PROCEEDINGS

IPIC 2018

JUNE 17 - 22 | University of Groningen

5th International Physical Internet Conference

BRINGING PHYSICAL INTERNET TO LIFE

Towards a smart hyperconnected era of efficient and sustainable logistics, supply chains and transportation

IPIC 2018
5th International Physical Internet Conference

Trust in a multi-tenant, logistics, data sharing infrastructure: Opportunities for blockchain technology

Simon Dalmolen[12], Harrie Bastiaansen[1], Hans Moonen[2,3], Wout Hofman[1], Matthijs Punter[1], Erik Cornelisse[3]

1. TNO, The Hague, The Netherlands
2. Universiteit Twente, Enschede, The Netherlands
3. CGI, Rotterdam, The Netherlands

Corresponding author: S.Dalmolen@utwente.nl

Abstract: *In support of the trend towards ever more complex supply chain collaboration for the Physical Internet, a trusted, multi-tenant (and interoperable) data sharing infrastructure has to be enabled. Trust is a condition sine qua non organizations may not be prepared to share potentially competitive sensitive information. As such, trust has to be an essential design aspect for any multi-tenant data sharing infrastructure for the data sharing stakeholders*

To overcome the challenges for trusted data sharing, various reference architectures for a trusted, multi-tenant, data sharing infrastructure are being developed. As such, the Industrial Data Space (IDS) initiative is currently gaining attention. It's based on the architectural principles of keeping the data owner in control over his data and keeping data, data processing and data distribution at the source. Its reference architecture is strongly grounded on a role / stakeholder model for the intermediary trusted roles to enable peer-to-peer data sharing over a controlled and trusted connector infrastructure.

The intermediary trusted roles may contain and process meta-data on the data sources, the data transactions and/or on the identities of the parties involved in the data sharing. This paper focuses on the role of blockchain technology for improving trust levels for such intermediary trusted roles.

Keywords: *Supply Chain Collaboration, Multi-Tenant, Trust, Data Sharing, Blockchain, Traceability, Enterprise Architecture*

1 Introduction

The world is increasingly becoming a networked society. To adapt to changing market dynamics, firms take a number of strategic actions. For one, a shift may be observed from companies optimizing their internal business processes into a more collaborative focus in which they focus on optimizing the supply chain as whole. In turn, this leads to organizations shifting from a strategy of competitiveness to a more benevolent strategy (Cruijssen 2006). Consequently, organizations are working together to serve customers through mutually dependent and co-operative supply chains via coordination and collaboration. This not only holds for organizations operating within the same sector, but ever more also for organizations operating in different sectors of society, leading to more complex, multi-tenant, supply chains. Improving the agility and flexibility of (supply) chain collaboration offers potentially major benefits but also poses real challenges, both form an organizational and a technical/IT perspective (Luftman, Lyytinen, and ben Zvi 2017).

For the logistics sector and the Physical Internet, the benefits and challenges for enhanced (supply) chain collaboration is illustrated by means of the potential opportunities it provides for sustainability and CO2 reduction, two of the major challenges for the next decades. Figures of the COP21 in Paris (2016) show that logistics represents 30% of all greenhouse gas emissions, 32% of energy consumption and 94% of all oil import of the Union. From the long-distance perspective, Eurostat surveys estimate that 24% of good vehicles in the EU are running empty and the average loading of the rest is 57% giving an overall efficiency: of 43%. Flow imbalances can explain only half of this loss. The efficiency improvement opportunity is estimated as €160 billion and 1.3% of EU27 CO2 footprint. Reported load factors in delivery vehicles in cities (e.g. 38% for vans in London15) show even a higher opportunity (European Commissission n.d.).

The latter report has various recommendations to increase sustainability of logistics, like fully available and visible intermodal transport services, resilient logistics networks, seamless transshipment, ‘smart’ hubs, and seamless information exchange in end-to-end logistics by participation of SMEs (Small and Medium sized Enterprises), public administrations and all other stakeholders in transport and logistics networks. Data sharing between stakeholders is at the core of improved collaborative decision making and planning. As such, the topic of trusted and seamless information sharing is expected to be boosted by the Digital Transport and Logistics Forum (DTLF).

