Horizon 2020 – The EU Framework Programme for Research and Innovation
Project Co-funded by the European Commission
Contract number: 761145
Call identifier: NMBP-22-2017
Project Start Date: 1st January 2018

MANUSQUARE

MANUfacturing ecoSystem of QUAlified Resources Exchange

# D3.2
# Security and privacy services

| | |
|---|---|
| Dissemination Level | Public |
| Partners | IBM |
| Authors | IBM |
| Planned date of delivery | 30/06/2019 |
| Date of issue | 30/06/2019 |
| Document version | V1.0 |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 761145

**DISCLAIMER:**
The herewith information reflects only the author's view. The European Commission is not responsible for any use that may be made of the information herewith included.

## DOCUMENT HISTORY

| Version | Issue date | Content and changes | Author |
|---|---|---|---|
| 0.1 | 02/06/19 | Initial full version for internal review | IBM |
| 0.2 | 04/06/19 | Incorporate review comments from Henrique Diogo Silva (INESC) | IBM |
| 0.3 | 04/06/19 | Incorporate internal review comments from Fabiana (IBM) | IBM |
| 0.4 | 11/06/19 | Incorporate review comments from Giuseppe Landolfi (SUPSI) | IBM |
| 0.5 | 26/06/19 | Incorporate review comments from Andrae Barni (SPSI) | IBM |
| 1.0 | 30/06/19 | Finalize | IBM |

| Role | Partner | Person |
|---|---|---|
| Reviewer 1 | SUPSI | Andrea Barni, Giuseppe Landolfi |
| Reviewer 2 | INESC | Henrique Diogo Silva, Antonio Soares |
| Quality assurance | SUPSI | Andrea Bettoni |

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

## LIST OF ABBREVIATIONS

**Table 1: List of Abbreviations**

| Acronym | Description |
|---|---|
| CA | Certificate Authority |
| DB | Database |
| IIoT/<br>Industrie 4.0 | Industrial Internet of Things |
| IoT | Internet of Things |
| MANU-SQUARE | MANUfacturing ecoSystem of QUAlified Resource Exchange |
| REST | Representational State Transfer |
| RFI | Request for Information |
| RFID | Radio Frequency Identification |
| RFQ | Request for Quotation |
| SDK | Software Development Kit |
| SME | Small and Medium Enterprises |
| VM | Virtual Machine |
| WP | Work Package |

## GLOSSARY

**Table 2 List of Terms**

| Term | Meaning |
|---|---|
| *Certificate Authority* | An entity that issues digital certificates to be used for authentication of the communicating party holding the certificate. |

| | |
|---|---|
| *Chaincode* | The implementation of a smart contract within Hyperledger Fabric. A programmatic manner which governs the interaction between a blockchain client and the blockchain network itself. |
| *Endorsing peer* | A member of the blockchain network that may be called to endorse transactions for a particular chaincode. The process of endorsing a transaction includes a speculative execution of the chaincode function included in the transaction proposal responding to the caller with the read and write sets (including versions) corresponding to the chaincode execution. In addition it indicates whether it supports the transaction. |
| *MVCC* | A multi-version concurrency control employed by Hyperledger Fabric to enable speculative concurrent execution of transactions without corrupting the underlying data storage. |
| *Ordering service* | A Fabric entity that provides total order among incoming transactions and their inclusion into blocks. |
| *Peer* | A central entity in the Fabric network which is in charge of validating incoming blocks (and associated transactions) and committing the blocks to its own copy of the shared ledger. |
| *REST* | A common manner of interaction among different processes. (https://en.wikipedia.org/wiki/Representational_state_transfer) |
| *RFID* | Radio-frequency identification (RFID) is mainly used to automatically identify and track tags attached to objects. |

# 1 Executive summary

The main goal of this document is to present the establishment of trust in an otherwise trustless business environment through blockchain based selective visibility mechanisms, to be used within MANU-SQUARE for supply chain scenarios support. The document starts from a short description of the technology and its specific use, and continues further to introduce selective visibility possibilities and their use within the framework of a Request for Quotation (RFQ) support system.

Please note that in this document we mainly refer to the permissioned flavor of a blockchain which is more suitable for business scenarios. We mainly focus on the Hyperledger Fabric implementation (https://www.hyperledger.org/projects/fabric).

This document should be perceived as a continuation of D3.1 (Connecting IoT devices to blockchain services); in order for it to be self-contained, a concise summary of major over-arching parts of D3.1 are presented in the first section.

One of the main aspects and advantages of a blockchain network lie in the security and privacy guarantees it provides. The different privacy preserving mechanisms discussed within our blockchain network are:

1. Full visibility to all channel participants. A channel corresponds to a ledger; thus all transactions shall be visible to all participants.
2. Application based filtering. Traditional blockchain applications contain the network layer (servers used for running the blockchain itself), smart contracts which run within the context of a channel, and a higher layer application which interacts with the business logic owners. In this variation the filtering of information is performed at the application level.
3. Private data collections – enables participants in the same channel to keep a part of the data confidential to a set of channel participants, while still being able to maintain the integrity of the shared ledger for all participants.
4. Multiple channels – complete separation between members of different channels. Each such channel maintains its own ledger among its participants

As a report of the activities carried out within T3.2, this document emphasizes the different privacy preserving mechanisms in general and their intended use within a specific MANUSQUARE capability, namely RFQ processing.

Following activities will further enhance and demonstrate the support for additional MANU-SQUARE capabilities, such as reputation management and ideas management.

The description of the work is organized in the following sections:

- Section 2 briefly introduces blockchain, specifically within a supply chain environment.
- Section 3 dives into the foreseen uses of Blockchain within MANU-SQUARE
- Section 4 provides more details as to the different privacy preserving mechanisms
- Section 5, puts the mechanisms introduced in section 4 in the context of RFQ processing support.
- Finally, section 6 provides conclusions and next steps.

# 2 Introduction

## 2.1 MANU-SQUARE in a nutshell (with a blockchain angle)

The MANU-SQUARE project aims at fostering an ecosystem that acts as a virtual marketplace in which surplus of industrial resources can easily meet corresponding shortage, thus bringing the available capacity (such as production capacity), as well as other virtual and physical assets, closer to the demand to obtain the optimal match (See Figure 1). This scheme has two main advantages:

- The rapid and efficient creation of local distributed value networks for innovative providers of product services;
- The reintroduction and optimization in the loop of unused capacity and potential that would otherwise be lost.

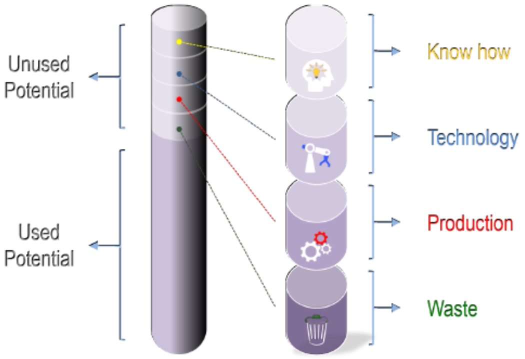

Figure 1: Composition of the unused potential

MANU-SQUARE establishes an ecosystem that is organized to match the needs of buyers with the availability of sellers in terms of know-how, technology, manufacturing capacity, and waste (or bi-product). The blockchain technology introduced in this deliverable provides trust, transparency, and security to the MANU-SQUARE platform, thereby serving as a single source of truth and distributed trust in an otherwise trustless environment amongst the different stakeholders of the platform.

Please note that in this documents we mainly refer to the permissioned flavor of a blockchain which is more suitable for business scenarios. We mainly focus on the Hyperledger Fabric implementation (https://www.hyperledger.org/projects/fabric). A permissioned network ensures that members agree to enter a joint network, and can control the identity of other entities in the network. This stands in contrast to public networks (such as bitcoin) in which anyone can join in any role, and the identities of participants is concealed.

Transactions through the platform are recorded in a final and immutable manner by the blockchain layer, providing all network members with an identical and trustworthy real-time view of the process.

The main objectives of the project are to match shortage with surplus on a wide spectrum of areas. The main reason for integration blockchain technology at the basis of the platform is to provide security, privacy, and trust in the process. In a multi-sided platform, such as MANU-SQUARE aspires to be, there are many entities with different kinds of relationships between them. That leads to different levels of privacy and data visibility requirements that should be supported by the platform, depending on the entities involved and the current interaction between these entities. As there are various modes of interaction between entities, there are various visibility scopes, to adhere to the required level of privacy and isolation. There's a wide spectrum of modes being made available, starting from full visibility of all information to all members of the network, through different levels of visibility separation either governed by an application, or by the creation of separate channels for specific interactions, through the establishment of private data collections which ensure that information is made available only to the intended entities even within the same channel.

