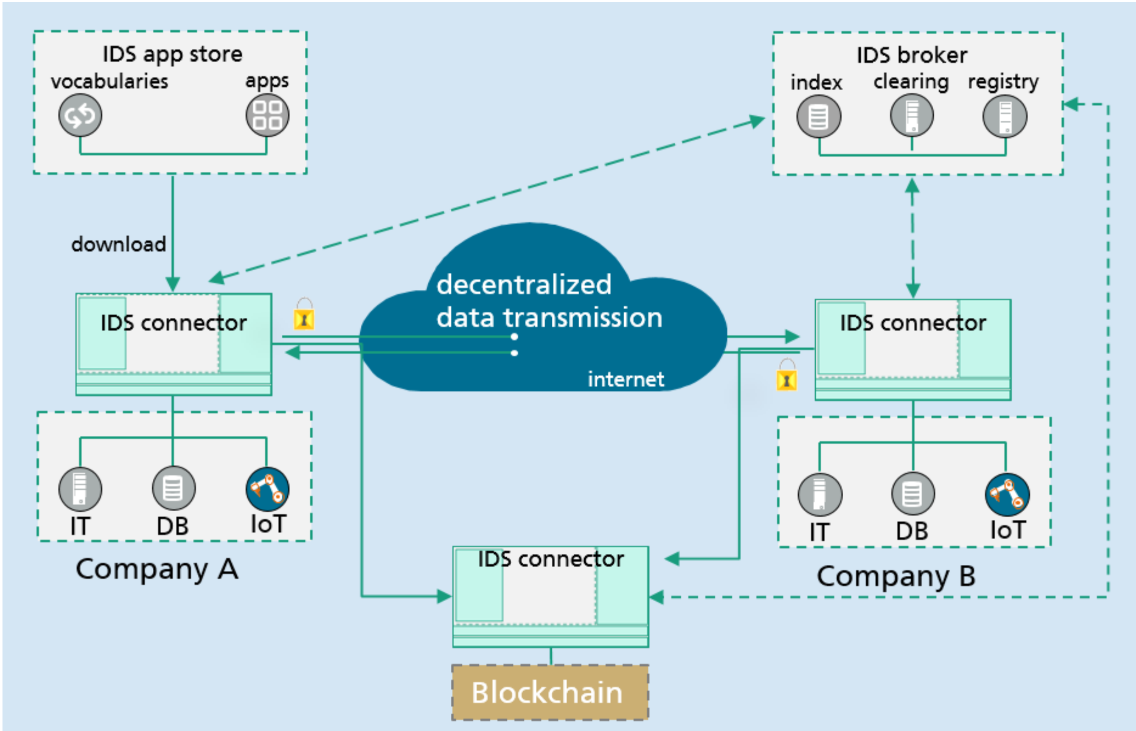

Figure 11 – Integrate blockchain as an external service via an IDS connector

In this case the blockchain implementation has to provide a connector interface. If a IDS connector wants to log a data transmission activity, the connector has to send a request to the blockchain connector. The blockchain connector is a regular IDS connector, that contains a blockchain service module inside a custom container. This service module receives the protocol request from an IDS connector and relays it to the blockchain infrastructure. This approach implies an implementation of a connector interface for the blockchain implementation including a grave change in regards to the implementation of the connector's core modules. A standard connector must process the communication with the blockchain connector in combination with the communication between the connectors of service users and service providers.

A second alternative would therefore be to integrate Blockchain as a core service integration, as shown in the following picture:

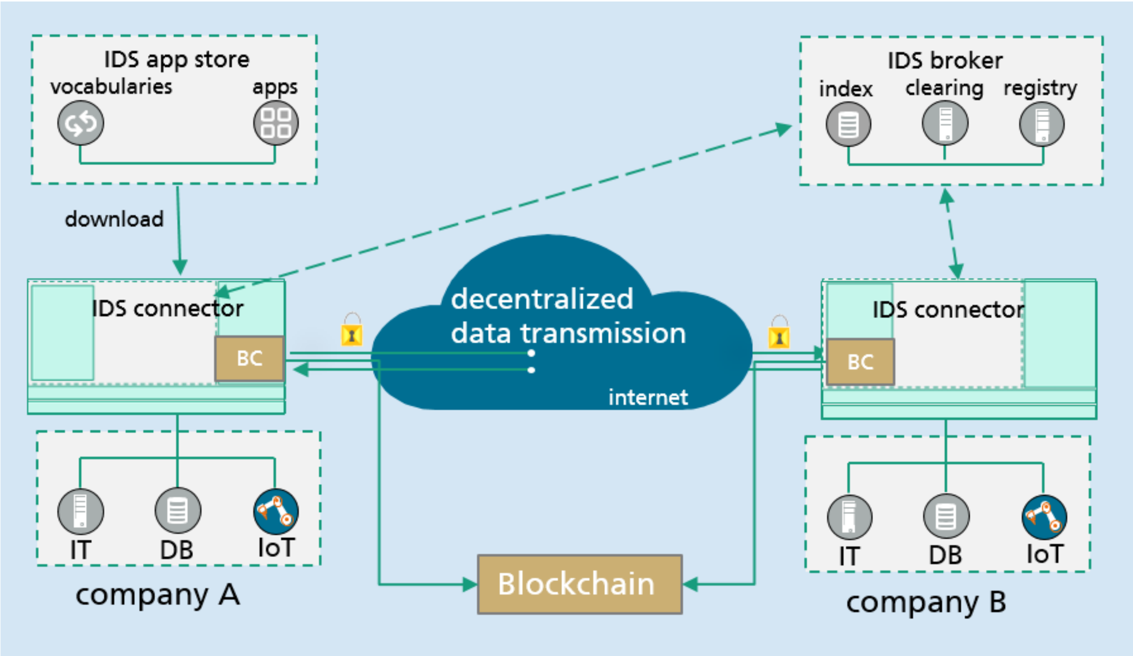

Figure 12 – Integrate blockchain as a core service

Data transfer logging is carried out in a »hidden« mode through a Blockchain module in the core container of the IDS Connector. This module connects directly to the Blockchain infrastructure. The respective core module would have to be adapted according to the requirements of the Blockchain infrastructure.

The advantages and disadvantages of the three options are thus shown in the following overview:

	1 - Blockchain as External Service	2 - Core Service Integration	**3 - Blockchain App Integration**
Pros	– Integration transparent to user – Complexity increase for core container not significant – Individual Blockchain technology replaceable as long as protocol is not changed	– Integration transparent for user	– Low effort, no change of core container – Individual Blockchain technology can be easily replaced – Same functionality as options 1 and 2
Cons	– Change to core container required – Dependency on external service during run-time	– Complexity increase, thus, reduction of reliability and maintainability of core container – Individual Blockchain technology cannot be replaced easily	– Explicit app call required
Assessment	– Middle way between options 2 and 3 – Cons outweigh pros	– Cons outweigh pros	– **Most pragmatic option that meets key requirements** – **Highly flexible** – **Pros outweigh cons**

Figure 13 – Pros/Cons analysis on different ways to integrate blockchain in IDS

As a consequence, we have opted alternatively for the integration of Blockchain in the IDS via an app, as shown in the following picture:

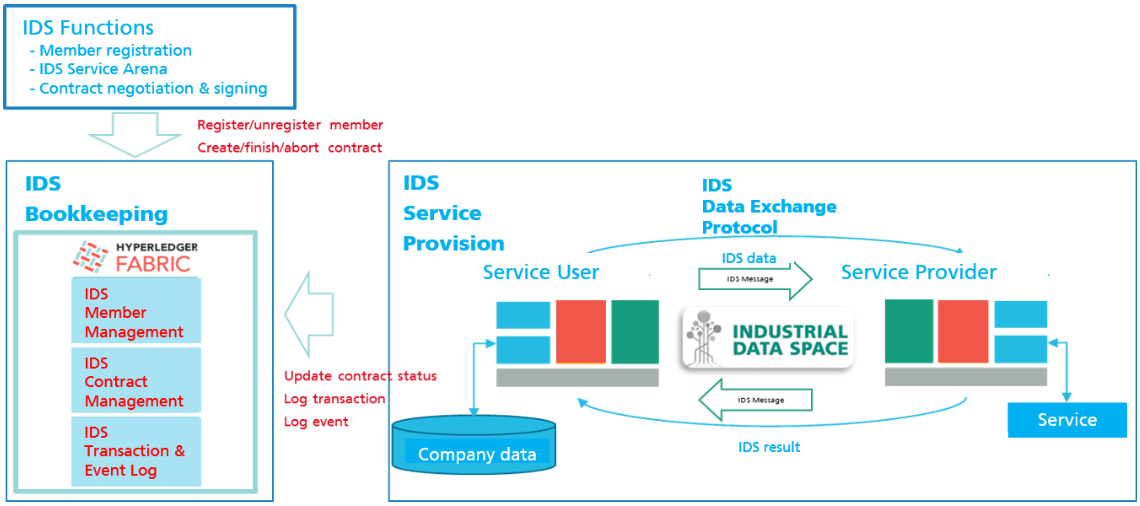

Figure 14 - Digital Data Chain

This app can be booked in the IDS App Store and, if necessary, integrated into a standard IDS connector in the app container. In order to record data transmission between IDS Connectors, the blockchain app communicates directly with the blockchain infrastructure.

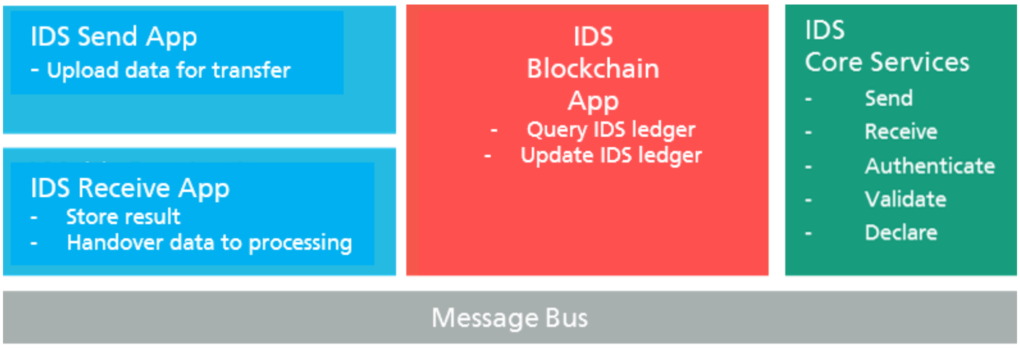

Figure 15 - IDS Connector with Blockchain App

The app only needs to be integrated into the workflow that is defined and executed in the execution area of the IDS Connector. Since a message bus is used as a communication backbone in a connector, this integration is straightforward.

The following figure demonstrates a transmission of a service request of a service user to a service provider.

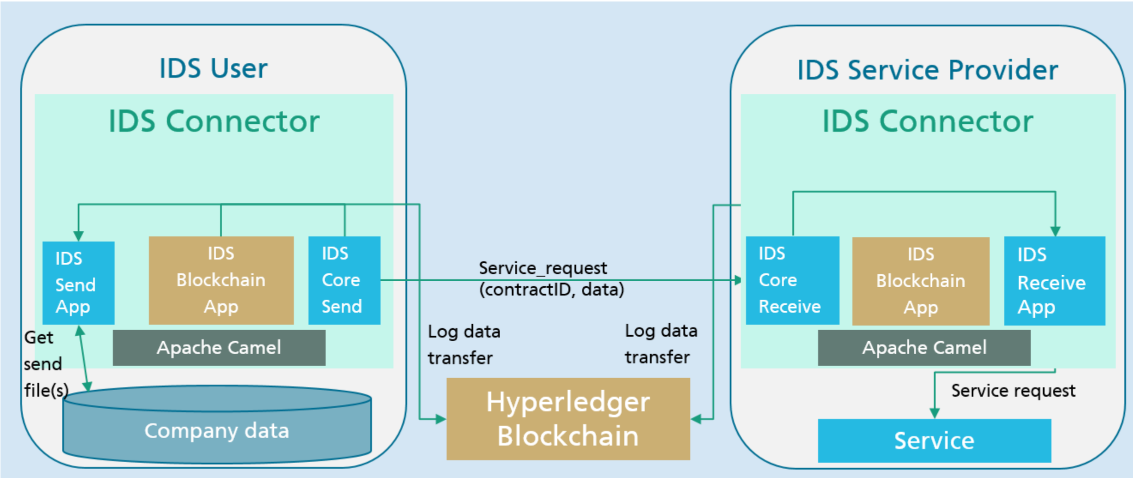

Figure 16 - Service request with Blockchain transaction logging

The next figure shows a communication between the blockchain apps in the service user's connector and the blockchain infrastructure.