As this logistics illustrative case indicates, there is a clear business advantage for stakeholders in the supply chain to share operational data in jointly optimizing the efficiency of the transport processes. However, it also gives rise to new challenges:

- *Trusted data sharing:* To reap the indicated benefits of exchanging data, operational data which may be valuable and business-sensitive has to be shared with stakeholders that could potentially be competitors. A trustworthy infrastructure based on solid agreements and contracts and a technical secure data sharing infrastructure are a prerequisite for convincing stakeholders to exchange such data, i.e. an interoperable, multi-tenant, trusted data sharing infrastructure.

- *Data provider/owner in control:* The ability to access information more easily doesn’t mean that all information will be available for everybody. Business requirements still require a solid authorization mechanism to protect competitive information or against criminal intentions. A direct consequence is the need for an adequate usage and access control capability, with the data provider / owner in control. It is noted that even in case the data is publicly available, authentication is still required to reduce misbehavior and malicious activities.

- *Semantic interoperability:* Organizations have implemented different technological solutions to achieve their specific goals. Therefore, sharing data to achieve the collaboration supply chain benefits may require major integration efforts to achieve semantic interoperability and increased accessibility of data based on strict authorization control. The integration can be realized on a bilateral implementation between individual organizations. Traditionally, only large companies could afford to implement dedicated gateways to enable their ERP systems to exchange information with each other. A next step is the dynamic configuration of communities to exchange information efficiently and effectively (Dalmolen et al. 2015; Dalmolen, S, Moonen, H M, and Cornelisse, E 2012). However, the need arises for a more flexible, interoperable and trusted way of sharing data between the connecting systems of different stakeholders to realize interconnectivity in a matter of days instead of development projects of months.

Reference architectures for trusted data sharing are currently being developed. (Trusted Computing Group 2013), (Dalmolen et al. 2015), (Boris Otto et al. 2016). In the mean-time, new technologies are emerging and maturing that will have impact on how trusted data sharing and their (reference) architectures are being developed and implemented. As such, this paper considers the potential role that emerging block chain technologies may fulfill in realizing the reference architecture, especially by circumventing the need for centralized trusted roles (with their potentially added vulnerabilities) in the reference architecture.

This paper has the following structure: The following section (Section 2), describes the IDS reference architecture for realizing a multi-tenant, trusted data sharing infrastructure that forms the basis in this paper on the considerations for deploying emerging blockchain technology. Subsequently, Chapter 3 gives a short elaboration of the potential benefits of blockchain technology. Chapter for elaborates this in the requirement and options that these blockchain technologies may provide for the actual implementation of the intermediary trusted roles in the IDS reference architecture for the multi-tenant, trusted data sharing infrastructure: the Identity Provider, the Clearing House and the Broker Service Provider. The concluding chapter (Chapter 5) presents the conclusions, the topics for discussion and future work.

2 A multi-tenant, trusted, data sharing infrastructure: reference architecture

The reference architecture that forms the basis of the considerations in this paper is the Industrial Data Space (IDS) reference architecture as it is currently gaining major international traction for realizing a multi-tenant, trusted data sharing infrastructure (Boris Otto et al. 2016). The IDS reference architecture can be considered an architectural elaboration of the Trusted Multi-Tenant Infrastructure (Trusted Computing Group 2013). Figure 1 depicts the main roles and the functions they provide, as part of the IDS reference architecture.