T3.2, which is summarized in this deliverable, enhances the base blockchain platform for supply chain established in T3.1 with the construction and use of additional layers on top of the base platform. This layer provides different security and privacy constructs to enable differential views of data residing in the blockchain based on certificates and capabilities agreed upon between different members of the blockchain network.

### 2.1.1 Blockchain – in a nutshell

A blockchain revolves around the concept of a shared ledger, representing the system of record and a single source of truth for business interactions. The shared ledger is maintained by a cluster of peer processes, providing an append only transactions log, while guaranteeing the immutability of inserted and validated transactions. It enables a network of business partners to perform transactions across organizations without resorting to a single unified trusted authority. A blockchain transaction represents a state change or asset transfer in the ledger; transactions are governed by smart contracts, which contain the rules for transactions to be invoked and the agreed upon resulting behaviour. Blockchain provides a shared, replicated, permissioned ledger ensuring trust, provenance, immutability and finality, to replace inefficient, expensive, and vulnerable processes.

These measures together provide a level of trust among partners which is difficult to achieve otherwise in an inherently trust-less environment. Most importantly, the trust is not due to a single actor within the network, but rather it is an outcome of the collective nature and properties of the underlying technology.

As can be seen in Figure 2 the shared ledger provides a real-time shared and replicated view of the state of the transactions among all members of a blockchain network. This reality stands in contrast to the pre-blockchain era in which each organization held its own ledger, opening the door to inconsistencies and disputes.

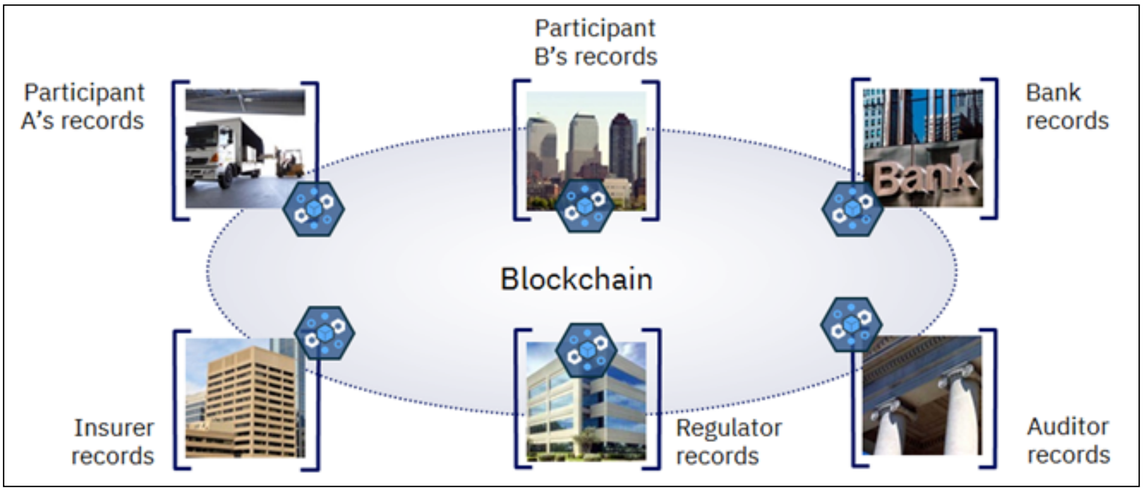

**Figure 2: Blockchain's core - the shared ledger**

The four cornerstones comprising the blockchain structure are a shared ledger, transaction verification by network members, smart contacts, and security & privacy measures. The last one shall be at the centre of this deliverable. All these building blocks combined together provide assurance for consensus, provenance, immutability, and finality.

Privacy and security measures supported ensure appropriate visibility and authentication, such that only authorized parties are exposed and have access to certain blockchain activities. There are various levels of privacy supported, governed by the agreements among partners in the network. These vary from having all transactions and associated data exchange visible to all members of the network (and to no one outside the network), through the exposure that there are transactions among partners without all associated data to be revealed, to the complete isolation of a business relationship such that only the involved partners can deduce that such a relationship exists. Cryptography is central to these processes.

The concept of channels was introduced  to Hyperledger Fabric to enable complete separation between entities that do not want to share any data or evidence of interaction. A channel can be seen as a different instance of a blockchain network, in which some of the underlying infrastructure can be shared. For example, there can be an ordering service which is responsible for several channels. A channel is associated with a ledger.

At a high level, the system is comprised of peers, which replicate and validate the blocks comprising the ledger; an ordering service which determines and publishes the order of the transactions, and a client that interacts with the system for invoking transactions or queries. A sub-set of the peers is involved also in endorsing transactions submitted to the system; supporting consensus for inserted transactions.

Blockchain technology usage is relatively new but interest in it is growing in many fields. The first such field is the financial services arena, but more areas are exploring the usage of this technology, supply chain being in the forefront. In various analysis reports it can be seen that Banking / Financial Services and Supply Chain remain top industries for blockchain activity[1]). A lot of attention and funds are being devoted to exploring blockchain contribution to supply chain scenarios[2], both by industrial partners, as well as large IT providers, such as IBM, Oracle, and Microsoft.

[1] https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf

[2] https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution
https://www.coindesk.com/pwc-australia-port-of-brisbane-unveil-blockchain-supply-chain-pilot
https://www.zdnet.com/article/alibaba-pilots-blockchain-supply-chain-initiative-down-under/

### 2.1.2 Blockchain for supply chain

Blockchain solutions are prominent in business relationships which require data to be shared between different entities, mostly in real-time or close to it. Companies involved do not , however, necessarily have trust in each other. Such relationships are prevalent in supply chain networks. The use of a blockchain based infrastructure enables parties which are a part of a supply chain relationship to leverage the technology to gain tangible benefits in important areas such as reduction in time, money, and risk. The blockchain serves as the single source of truth, which is shared among all participants, and is not controlled by a single entity.

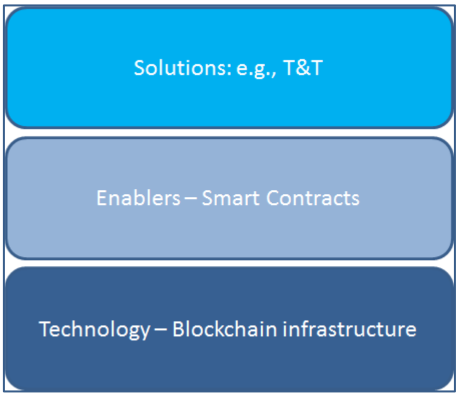
Solutions: e.g., T&T
Enablers – Smart Contracts
Technology – Blockchain infrastructure

**Figure 3: Technology Layers**

In Figure 3, a high-level view of the technology layers involved is depicted.

At the bottom resides the blockchain infrastructure itself, which consists for example of consensus mechanism, cryptographic validation, mechanisms for replication of blocks, and certificate authorities (CA). At the middle layer reside the enablers which enable developers to insert specific logic which shall be tightly coupled to a specific deployment of a blockchain. This layer will encompass the specific rules governing the interactions supported for a specific network of participants. This layer is mostly associated with and implemented by Smart Contracts. At the higher layer resides the solution or application, which is a mean to interact with the end-users, or digital processes and devices on their behalf, on the one hand, and with the blockchain infrastructure on the other hand.

As a part of the vision to incorporate a blockchain based supply chain platform, the first step is to incorporate partners data, putting a specific emphasis on IoT data. The data serves as the driving element to the agreed upon logic which resides in the blockchain level as well in the form of smart contracts. Examples as to the kind of data which shall participate includes RFQ related (such as negotiations process, tenders processes), and data coming from sensors which enables tracing the state of items in real-time to drive potential notification on out-of-bounds conditions affecting agreements.

This capability enables a coherent and updated view of the status of the supply chain ecosystem including availability of production resources, flow of materials and components, and the associated state as can be reported by attached IoT devices; all according to the scope, rules, and conditions agreed upon among the network partners. The mechanisms for setting up and ensuring proper visibility of data and interaction shall be elaborated in the rest of the current document.

All in all, a blockchain infrastructure can be used to reduce the rate of disputes and errors in logistics and to enable real-time tracking of transactions in the supply chain providing elevated accuracy, security and speed; while ensuring that data and interactions are not made visible to unauthorized partners.

## 2.2 Advantage of Blockchain based scenarios in the area of supply chain

In general, several benefits can be obtained by applying blockchain based scenarios in the area of supply chain.