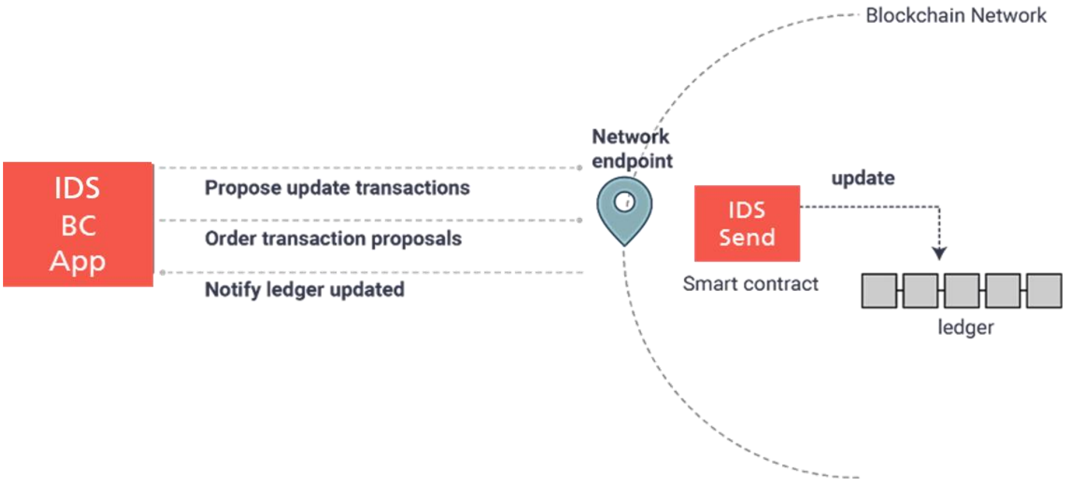

Figure 17 - Blockchain app communication (sender side) [14]

A service user chooses the data to be transmitted and uploads them with the sending app. The send app triggers a general ledger update in the blockchain app before the data to be transferred is transferred to the sending module of the connector core. After receiving a "ledger updated" confirmation, the connector core transfers the data from the blockchain app to the receiving connector.

When receiving data, the receiving connector checks the blockchain protocol for a corresponding entry on the sending side (see figure below) by forwarding a request from the connector core to the blockchain app.

[14] Source: http://hyperledger-fabric.readthedocs.io/en/latest/write_first_app.html

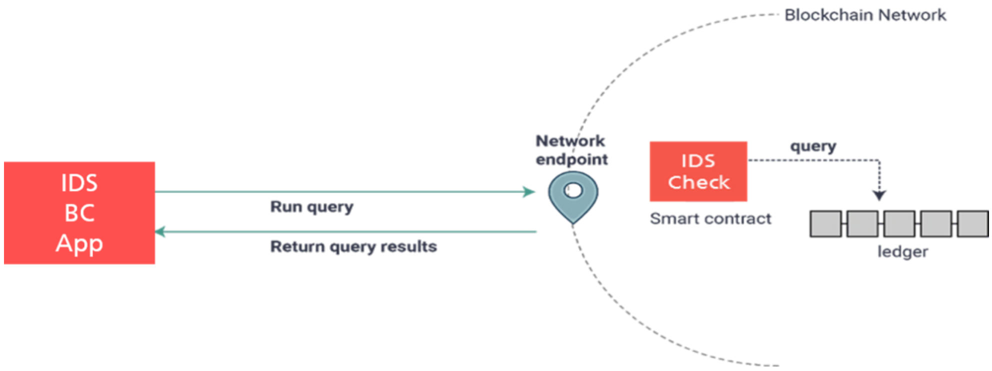

Figure 18 - Check Blockchain for send transaction[14]

If the requested log entry is present, the blockchain app updates the general ledger with a "data received" entry and returns the successful update information to the connector core.