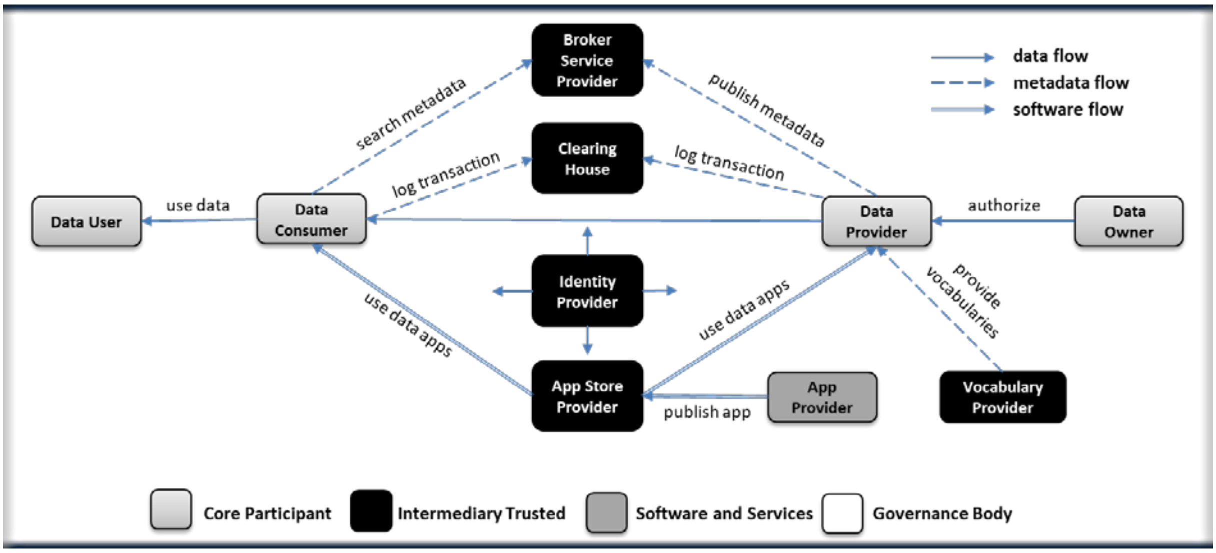


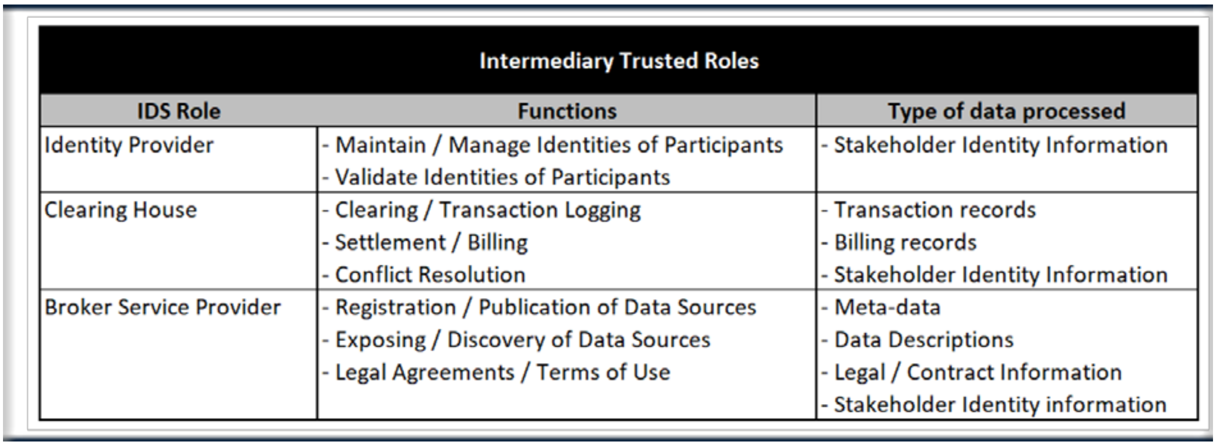
Figure 1: Roles in the IDS reference architecture (Boris Otto et al. 2016).

The roles in the IDS reference architecture as depicted in the figure can be assigned to one of four categories (Boris Otto et al. 2016):

- *Core Participant*. Core Participants are involved and required every time data is exchanged in IDS.
- *Intermediary*. Intermediaries act as trusted entities. Only trusted organizations should assume these roles. They add value for participants in IDS by establishing trust and providing metadata.
- *Software and Services*. This category comprises IT companies providing software and/or services to the participants of the IDS, e.g., in a software-as-a-service model.
- *Governance Body*. IDS is governed by the Certification Body. They ensure that only compliant organizations may participate in this trusted business ecosystem.

The IDS reference architecture is aimed at enabling the trusted sharing of (primary, sensitive) data between ‘Core Participant Roles’. This is done on a peer-to-peer basis between their trusted connectors. No storage of this primary data occurs within the IDS infrastructure. As such, the exchange of this (primary, sensitive) data complies to the design criterion of keeping the data at a source.

The ‘Intermediary Roles’ in the IDS reference architecture act as trusted entities and should only be assumed by trusted organizations. The functions they provide and the data they process are listed in Table 1 for the main intermediary trusted roles.