- Enhance trust in a trustless environment – providing end-to-end provenance. Blockchain based supply chain relationships will become a validated, trusted, self-executing process, supporting non-repudiation
- Tie in fragmented and siloed systems: A shared ledger, can remedy this situation by providing a unified view to all participants at the same time. That provides a clear picture for making decisions to all involved entities.
- Minimize disputes – Having a single source of truth, verifiable and auditable can lead to a reduced number of disputes, and a shorter time to resolution of disputes.
- Data integration, including IoT, can lead to greater transparency and better, more efficient, collaboration by taking actions programmatically and automatically based on incoming data. Provide the capability to track, monitor, and report the location and status, of shipments, goods, or supplies with the integration of IoT devices
- Automating contracts and processes - Terms of a contractual agreement between parties can be manifested as a smart contract running in the blockchain.
- Differential visibility and data privacy ensure that the information is shared only among the intended partners.

# 3 Blockchain use in the MANU-SQUARE project

## 3.1 Blockchain roles in the overall platform architecture

The blockchain platform plays a role both in the underlying data layer as well as in the tools layer. It is located at the lower infrastructure layer of the platform, exposing interfaces to services that the different higher level components of the platform can use. At the data layer it does serve as a unique kind of data store in the form of a shared ledger exhibiting the capabilities detailed in sub-section 2.1.2. At the same time, it does play a role at the tools layer as well, since a part of the logic does reside in the blockchain internals in the form of a smart contract[3] which is a programmatic manner to declare and enforce the rules that govern specific interactions via the blockchain. Thus, different platform components shall use interfaces exposed by the blockchain component in order to take advantage of the capabilities and promises of a shared ledger. The blockchain component shall expose a REST interface to other platform components. There shall be two main kinds of activities supported by the interface:

1. Invoke smart contact transactions – intended for MANU-SQUARE modules to be able to invoke transactions residing in smart contracts. These interactions are made to change the state of an entity and record that for posterity. For example, while supporting an RFQ process transactions can be invoked for publishing a new RFQ or providing a response to an RFQ.
2. Query - expose query capabilities to retrieve data which was previously stored at the blockchain. For example, while supporting an RFQ process such queries can be used for retrieving information on the complete journey so far of an RFQ (publisher, offers, negotiations, acceptance / rejection).

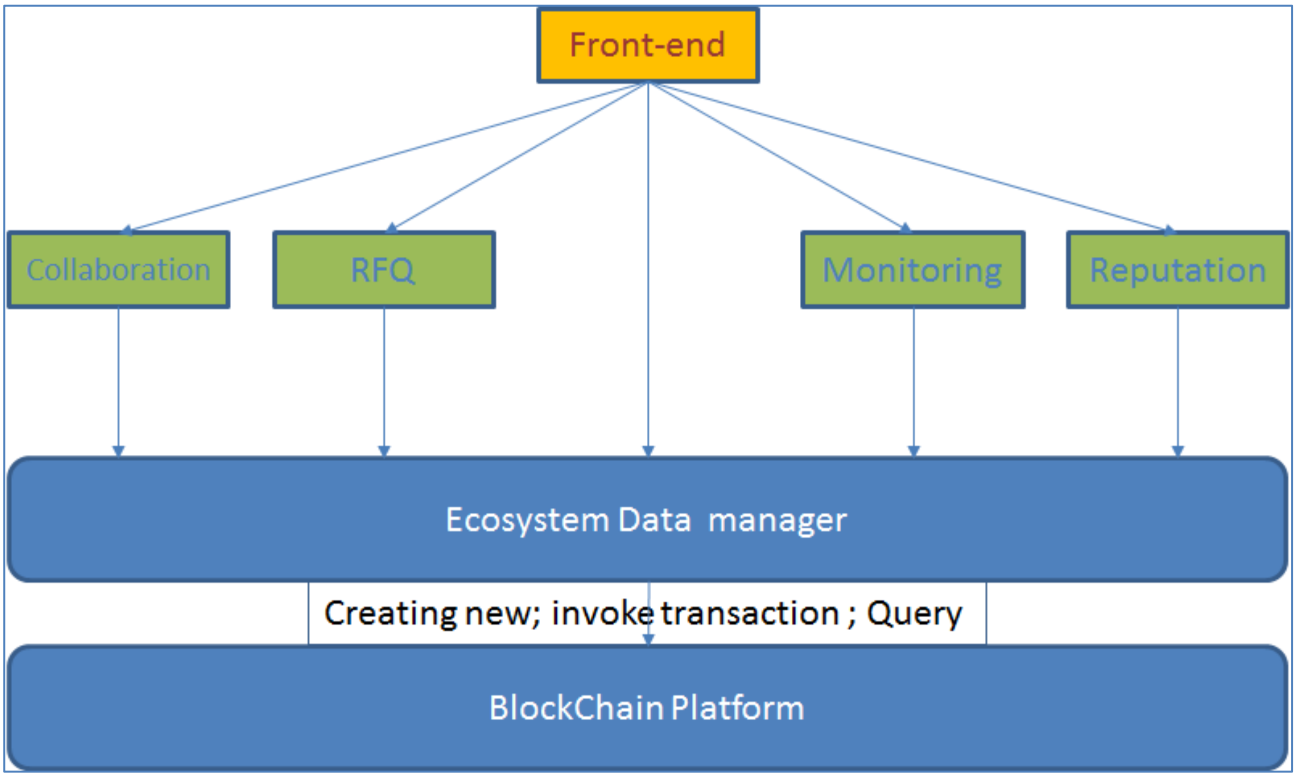

Figure 4: Components interactions

In Figure 4 a broad sketch of the integration of Blockchain within MANU-SQUARE is depicted. In the diagram we can see the blockchain network, depicted on the right hand side by a collection of ordering service and peers belonging to several

[3] In Hyperledger Fabric smart contracts and implemented in the form of chaincode (https://hyperledger-fabric.readthedocs.io/en/release-1.4/chaincode.html)

organisations. Communicating directly with them is an application, which wraps internally a NodeSDK client that is in charge of the direct communication with the blockchain.

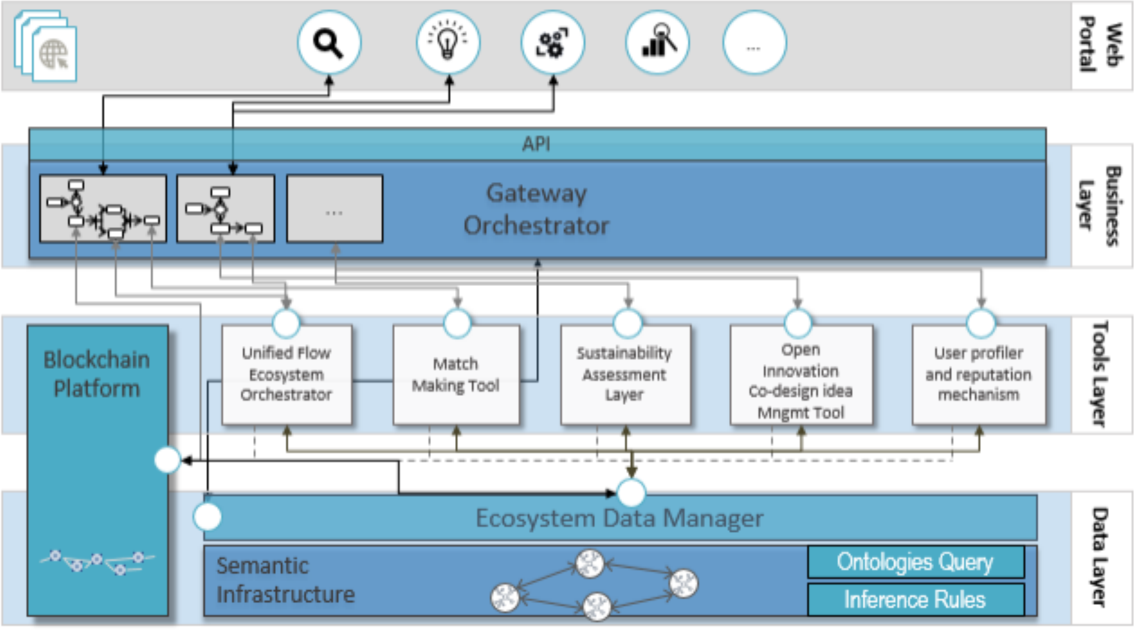

Figure 5: MANU-SQUARE high level architecture

Figure 5 provides a higher level view of the location of the Blockchain component within the platform, and the foreseen interactions with additional components and tools.