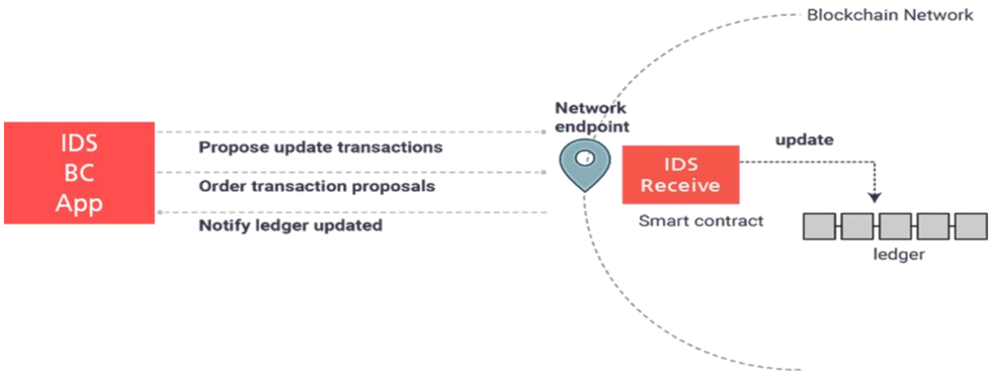

Figure 19 - Blockchain ledger update on receiving side[14]

After receiving the update confirmation from the blockchain app, the connector core forwards the received data to the receive app for further processing.

5.3 Deployment and hosting infrastructure

One of the means for the achievement of QU4LITY project's objectives is the availability of a suitable ICT infrastructure that may support all the pilot sites in their experimentation. For what DLT in concerned, as already mentioned in previous parts of this document, we have chosen to have one single physical infrastructure in place, playing all the roles defined in the QU4LITY reference architecture ("value chain ledger" and "private ledgers"). This approach will radically simplify the integration of pilot applications with the blockchain, given that specific technical skills are required and may not be available in every context. In other words, for the sake of the QU4LITY experimentations, we are going to centralize an otherwise decentralized system, running all the nodes on a common Cloud infrastructure, operated by one technical partner with the required expertise. While this obviously negates the very rationale for DLT to exist – giving each participant enforcing power on all the others, thanks to the – it is perfectly acceptable in a project that doesn't aim at demonstrating the basic functionalities of blockchain platforms, but rather at exploring their potential (and limitations) in real-world quality management business cases.

The key enabler of this strategy is the capability of the DLT platform of choice, Hyperledger Fabric (see section 4.3), of providing all "tenants" (i.e., the individual use cases) with their private "logical" distributed ledger, better described as *channel*. In this way, a single physical HLF instance can be used in any of the following modes, also combining them according to needs – thanks to the possibility of one peer node to belong to more than one channel at the same time:

- One peer node per organization
- Multiple peer nodes belong to the same organization
- One channel reserved for one organization which operates multiple peer nodes
- One channel shared by multiple organizations, each operating one or more peer nodes

The HLF software packaging is of help here, as peer nodes come virtualized as Docker images[15], which can be deployed on any computing device that can run a Docker container. This not only makes the creation of a multi-node, Cloud-based instance very easy, but also means that any configuration created on the Cloud may be quickly migrated to a "real" distributed environment if required.

The deployment plan for the QU4LITY DLT Infrastructure is to create a baseline system with one Certificate Authority (CA) and Membership Service Provider (MSP) and one Ordering Service; the CA and the MSP will also be operated by the same technical partner that hosts the DLT Infrastructure. Peer nodes will then be provisioned and channels configured on demand, following the analysis of use cases and the roadmap of their implementation. Given the experience made in the FAR-EDGE project, where a similar approach was adopted, although on a smaller scale (on two pilot sites), in QU4LITY we expect to be creating eight peer nodes at most; however, any number of nodes can be supported, given the flexibility of the hosting Cloud infrastructure.