Intermediary Trusted Roles		
IDS Role	**Functions**	**Type of data processed**
Identity Provider	- Maintain / Manage Identities of Participants - Validate Identities of Participants	- Stakeholder Identity Information
Clearing House	- Clearing / Transaction Logging - Settlement / Billing - Conflict Resolution	- Transaction records - Billing records - Stakeholder Identity Information
Broker Service Provider	- Registration / Publication of Data Sources - Exposing / Discovery of Data Sources - Legal Agreements / Terms of Use	- Meta-data - Data Descriptions - Legal / Contract Information - Stakeholder Identity information

Table 1: Description of the main Intermediary Trusted Roles in the IDS reference architecture.

As the table shows the intermediary trusted roles of the Identity Provider, the Clearing House and the Broker Service Provider process data that should be handled as trusted. They may contain and process trusted data that is related and refers to the data provider and data consumer and the data that they exchange, as enumerated in the right column of the table. Hence, these roles require additional attention as they are an integral part of the sharing of data in the supply chain, and as such form an essential link in the overarching trust architecture for the multi-tenant data sharing infrastructure.

The remainder of this paper will consider whether and how emerging block chain technologies may play a role in the architecture and design of the intermediary trusted roles of the IDS multi-tenant, trusted, data sharing reference architecture.

To assess this potential role of the emerging block chain technologies in the implementation design of the IDS multi-tenant, trusted, data sharing reference architecture, it is essential to start with the concept of trust and what block chain technologies may mean for realizing trust. This is described in the following section.

3 Blockchain technology: its potential

Blockchain technology provides a promising option for implementing distributed ledger architectures. As such, it is currently attracting major attention. The essence of block chain technology can be described as (literal citation from (“Blockchain” 2018):

“A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

A blockchain based solution can add (significant) value in improving efficiency and stimulating trust in multi-tenant data sharing in the supply chain:

- *Minimization the functionality of trusted roles:* As described in the previous section, the intermediary trusted roles (such as the Identity Provider, the Clearing House and the Broker Service Provider in the IDS reference architecture) process data that should be handled as trusted. Hence, these roles require additional attention as they are an integral part of the sharing of data in the supply chain. Blockchain technology may minimize the functionality of trusted roles by circumventing a centralized and trusted data processing function.

- *Conflict resolution:* A distributed ledger can prevent conflicts and discussion. All parties in the supply chain need similar information- and a shared ledger creates a unambiguously overview of the agreements made and the status of the goods at “moment and location X”. In the traditional process the status of goods – and the exact terms parties agreed upon can cause a lot of discussion – due to the fact that every party is holding its own truth/database, and agreements are unique for each contract;

- *Smart logic:* Processes in the supply chain can be automated based on (simple) smart contract logic. Time, location and condition-based triggers can fire specific rules. When you record that ‘a specific container arrives at a specific location in a specific condition’ payments can be made, or release statuses automatically set. In a similar setting it can be arranged how much a company needs to pay in case a container arrives at a certain location earlier or later than agreed on. If both agreements and status updates are immutable recorded (and legally traceable) in a distributed ledger, the ultimate output – payments, releases, information – can be automated as conditions are filled.

4 Using blockchain for intermediary, trusted, roles in the multi-tenant, data sharing reference architecture

The intermediary trusted roles in the IDS reference architecture as depicted in Figure 1, should take a similar architectural and design approach into account for processing the trusted data (as described in Table 1). In these complex supply chains, not only do the data sharing parties often don’t know each other, they often also lack the knowledge and trust (in the ‘trustworthy’ data processing function) of these intermediary trusted roles. Therefore, preventing centralized storage of this data and thereby creating dependency on (actual trustworthiness of) an intermediary trusted role, may provide an attractive implementation option.

As described in the previous section, emerging blockchain technologies may provide such alternatives for the minimization and implementation of the centralized data storing and processing functions of the intermediary trusted roles (Boston Consulting Group n.d.). The subsequent paragraphs of this section describe how blockchain technology could be positioned for implementing the intermediary trusted roles of the Identity Provider, the Clearing House and the Broker Service Provider, respectively.

It is to be noted that this approach on assessing blockchain technology as implementation alternatives within the role and functional model as illustrated in Figure 1, ensures that these technologies are positioned in compliance with the high-level IDS reference architecture. Alternatively, it could also be considered and assessed whether and how blockchain technologies may lead to alternative architectures in which this (primary, sensitive) data is stored, processed and distributed using a blockchain. In our perception, that would imply a fundamentally different architectural approach, not in compliance with the high-level IDS reference architecture and principles. However, this fundamentally different approach is ***not*** part of the current paper.

4.1 Identity Provider

Identity provisioning is a research topic for a long time, however recently it gained more attention due to the blockchain developments. (Allen 2018) has written down ten principles for self-sovereign identity and ensuring that user control is the core part.

1. **Existence.** *Users must have an independent existence.*
2. **Control.** *Users must control their identities.*
3. **Access.** *Users must have access to their own data.*
4. **Transparency**. *Systems and algorithms must be transparent*
5. **Persistence.** *Identities must be long-lived.*
6. **Portability.** *Information and services about identity must be transportable*
7. **Interoperability.** *Identities should be as widely usable as possible.*
8. **Consent.** *Users must agree to the use of their identity.*
9. **Minimalization.** *Disclosure of claims must be minimized.*
10. **Protection.** *The rights of users must be protected.*

Within IDS the role of identity provider is described as a central role in the architecture. Hence, we suggest that an identity blockchain such as Sovrin can give more advantages instead of a central role in the architecture.

"*As an individual's or organization's Sovrin identity builds up over time, so does their reputation. Stepping up from a low trust level to a higher trust level happens seamlessly as more verified attributes and claims are accumulated by the identity owner. This reputation becomes an asset of the identity owner. For example, an individual may choose to reveal their reputation to others to establish and reinforce trust, or an organization may publish its Sovrin-based reputation ratings as a badge of honor.*

This also produces a virtuous network effect. Organizations that are trusted by other organizations as providers of verified claims automatically enhance their own reputations. The more individuals and organisations that rely on your claims, the higher your reputation." ("Inevitable Rise of Self-Sovereign Identity" n.d.)

By using this approach, we foresee a higher acceptant rate in the business field for sharing data. Currently multi-tenant, trusted data sharing infrastructure are hard to maintain and especially the usability is below the norms that are required in the supply chain. In the real world we have an identity document or a driver license where a central authority provides the document, however in the online world this is hard to achieve. In practice you only have a username and password for each site and/or environment.
With Sovrin for example it is possible to create automatic checking of your identity and get access to right information depending on the right you have. And able to share data with other on your own terms.

4.2 Clearing House

The clearing house acts as a trusted, intermediate entity between the Data Provider and the Data Consumer. Its main function is to provide clearing and settlement services for data exchange transactions, including (Boris Otto et al. 2016):

- *Clearing / Transaction Logging*: Both the transmission of data by the Data Provider and the reception of data by the Data Consumer should be confirmed by logging them in a transaction record at the Clearing House.

- *Settlement / Billing:* Billing records can be created based on the transaction record. The transaction can be billed, and the invoices created.

- *Conflict Resolution:* Conflicts can be resolved based on the information that has been logged in the clearing house. This may for instance occur when it needs to be clarified / confirmed that a specific data transaction has occurred and that the data has been received by a Data Consumer.

To implement clearing and settlement services for data exchange transactions by means of blockchain technology, imposes several requirements on the blockchain implementation for ensuring the added trust level:

- The data provider is in control over the insertion of his data transaction logging information on the provisioning of data into the appropriate data transaction ‘clearing’ blockchain, i.e. without an enabling intermediate party. This avoids an additional intermediate party to be trusted.

- Similarly, the data consumer controls the insertion of his data transaction logging information on the reception of data into the appropriate data transaction ‘clearing’ blockchain, i.e. without an enabling intermediate party. This avoids an additional intermediate party to be trusted.

- Confidentiality of transaction records: both with respect to the transaction meta-data (e.g. the identities of the involved parties) and the actual content of the data transaction (type and content of the data that has been shared).

For providing trustworthy clearing and settlement services, it is a prerequisite that trustworthy identities are used when inserting logging data into the appropriate data transaction ‘clearing’ blockchain, for which the services of the Identity Provider (possibly based on a blockchain implementation as described in the previous paragraph) may be used.

A blockchain solution direction for the clearing house functions that circumvents the (potential) trustworthiness issues of a centralized, data storing, trusted clearing house role may have the following features:

- Instances of data transaction ‘clearing’ blockchains being initialized by the data provider for logging specific data sharing sessions;

- The receipt of trusted data sharing transactions is acknowledged by means of secured data receipt records, preferably with (reference to) the legal agreements / terms of use under which these data sharing transaction has been done;

- The secured / certified data receipt records are inserted in the data transaction ‘clearing’ blockchain.