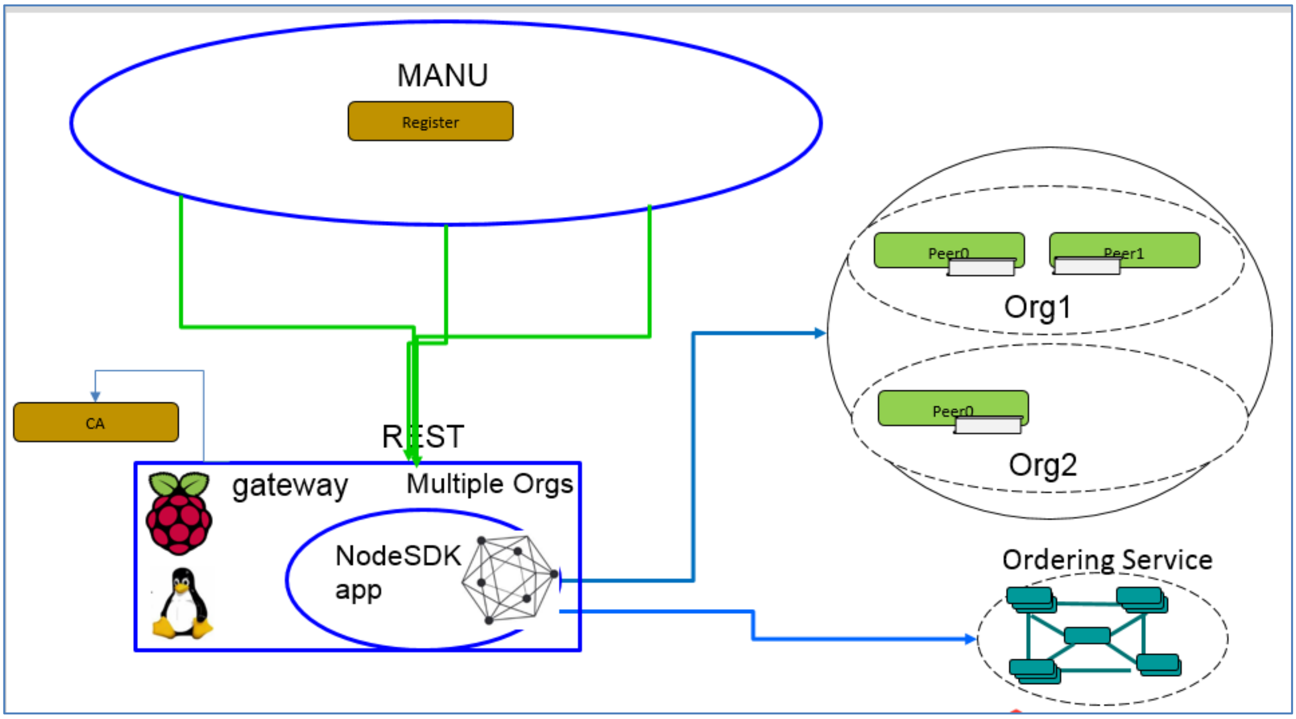

Figure 6: Embodiment within MANU-SQUARE

Such an application exposes a REST interface to the rest of the MANU-SQUARE platform, and acts as gateway connecting between MANU-SQUARE on the one hand and the blockchain infrastructure on the other hand. The application communicates as well with a certificate authority (CA) in order to resolve the cryptographic material and identification of entities.

## 3.2 Capabilities supported in the MANU-SQUARE platform

This section is intended to dive deeper into the definition of the specific use cases foreseen to apply blockchain technology within the MANU-SQUARE project. Taking as a starting point the DoA and the evolution of the project use cases as the project advances as main result of WP1, the Blockchain integration shall focus on three representative scenarios, namely RFQ management, reputation management, and traceability of innovative ideas.

At a high level, the use cases can be divided into two broad categories. First, matching between surplus and need (for example of production capacity or by-products) to support capacity sharing. Second, innovation management of collaborative design. For both categories the MANU-SQUARE platform shall take advantage of a blockchain based infrastructure as the providers of a trusted (in a trust-less environment) single source of truth.

The functionalities that a blockchain infrastructure can support in supply chain scenarios will be translated into plans for specific use cases to be deployed in the MANU-SQUARE platform. Hereinafter, a short description of each use case is provided.

### 3.2.1 RFQ management

RFQ is a structured and often complicated process which may involve multiple hops and interactions between the entities involved (from the initial offer through a negotiation process, culminating in a signed deal). The blockchain will help structure the process and safeguard all the interactions and advancements of the process throughout its lifecycle. This capability shall help to centralize the process and related communication, to overcome current scattered RFQ related documentation.

The process is initiated by a prospective customer and is targeted towards a potential supplier, and may consist of various items to be agreed upon (such as price and time). Several rounds of negotiation may be required for the positive (or negative) finalization of the process. All information exchanged digitally shall be part of a permanent record kept and made available by the blockchain.

In supporting such a process there needs to be awareness as to the data that is distributed on the blockchain platform and the visibility scope associated with that data. Different stages of the process require the visibility to a different subset of stakeholders. This requirement poses challenges to the underlying blockchain infrastructure. In a nutshell, an RFQ process with a prospective customer publishing the initial RFQ. The visibility associated with that should be wide, thus all members of a network shall be able to receive that information. On the contrary, when responding to an RFQ, normally the entity in question wants that information to be shared only with the RFQ publisher. Such differential visibility and privacy constraints shall be addressed in section 4.

### 3.2.2 Reputation management

Reputation management is of crucial importance to the adoption of the platform. Thus, the trust that can be associated with this component is of great importance as well. The blockchain infrastructure shall support the traceability of the entire history related to the reputation of all involved entities at different points in time. As the platform is intended mostly to establish relationship among entities that have no prior engagement between them, the reputation management capability plays an important role. Without the MANU-SQUARE platform, companies often go through much pain over a prolonged amount of time before embarking on a business interaction with a new partner. The intention in this case is that with the added trust that can be associated to this component, companies will rely on reputation scores provided by the platform to make more informed and faster decisions for establishing new relationships.

### 3.2.3 Traceability of innovative ideas

In this use case Blockchain can be applied to the tracking of contribution of innovative ideas within the MANU-SQUARE ecosystem. Considering that the platform is intended to support the evolution of ideas form basic concepts to fully set-up projects in a cooperative and open manner, BlockChain should be involved to keep track of the contributions of each participant and register the ownership of every single contribution. This capability should support the ability to reward respectively the participants of ideas creation at a later stage in the product development.

One possibility is to have a blockchain based incentives program in place rewarding participants for contributing ideas and information to the project. Incentives can take many shapes and could encourage people to participate in the research effort.

### 3.2.4 Tracking and Tracing

Efficient and reliable tracking and tracing solutions bring clarity to the relationship among all partners in a supply chain scenario. Transactions on the blockchain create a traceable permanent history of the product or interaction, throughout their lifecycle, which is shared by all members of a collaboration.

With the help of technology that can easily and cheaply provide product identification (such as QR codes) the individual products can be traced throughout their lifetime; including change of ownership or inclusion into larger shipments. This capability enables the platform to keep track of the state of a product and play back the entire history of the specific product from the moment it was introduced into the blockchain until the present day.

This capability may follow directly a successful RFQ process. Some of the clauses in the RFQ may guide the items that will be tracked and traced, and potentially the conditions for their handling. The result may be a smart contract that is deployed on the blockchain network and keeps track for example of the location(via GPS) and environmental conditions (temperature, humidity), and alerts parties when agreed upon conditions are breached.

A prominent example of the potential seen in such use cases can be seen in an endeavour with the participation of IBM called, TradeLens[4], with the goal of digitizing the global supply chain using blockchain.