All the nodes and services will be reachable from the public Internet using gRPC[16], which is a secure communication protocol specifically targeted at low-overhead remote procedure calls. As gRPC is fairly low-level and client integration is not a trivial task, developers of client applications will be provided with a software development kit (SDK) that abstracts away much of the complexities. Such SDK will be available for Java and NodeJS only, thus limiting the options for client developers to these two languages. Moreover, client software will need to embed a digital identity released by the CA in order to be allowed to join the system, meaning that every client will need to be registered with the MSP and given the appropriate access rights.

[15] See https://www.docker.com/
[16] See https://grpc.io/

6 QU4LITY DLT Services

Preliminary analysis of smart contracts for quality management (to be detailed in D3.12). Basically, each consists of a data model and some business logic exposing a service interface for a data-sharing task. The purpose may be generic (task defined in QU4LITY but generic enough to be part of any quality-focused process) or solution-specific (designed as part of a pilot solution). In FAR-EDGE we had both types, while in QU4LITY we aim at the former.

The QU4LITY blockchain infrastructure will provide a range of services that will enable the implementation of autonomous, intelligent and decentralized quality management use cases. In principle, each service will be implemented as a Decentralized Application (DApps) over the selected permissioned blockchain infrastructure (e.g. a Hyper Ledger Fabric (HLF) chaincode program in the case of Hyperledger Fabric). The QU4LITY DApps / chaincode will always support well-defined, application-specific processes as required by the QU4LITY blockchain based use cases. However, a set of reusable "framework" DLT services are specified and implemented in order to accelerate the process of developing Chaincode and to improve the cost-effectiveness of the DApps development. Such services are prescribed in the following paragraphs. Furthermore, following paragraphs illustrate the common properties/characteristics of the DLT services of the project.

6.1 Common Properties of QU4LITY Ledger Services and DApps

6.1.1 Data model

The QU4LITY DLT will automatically keep track of the global state distributed ledger, which will log every state change and will propagate this change across all peer nodes of the blockchain. However, the data based on any Ledger Service or DApps will be initialized according to a specific data model, which will be maintained across the entire lifecycle of the service. Hence, every Ledger Service will be associated with a specific data model (as defined in T2.5 and T3.7) that will be specified in a popular format like JSON, CSV or XML. For instance, in a smart diagnostics context it's not so trivial to handle different sensor measurements coming from several machineries, it's impossible when coming under different data models. For this reason, a unified data model will be defined in QU4LITY to assure that every measurement coming from the field can be processed by analytics components with ease.

6.1.2 Business Logic

Each DApp or Ledger service will have some business/application logic, which will be coded in the various nodes based on appropriate endpoints. The latter will be called by the various peer based on appropriate APIs. The latter APIs will enable peers to access and update the global state of the Ledger Service at hand. Due to the use of a permissioned blockchain, these APIs will be usable by authenticated and authorized peers/parties only. In order to access this API, an appropriate library could be abstracted and implemented (i.e. a Ledger Client application).

6.1.3 Access and/or usage policies

Each ledger service should implement some policy for access and usage control. In all cases, invoking a ledger service requires that clients are authenticated based on basic access level control, which verifies the digital identify of the client and is provided by the DLT/blockchain infrastructure. However, it is also possible to implement more fine-grained access control, such as regulating access to specific end points. This should be managed as part of the code of the Ledger Service or DApps, by means of interacting with some external security-related component such as a Policy Decision Point (PDP)

6.2 Orchestration Services

Orchestration Services are DLT services that create digital manufacturing automation workflows as DApps. They are used to orchestrate distributed processes in order for example to trace and validate the quality of a production process end-to-end (i.e. across all of its steps).

6.3 Data Publishing Services

Data Publishing Services support the creation and execution of distributed data analytics pipelines. They will enable the validation of the integrity and the consistency of the data, as well as of the data analytics algorithms applied over them. As such they will boost the reliability of the datasets and of the analytics algorithms, despite the inherent inaccuracy and inconsistency of distributed industrial data.

6.4 Configuration Services

The QU4LITY DLT should also provide configuration services as a means of configuring the deployment configurations of DLT system as a whole i.e. giving dynamicity to the overall system. In particular, the configuration services will enable the registration of the various industrial devices and CPS systems in the distributed ledger, along with mechanisms for validating the integrity of the deployment configuration and for ensuring its consistency. Hence, the configuration services will support the registration, de-registration and discovery of devices, analytics algorithms and other artifacts of the deployment configuration of a quality management application.