Several implementation strategies can be considered. The data provider may have its own infrastructure for initiating and managing his instances of data transaction ‘clearing’ blockchains. The advantages are higher level of control and low (non) dependency on the (trustworthiness of) third party clearing house role. The disadvantage is the added complexity of managing the blockchain infrastructure. As alternative, a Blockchain Service Provider role may be introduced that provides blockchain management services for initializing and managing instances of data transaction ‘clearing’ blockchains. This unburdens the data provider from the added complexity of managing the blockchain infrastructure. However, this again introduces a central trusted role, although with a limited / lightweight (and possibly untrustworthy) functions it provides as compared to a full Clearing House role. Both variants are depicted in the left-hand side and the right-hand side of Figure 2, respectively.

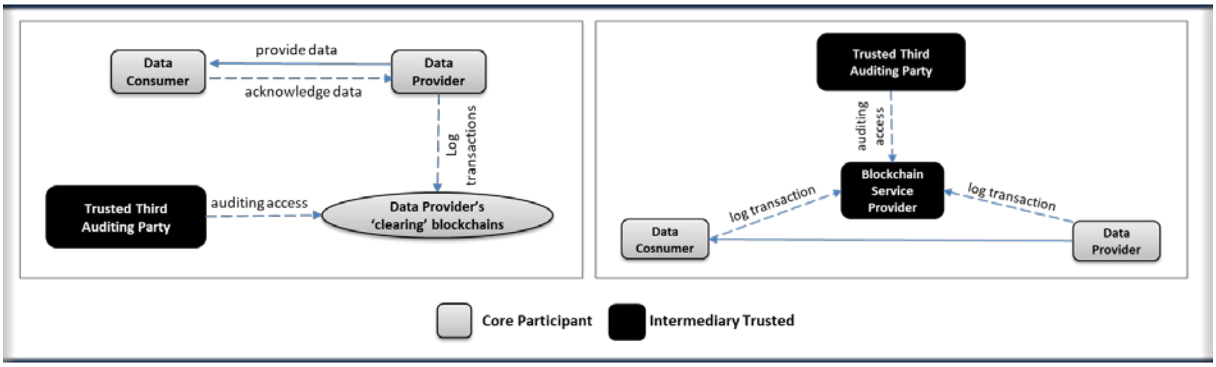


Figure 2: Implementation variants for blockchain technology to support clearing house functions.

4.3 Broker Service Provider

As listed in Table 1, the main functions of the trusted Broker Service Provider role is to enable a registry for the publication and discovery of available Data Sources, together with the applicable legal information and terms of use. As such, a Broker Service Provider handles metadata on the available data sources and contract information. With the combination of metadata on available data sources and contract information, various inter-organizational governance arrangements can be supported (market, bazaar, hierarchy, network) (van den Broek and van Veenstra 2017).

The metadata and contract information to be handled by the Broker Service Provider is in principle public data and is freely available for all interested parties to search for and be discovered. As such, the added value of blockchain features for implementing the data registry of the Broker Service Providers include:

- Integrity can be ensured of the combined and linked information on the available data sources, the legal agreements / terms of use and contractual / pricing conditions under which the data will be provided by the Data Provider.
- The combined and linked information is transparent, traceable and auditable, thereby providing the possibility for conflict resolution in case of differing perceptions between stakeholders on the data description, the legal agreements / terms of use and contractual / pricing conditions and legal under which the data source has been advertised.

- The Data Registry system is resilient, without a single point of failure or corruption,

In case a specific Data Provider decides to selectively publish and make available the metadata for his data only to specific communities or parties, various implementation variant may be considered. The data provider may have its own infrastructure for initiating and managing his instances of data transaction ‘clearing’ blockchains. The advantages is higher level of control and low (non) dependency on the (trustworthiness of) third party clearing house role. The disadvantage is the added complexity of managing the blockchain infrastructure. As alternative, a Blockchain Service Provider role may be introduced that provides blockchain management services for initializing and managing instances of data transaction ‘clearing’ blockchains. This unburdens the data provider from the added complexity of managing the blockchain infrastructure. However, this again introduces a central trusted role, although with a limited / lightweight (and possibly untrustworthy) functions it provides as compared to a full Clearing House role. Both variants are depicted in the left-hand side and the right-hand side of Figure 2, respectively.

5 Conclusions, Discussion

In this paper we have considered the potential role of blockchain technology for realizing added trust levels in a trusted multi-tenant data sharing infrastructure by providing de-centralized data storage functionality for the implementing roles of the Identity Provider, the Clearing House and the Broker Service Provide roles.

On the basis of the results as presented in this paper, the next step is to further elaborate this high level blockchain architectural approach in a detailed infrastructure design, in which the embedding of blockchain technologies within the IDS trusted, multi-tenant data sharing reference architecture is further detailed. This will be done in close cooperation with the blockchain community with the IDS research and development initiative.

5.1 Future work

We foresee that more work is required in the sense of validation of the IDS architecture in combination with our claim that blockchain technology can beneficial as an intermediary, trusted, roles in the multi-tenant, data sharing reference architecture. Instead having a central roles and actors this can help to build trust amongst partners and not having a single point of failure. Furthermore, we aim to setup a business experiment in validating our suggestion to improve IDS.

Currently there aren’t successful implementations of a heterogenous trusted data sharing infrastructure due to all kind off reasons (trust, IT, cost, competition), however with the speed of the adoption of the blockchain we foresee some progress on some of these factors. And this will also increase the knowledge regarding these complex subjects in the practitioner field. Which is very important.

Acknowledgement

The work as presented in this paper has been done as part of the Dutch NOW Research project ‘Data Logistics for Logistics Data’ (DL4LD), supported by Dutch Institute for Advanced Logistics ‘TKI Dinalog’ (www.dinalog.nl) and the Dutch Commit-to-Data initiative (www.dutchdigitaldelta.nl/big-data/over-commit2data).

References

Allen, Christopher. 2018. *Self-Sovereign-Identity: Articles and Documents Associated with Designing and Implementing Identity Technology Using Self-Sovereign Identity Principles*. https://github.com/ChristopherA/self-sovereign-identity.

Boris Otto, Jan Jürjens, Jochen Schon, Sören Auer, Nadja Menz, Sven Wenzel, and Jan Cirullies. 2016. “INDUSTRIAL DATA SPACE DIGITAL SOVEREIGNITY OVER DATA.”

Boston Consulting Group. n.d. “Does Your Supply Chain Need a Blockchain?” Accessed May 8, 2018. https://www.bcg.com/publications/2018/does-your-supply-chain-need-blockchain.aspx.

Broek, Tijs van den, and Anne Fleur van Veenstra. 2017. “Governance of Big Data Collaborations: How to Balance Regulatory Compliance and Disruptive Innovation.” *Technological Forecasting and Social Change*.

Cruijssen, F. C.A.M. 2006. “Horizontal Cooperation in Transport and Logistics.” *Open Access Publications from Tilburg University*.

Dalmolen, S, Moonen, H M, and Cornelisse, E. 2012. “Information Architecture Using a Cargo Centric Approach – Digital Shadows of Real World Objects.” In .

Dalmolen, S., H. M. Moonen, J. van Hillegersberg, A. J. R. Stoter, and E. Cornelisse. 2015. “Supply Chain Orchestration and Choreography: Programmable Logistics Using Semantics.” In *Advanced Logistics and Transport (ICALT), 2015 4th International Conference on*, 76–81. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7136596.

European Commississsion, EU Agenda. n.d. “A Truly Integrated Transport System for Sustainable and Efficient Logistics.” EU Agenda. Accessed May 7, 2018. https://euagenda.eu/publications/a-truly-integrated-transport-system-for-sustainable-and-efficient-logistics.

“Inevitable Rise of Self-Sovereign Identity.” n.d. *Sovrin* (blog). Accessed May 8, 2018. https://sovrin.org/library_items/rise-of-self-sovereign-identity/.

Luftman, Jerry, Kalle Lyytinen, and Tal ben Zvi. 2017. “Enhancing the Measurement of Information Technology (IT) Business Alignment and Its Influence on Company Performance.” *Journal of Information Technology* 32 (1): 26–46.

Trusted Computing Group. 2013. “Trusted Multi-Tenant Infrastructure Work Group - Reference Framework.”

IPIC 2018

wwww.pi.events
ipic2018@rug.nl