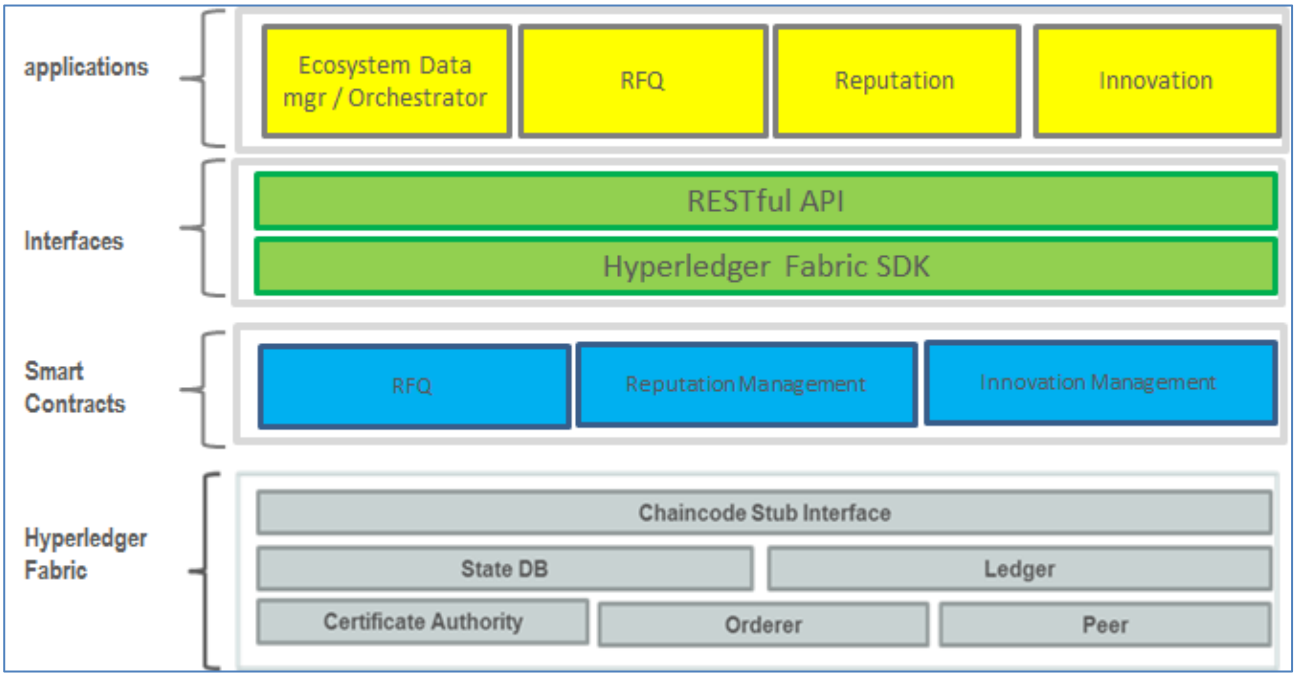

**Figure 7: Positioning within MANU-SQUARE**

## 3.3 Contextualising blockchain use in the capacity sharing scenario

Following a first version of the envisioned business process flow for a capacity sharing scenario[5]. The process in general calls for the following steps:

1. Customer to Invoke the match making capability of the platform to receive a ranked list of potential suppliers. A part of the ranking mechanism shall be supported by the reputation management component and its underlying blockchain platform.
2. Embark on an RFQ process between the customer and the prospective suppliers. In this stage, the customer publishes an RFQ, which is recorded on the blockchain and is made available to all prospective suppliers. Negotiation steps are made within a visibility constraint of the specific potential supplier and the customer. When the final decision is made, all participants are made aware of the end result (accepted or rejected).

[4] https://www.tradelens.com/

[5] A comprehensive explanation can be found in D1.3 (Business processes and early validation scenarios), and D5.1 (Platform services portfolio)

3. For the chosen supplier, start the project upon input material delivery. This step can be stored in the blockchain as well, with visibility limited only to the parties in question.
4. Periodic monitoring of the project status and a corresponding update of the project status and advancements. This step can be stored in the blockchain as well, with visibility limited only to the parties in question
5. Project closure – delivery of the goods This step can be stored in the blockchain as well, with visibility limited only to the parties in question
6. Update reputation management for both the customer and the supplier. This step is executed using the reputation manager component, storing the updated scores in the blockchain platform.

In the following section we can see the main corresponding interactions of the blockchain component with additional MANU-SQUARE platform components (for a visual reference please turn to Figure 7**Errore. L'origine riferimento non è stata trovata.**). For all such interactions there are two broad categories of actions that are taken and supported by a REST interface exposed by the blockchain platform, namely invoking a transaction on the blockchain, intended to record data, and querying the blockchain platform for data previously recorded (latest state or historical data). A possible third mode of interaction will be discussed and developed based upon need, in which the blockchain platform invokes callbacks on registered entities based on events in the blockchain activity.

1. RFQ management – the blockchain component shall provide the underlying mechanism for keeping track and advancing the RFQ process among the customer and the suppliers. Naturally, the blockchain shall keep track of the history of the interaction from beginning to end and can serve as the reference point for the agreed upon terms and the evolution of the process. An example tentative basis for this component is described later in section 5.
2. Reputation management – the reputation management process shall be handled by the MANU-SQUARE platform, for all involved entities, both suppliers and customers. This process is deemed an important one for attracting entities to use the platform, and for the long term sustainability of the platform. Having a blockchain based infrastructure to keep track of reputation management is essential for the trust associated with the entire platform by current and prospective customers to join and use the platform.
3. Innovation management – tracking the evolution of an idea through its cycles. Including potentially the way that get used by organizations in implementation processes.
4. Collaboration – As explained above the lifecycle of a capacity sharing MANU-SQUARE interaction goes through a set of states in which interaction is expected between parties in the platform (mostly a customer, a supplier, and the platform). At a high level, the blockchain can serve as the reference point which keeps track of the current location in the process view for each interaction, along with all the history that led to this point. The information shall be querriable for all allowed parties (such as the platform manager, supplier, and customer), via the platform front-end. Potentially an exposed programmatic interface shall be provided as well. This feature may include monitoring at the production site making use of IoT devices.

Similar capabilities and interactions are foreseen as well for the collaborative design and ideation management scenarios. The content and internal structure of tracked items shall differ, but at the core, similar blockchain related processes and interactions shall take place. Thus, for innovation management and ideas tracking the blockchain infrastructure shall provide a basis for the management of the entire process from a design need all the way to delivery of a product. Including along the way the contribution of each party to the final products.

# 4 SECURITY AND PRIVACY

Along with the transparency brought in by the blockchain it is important in enterprises scenarios to ensure selective visibility of collaborations and data. Data needs to be available to the designated participating partners and to no other entities (only to the intervenient partners of a determined process.) Visibility and full transparency should be limited to only the members who are entitled to have access to the data. Thus, the technology provided will ensure that differentiated visibility is supported at multiple levels. A first degree of visibility is expected in cases of full collaboration and exposure of data among members of a consortium who share a blockchain network and channel. A second level may allow companies to be aware that a business relationship exists between other partners without being exposed to the internal details and data associated to that relationship. Finally, a complete separation in which a company is not able to know that other companies are collaborating and exchanging business related information is described.

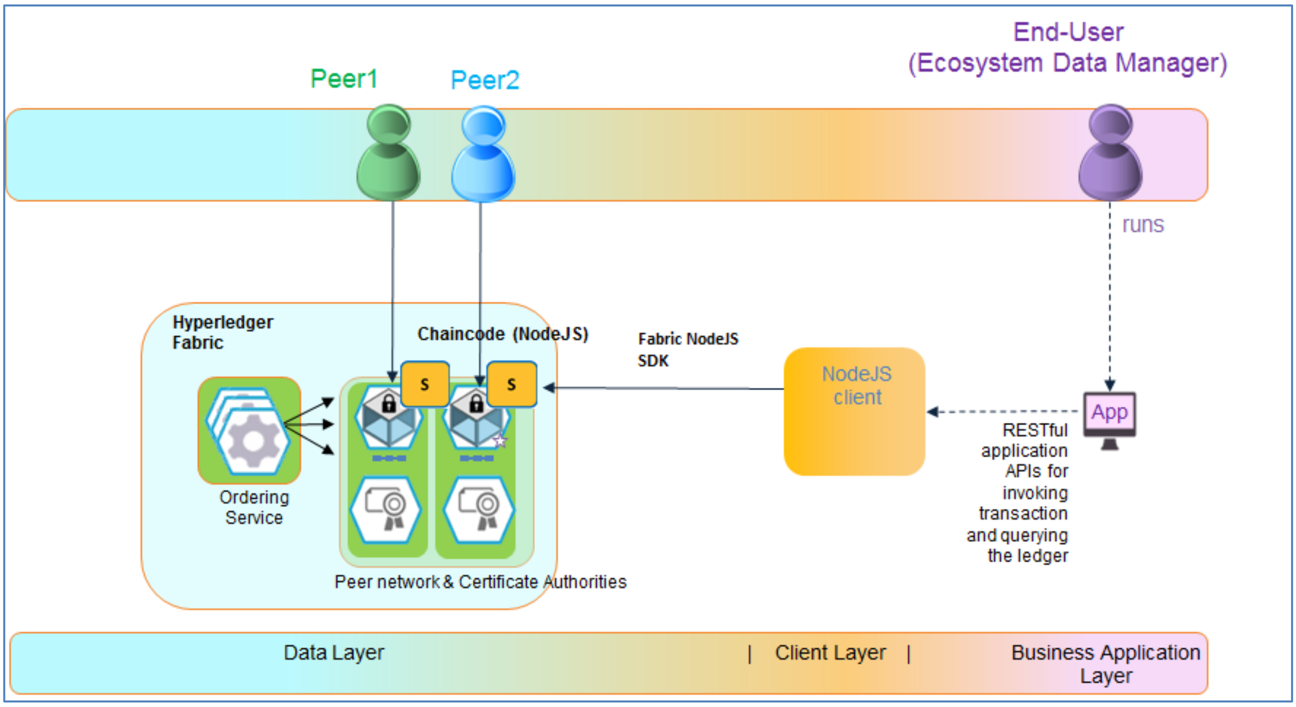

Figure 8: Blockchain ecosystem layers

The Blockchain system mostly consists of three layers as can be seen in Figure 8. First, a physical layer of deployment which includes the establishment of the network consisting of organizations, their participating servers (peers in Fabric), channels, cryptographic material, and more (depicted as the data layer in the figure above). A second component is the establishment and distribution of smart contracts (chaincode), which programmatically determine the rules and actions to be followed (referred to as the Client layer in Figure 8). These smart contracts control the state that is saved in the DB. On top of these lie the business layer which connects between the external world and the underlying blockchain infrastructure. In our development, as in most cases, this layer consists of the programmatic core of the interactions to follow, which exposes to the higher layers, a RESTful interface through which the interactions with the blockchain are mediated. On the other hand it includes a Blockchain client (such as the Fabric NodeSDK),which is in charge of interacting directly with the blockchain in the form of invocation of transactions, invocation of queries, and the establishment of call-backs. These call-backs enable an asynchronous mode of operation in which a process is notified by the blockchain network on the occurrence of events which were declared as being of interest to the application or higher layers.

Enclosed below is a brief summary of the different options that may be used for different visibility scopes within a Fabric Blockchain network, and specifically their use within the MANU-SQUARE platform.

## 4.1 Single channel

A single channel illustration can be seen in Figure 9. In the figure we see that all organizations are a part of the channel. Thus, all organizations have peers that replicate the specific channel ledger, or have access as clients to peers that have access to the channel in question.

A channel is characterized by being associated with a single shared ledger. A channel is used as a meeting point for members of different organizations to conduct business, which remain confidential outside the scope of the channel, and available only within the bounds of the participating organizations. Members of each participating organization may be able to connect to the ordering service in order to obtain from it the newly created blocks, containing the ordered set of transactions. The connected members make the blocks available to the rest of the member servers of their organization and network.

In the MANU-SQUARE context such a scheme can be used for example for collecting and making available reputation information, which is assumed to be accessible to all network members.

Smart contracts are defined within the scope of a channel. The smart contract is not necessarily installed on all peers, but is required for the servers which endorse incoming transactions (determining whether the transaction in question is to be accepted), providing consensus. Every transaction is executed in the context of a single channel. No transactions or associated data of any sort can be made visible from one channel to another.

Channels enable different entities to reside on the same blockchain network while scoping the visibility of transactions taking place therein among organizations that have entered into appropriate agreements.

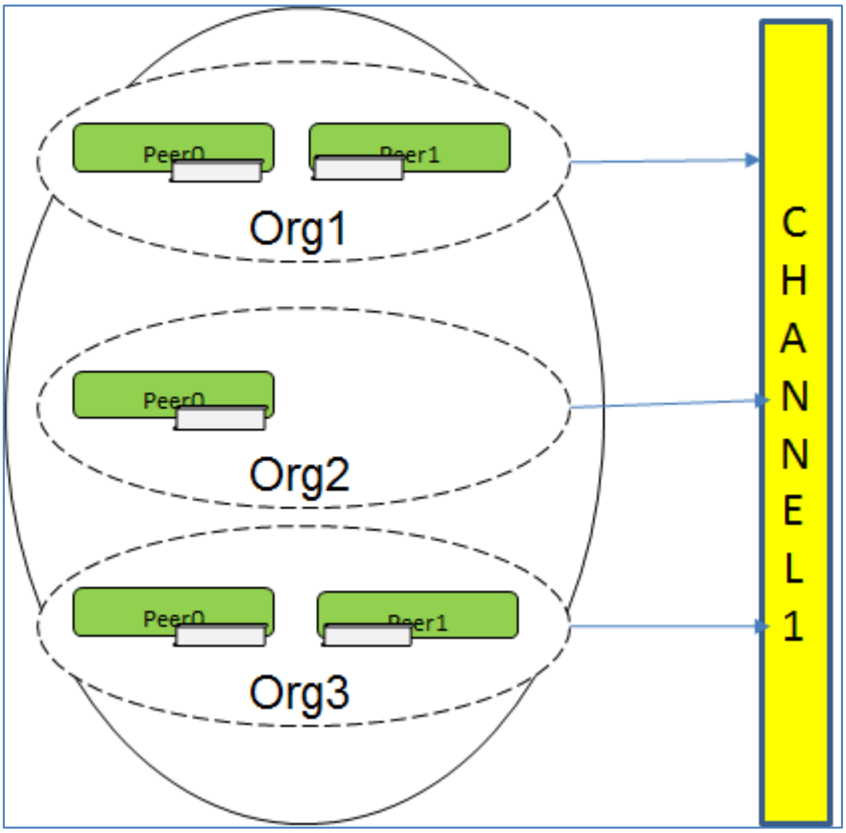

**Figure 9: Single Channel**

## 4.2 Shared channels with application level visibility control

This visibility mode, as depicted in Figure 10, places the responsibility in the hands of the application running above the blockchain network. The lower part of the application, which connects to the blockchain network, can be aware of all transactions taking place in the network, but not everything is made transparent to the upper half, which is in charge of interaction with the higher business layers. Thus,  events can be marked to be visible only to a subset of the servers in which case the blockchain application shall determine whether the information should be made available to higher layers or not.

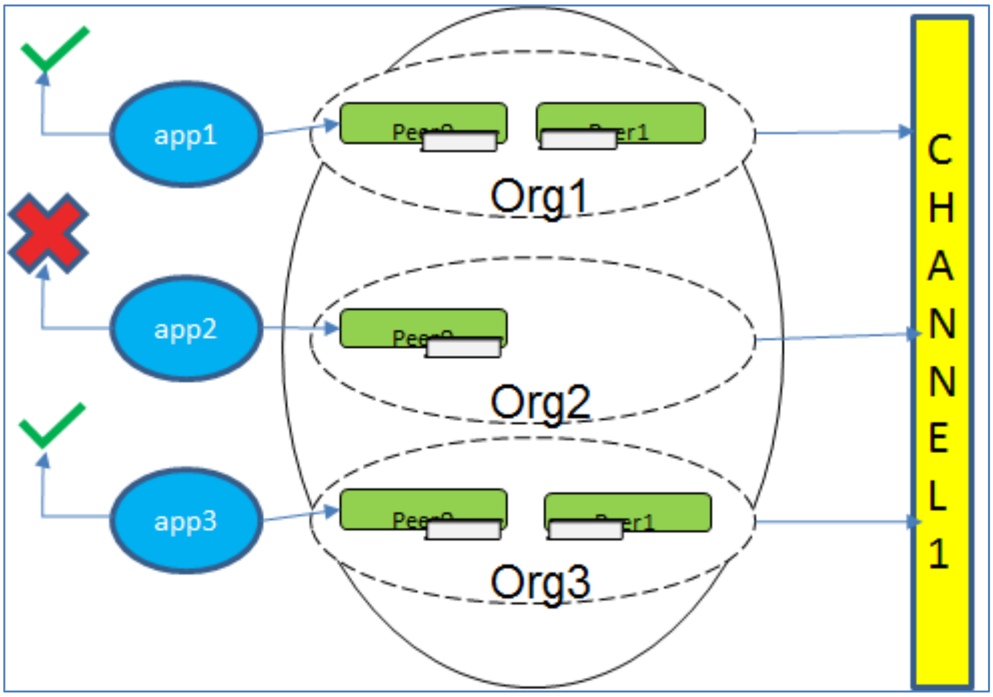

Figure 10: Single Channel with application level visibility control

Furthermore such a capability can be inserted into the smart contracts themselves ,which run closer to the actual blockchain. Such rules can govern which entities are eligible to involve certain transactions and queries. In addition, the establishment of event call-backs can be governed by these agreed upon rules of visibility.

In the MANU-SQUARE context this scheme can be used for example for notification of events taking place on the blockchain channel. An entity can be registered to obtain changes of reputation information concerning themselves.

## 4.3 Multiple channels

Multiple channels enforce complete separation between  different networks and the associated set of partners. Each channel keeps its own ledger and no information about it is disclosed to members outside the associated network. Even when an entity is associated with more than one channel, and even if the same servers are used to replicate the associated ledger, no information flows between different channels. The information includes the participants in the network as well as transactions that are run on a spcific channel. This capability can be viewed as running separate ledgers using the same infrastructure.

Such a setup is useful when there is a desire to share infrastructure elements, such as the ordering service, without sharing any additional business related information. In such a setup complete seperation is enforced and an entity cannot obtain information on relationships or specific transactions that are exchanged between other entities using a different channel.

In the MANU-SQUARE context such a scheme can be used for example for distributing an initial RFQ. The assumption is that entities with common interest shall be members of a common blockchain network and shall use a dedicated channel as the means of communicating information in transactions that are of interest to all parties. The network can consist for example of potential producers and consumers of surplus production capacity. Each consortium sharing specific interest shall operate on a dedicated channel.

Figure 11 depicts a simple multi-channel blockchain setup, consisting of 2 channels. There is a total of three organizations, with only one of them (Org2) being associated with both channels, and two organizations (Org1 and Org3) being associated with a single channel. This reflects a business relationship in which Org2 has business relations seperately with Org1 and with Org3, in which each such relationship is strictly bilatertal and no information from one network should be leaked to the second network.

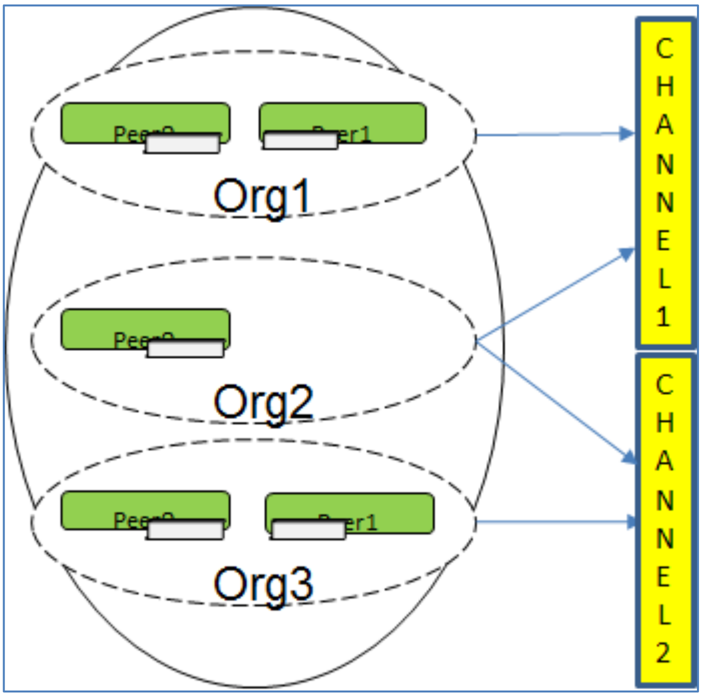

**Figure 11: Multiple Channels**

## 4.4 Channel(s) with private data collections

As noted above, all members of a single channel have visibility of all the information that is associated with that channel. In particular, all members get to see all transactions and associated data. In some cases partners do not want to share all the information with all partners, but creating a specific channel for each such relationship is excessive (in terms of HW and administration), a middle ground was devised, namely private data collections. This mechanism calls for all transactions to be made available to all participating partners in a channel, but a sub-set of the data in the body of the transactions may remain visible only to a designated subset of the participating organizations.

In such a scheme just a hash of the data is stored as a part of a transaction on a block that is visible by all members, while the actual data, which corresponds to the hash mentioned above, gets transmitted only to the designated members of the specific data collection in question. Information transmission is achieved via separate mechanisms than the standard transactions. In particular, the data is not passed through the ordering service, since it is not guaranteed that organizations comprising the ordering service are a part of the private data collection membership.

Such a scheme is useful when overall there is a considerable amount of transactions traffic that may be visible to all participants in the network, but at the same time there are cases in which data should be shared only among a subset of the members of the entire network. For example, organizations can use the same channel for their main interactions, while keeping private information such as the exact price paid by an entity for a product (which may be a different price when a different entity is involved).

In the MANU-SQUARE context this scheme can be used for example by companies submitting their filled proposed RFQ. The knowledge that there was an RFQ published may be shared by all members of the channel, but the exact terms proposed by a single entity are only made available to the RFQ publisher and the entity submitting a response to a specific RFQ.

Figure 12 illustrates the case in which three organizations share a single channel on which to perform most of their services, but at the same time for a subset of the information that needs to be kept bilaterally, there exists a private collection between Org1 and Org2, and a separate private collection between Org 2 and Org 3.

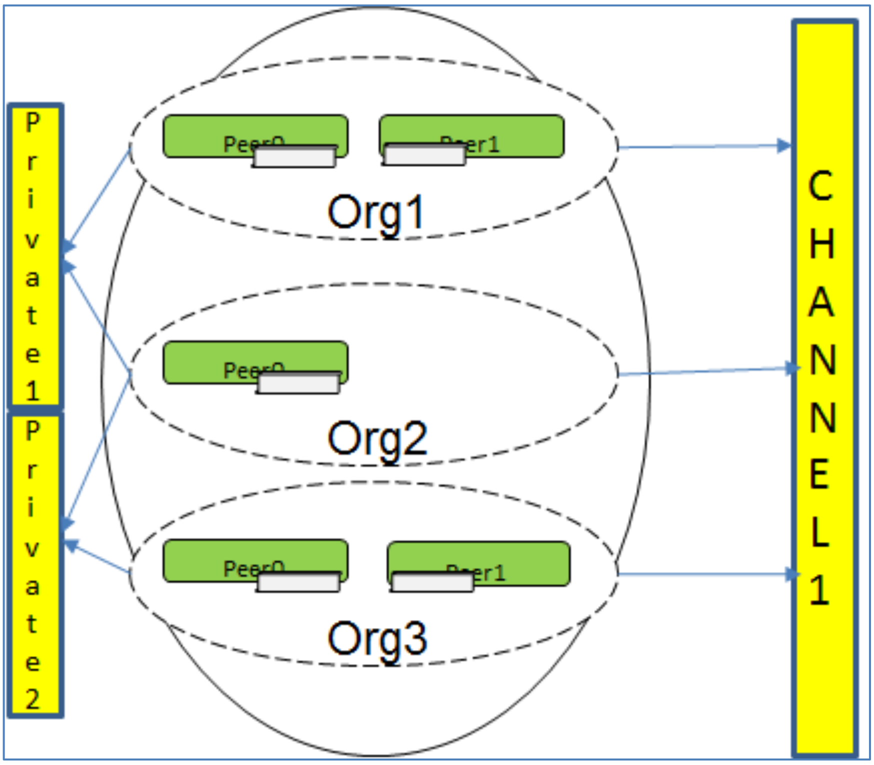

**Figure 12: Private data collections**

### 4.4.1 Channel(s) with local collections

There is an additional variance of supporting private data Channel(s) with local collections. Such a scheme should provide stronger confidentiality by concealing collection membership, thus no identifiable information would be distributed to entities outside the designated group scope, and the private data will be disseminated only within the organization.

## 5 SERVICES ADOPTION IN MANU-SQUARE: RFQ MANAGEMENT

One of the prime examples of supply chain constructs that can be supported by a blockchain backbone is the RFQ process. We have created a simple template which demonstrates the utility of the blockchain as the underlying RFQ process back-end. In this case the blockchain serves both as the single source of trust and truth, and as the driver mechanism used to communicate between different parties. Naturally, variations of this RFQ process can be constructed, based on the foundations we detail below, supporting both structured and less structured manners of interaction between the counter-parts.

The RFQ process support enables the demonstration of the utility of the different available visibility and privacy protecting mechanisms detailed above.

The proposed and demonstrated RFQ process consists of three main primitives (as can be seen in Figure 13), namely: Publish RFQ (offer), negotiate / communicate (counter-offer), and finish (accept or reject). The initial tender corresponds to an action that is advertised using a single channel to which the entity publishing the RFQ participates along with all relevant entities that potentially are able and willing to respond to the proposed RFQ. Thus, the process is initiated by an entity producing a tender and submitting it to the blockchain as a transaction invoking the "offer" function of an RFQ smart contract.

This process can work in a pull or push mode. In a push mode, in the background entities which are interested in receiving new RFQs, register themselves as interested in receiving such events on relevant RFQ related transactions performed on the blockchain. Upon the inclusion of such a transaction in a block, the corresponding call-back shall be invoked. A complementary pull mode would require the deployment of smart contracts that support various kinds of queries to respond to an entity looking for open and available RFQs, or looking for the history of a particular RFQ. Once again such operations should be supported by a single channel for total visibility.

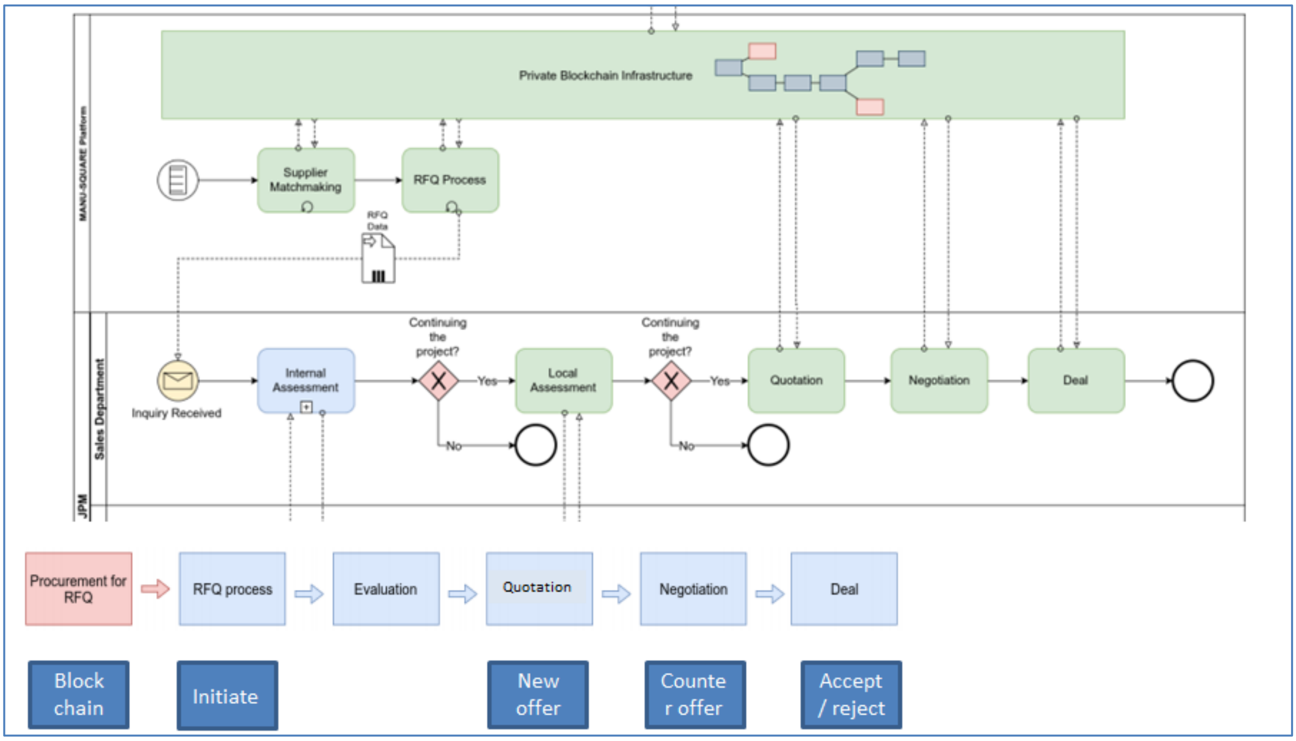

**Figure 13: RFQ backed by blockchain**

In the running example we use in this section the item the first entity is interested to buy is a capacity of a service for stainless steel cutting, and the conditions dictate the humidity in which the produced artefact should be kept throughout the process.

Entities receiving the notification of the publication of a new RFQ evaluate it and if interested can take one of two kinds of actions. First, they can ask for clarifications, and second they can respond to the RFQ. Note that these operations may be repeated multiple times until both sides are satisfied. This corresponds to a phase of clarifications, and potentially negotiations between the initiator of the tender and the potential responders. For this stage, we assume that most of the times the correspondence for clarifications along with the actual response to the RFQ would require limited visibility of the exchanged information. There may be cases in which the information exchange (questions and answers) is agreed upon between the entities to be open to all, in which case these operations will take place on a single channel. In the demonstration, we opted to support this stage via application level filtering (see Section 4.2), which passes the received information to the higher business layer only on the nodes that are designated as valid recipients of that information. That is achieved through an application that is distributed and used on all participating servers.

All the negotiation process consists of transactions being submitted to the blockchain, which are in turn recorded and committed into the ledger. Both parties to the negotiation process are notified as to the existence of new relevant information by using the blockchain call-back events mechanism.

The content of the RFQ responses themselves should be shared only between the issuer of the RFQ and a responder. It is anticipated that for this stage the parties shall use the single channel with private data collections being established among the responders and the issuer. In this case, only the parties which are a part of a private data collection shall have access to the information exchanged between the parties, thus the content of the RFQ response shall remain confidential. In Figure 12, for example, we can see a private data collection that has been established between Org1 and Org2, using Channel1. This data collection shall be used for sharing the RFQ response between Org1 and Org2. In this case Org3 will not have access to the RFQ response sent by another organization.

Finally, the last step consists of the RFQ issuer choosing to accept an offer. In that case an accept message is sent to the selected company and all the other companies that participated in the RFQ process receive a message indicating that the RFQ is now closed, which means that they were not chosen. It is anticipated that these exchanges will take place on a single channel which is visible to all parties. Specific issues that require limited visibility can still be shared via the private data collection. The continuation of the process between the RFQ issuer and the chosen party shall be conducted mostly using a private data collection (in some cases a separate dedicated channel shall be used. Mainly if this marks the beginning of a long collaboration including multiple transactions that all need to be kept private only to a sub-set of the channel participants).

# 6 Conclusions

This document delved into the benefits of using a blockchain network, supporting various visibility scopes, as the back-end for supply chain scenarios, with specific emphasis on an RFQ process. Being a shared ledger, all the steps of the RFQ process are clearly stored and can be made available to the parties involved, while ensuring that each entity has access only to the information that is within the scope of visibility of that entity. This document elaborated on various methods and mechanisms which enable different visibility characteristics based on the nature of the action taking place and the agreements between the counter-parties.

Thus, due to the technical characteristics of the blockchain, the shared ledger can serve as the single source of truth in which all parties can access their data and act upon it, without revealing information to non-intended audience.

The main goal of this deliverable is to enhance D3.1 (Connecting IoT devices to blockchain services), which provided an overall description of the blockchain platform which shall be used as a cornerstone for the supply chain related activities within the MANU-SQUARE project. The primary focus was to demonstrate trust in the system though the provisioning of a variety of privacy preserving scopes available. The discourse was exemplified by one of the MANU-SQUARE use cases which shall use this technology, namely an RFQ process.

The code developed as a part of this task (covering also aspects that were developed in T3.1) is being uploaded to the project GitLab repository (https://gitlab.com/manusquare). In addition, an accompanying video recorded demonstration is being uploaded to the same repository as well, covering aspects of RFQ process support, reputation management support, and the incorporation of IoT data into a Tracking and Tracing scenario.

## 6.1 Next steps

Example support for tenders in the platform via the blockchain shall be demonstrated, based on existing artefacts providing support for the entire RFQ process aided by a blockchain network.

T3.3 shall develop further supply chain constructs to be used in the project, with a goal of being able to present a dashboard including assets and associated state from creation to destruction, abiding by the privacy policies established on different parts of the network. Ultimately, developed services shall be incorporated as a part of the MANU-SQUARE platform, providing capabilities and support to the identified use cases within the project.

The current constructs that are being developed include the RFQ process described above, and a reputation management module. Reputation management is a centre piece to a platform such as MANUS-QUARE, and especially the trust that can be placed on this mechanism. One of the pre-conditions for entities to use such a platform is that they can trust and thus use the reputation management capability. Companies need to be reassured that when locating new potential partners via the platform, they can obtain a credible assessment of them before embarking into a business collaboration.

Finally, there shall be support for a collaborative ideas management system, which will enable people to share and contribute to forming ideas knowing that the underlying blockchain based infrastructure keeps track of the contributions of each individual to the forming idea.