7 Conclusion

This deliverable describes the first results of the tasks T3.6 providing the high-level overview of QU4LITY Permissioned Blockchain platform and outlining a preliminary specification (to be further refined in D3.12). These results have been driven by earlier work and results from WP2, notably the analysis of requirements, Reference Architecture and relevant business scenario.

Overall, this document provides a sound basis for development and integration activities that will be performed in the on-going Task 3.6. In particular, T3.6 defines the main components and structuring principles of DLT usage in QU4LITY, thus identifying the baseline platform to satisfy QU4LITY DLT Infrastructure key requirements.

The QU4LITY blockchain infrastructure will enable secure state sharing and synchronization of distributed industrial processes involved in AQ/ZDM implementation and will support the traceability of the data, improving the way this information is shared across the different stakeholders involved in the process. Moreover, assets traceability will be able to address counterfeiting and pose the basis to make environmentally sustainable practices a reality for the corporations.

The results of analysis conducted in QU4LITY will also bring new insights to IDSA developments, stimulating new discussions and publications on blockchain technology usage in data-driven business ecosystems.

The future work inside the Task 3.6 will be the prototyping and the implementation of "generic" smart contracts that will expose generic or specific business logic by the means of Decentralized Application. Furthermore, smart contracts will improve agreements management between manufacturers, customers and other stakeholders solving of the many challenges faced in today's complex supply chains. The infrastructure to be developed in Task 3.6 will be validated in the project's pilots and/or in the applications that will be developed in the scope of the open calls of the project. In this respect, Section 4 of this deliverable provides information that could be used to share the scope and content of the QU4LITY open calls for proposals.

References

[Andrews17] Andrews, Colin, et al. "Utilising financial blockchain technologies in advanced manufacturing." (2017).

[Kim18] Kim, Henry M., and Marek Laskowski. "Toward an ontology-driven blockchain design for supply-chain provenance." Intelligent Systems in Accounting, Finance and Management 25.1 (2018): 18-27.

[Li18] Li, Zhi, et al. "Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing." Industrial Management & Data Systems 118.1 (2018): 303-320.

[Ott19] B. Otto et al, "IDS REFERENCE ARCHITECTURE MODEL - INDUSTRIAL DATA SPACE, version 3.0" 2019. [Online]. Available: https://www.internationaldataspaces.org/en/ressource-hub/publications-ids

[Uriarte18] Uriarte, Rafael Brundo, Rocco De Nicola, and Kyriakos Kritikos. "Towards distributed SLA management with smart contracts and blockchain." 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2018.

[Wang17] Wang, Jun, et al. "The outlook of blockchain technology for construction engineering management." Frontiers of engineering management (2017): 67-75.

[Zhang19] Zhang, Yongping, et al. "Blockchain-based trust mechanism for iot-based smart manufacturing system." IEEE Transactions on Computational Social Systems (2019).

List of figures

List of tables

List of Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
AQ	Autonomous Quality
AS2	Applicability Statement 2
BC	Blockchain
B2B	Business to Business
CA	Certificate Authority
CLM	Closed Loop Manufacturing
DApp	Decentralized Application
DLT	Distributed Ledger Technology
DSC	Digital Supply Chain
DSS	Decision Support System
EDI	Electronic Data Interchange
ERP	Enterprise Resource Planning
ETL	Extract, Transform, Load
GDPR	General Data Protection Regulation
HPC	High Performance Computing
HLF	Hyperledger Fabric
ICT	Information and Communication Technologies
IDS	International Data Space
IDSA	International Data Space Association
IoT	Internet of Things
LTS	Labelled Transition System
MSP	Membership Service Provider
M2M	Machine to Machine
OLTP	OnLine Transaction Processing
PDP	Policy Decision Point
PoS	Proof of Stake
PoW	Proof of Work
P2P	Peer to Peer
RA	Reference Architecture
sFTP	Secure File Transfer Protocol
STF	State Transition Function
TTP	Trusted Third Party
VAN	Value Added Network
VP	Validation Peer
WP	Work-package
ZDM	Zero Defect Manufacturing

Partners: