New ICT infrastructure and reference architecture to support Operations in future PI Logistics NETworks

D2.11 Blockchain Transactional Ledgers and Smart Contracts as PI Enablers v3 (Final)

Document Summary Information

Grant Agreement No	769119	**Acronym**	ICONET
Full Title	New **IC**T infrastructure and reference architecture to support **O**perations in future PI Logistics **NET**works		
Start Date	01/09/2018	**Duration**	30 months
Project URL	https://www.iconetproject.eu/		
Deliverable	D2.11 Blockchain Transactional Ledgers and Smart Contracts as PI Enablers (final)		
Work Package	WP2		
Contractual due date	31/05/2020	**Actual submission date**	30/05/2020
Nature	Other	**Dissemination Level**	PU
Lead Beneficiary	ILS Group		
Responsible Author	Alexander Papageorgiou (ILS Group)		
Contributions from	CNIT, IBM, NGS, VLTN, eBOS (and input from the Living Labs)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 769119.

Disclaimer

Copyright message

Table of Contents

List of Tables

List of Figures

Glossary of terms and abbreviations used

Abbreviation / Term	Description
ADRS	Automated Dispute Resolution System – A system that utilizes contextual inputs as well as, whenever necessary, human intervention to assess a dispute and provide an outcome for the case
API	Application Programming Interface – A method via which computer code is able to interface with a program, usually defined for web services and system utilities
DX	Deliverable X – The ICONET Deliverable identified by the number X
EOS	EOS – A blockchain that is based on a Directed Acyclic Graph architecture and is one of the highest Transaction-Per-Second blockchains currently in wide use
ES6	ECMAScript 6 – A scripting language specification whose most widely known implementation is JavaScript
GA	Grant Agreement – The Grant Agreement of the ICONET project outlining the scope of work of the project
GPS	Global Positioning System – A system that uses satellites to pinpoint the location of an object using longitude and latitude coordinates
HF	Hyperledger Fabric – The enterprise grade blockchain implementation of the Hyperledger umbrella project, focusing on business networks and logic
JSON	JavaScript Object Notation – A specification as to how to define JavaScript objects in a standardized format that is easily converted from and to a textual format
KPI	Key Performance Indicator – A usually numerical indicator of a system's performance that is associated with an explanation of what it indicates
LL	Living Lab – A testbed where the ICONET solution is meant to be tested on
NLP	Neural Language Processing – A methodology via which natural language is analysed and contextual information is extracted from it
N/A	Non-Applicable – A case where the corresponding column of a row in a table does not have a value associated with it as it is not possible to have one
OLI	Open Logistics Interconnection – A framework that specifies how the overall logistics operators should be categorized into groups and interact with each other in a layered format
PI	Physical Internet – The "internet" as formed by the various operators and enablers of the global logistics network w/ the assistance of state-of-the-art technology and IoT
P&G	Procter & Gamble – One of the Living Labs and partners of the ICONET project
QX	Quartile X – Usually denotes the quartile of a year where something is expected to occur with X indicating the number of the quartile

RESTful	Representational State Transfer (ful) – A set of definitions that dictate how a web API is supposed to be interfaced with by providing verbose HTTP types, such as PATCH for updates or POST for creations
SHA	Secure Hashing Algorithm – An algorithm that is widely accepted to be the most secure hashing algorithm to date that produces a deterministic uniformly random output of a specific length with any type of input sequence of bytes
SLA	Service Level Agreement – An agreement that dictates certain KPIs a service is meant to achieve, usually utilized as a guarantee that a purchased service will meet a set of requirements
STX	SubTask X – The sub-task number X of a specific task as defined in a WP
TDD	Test Driven Development – A programming method of operation that requires any functionality that is coded for a program to be accompanied by tests that confirm that functionality via meaningful language e.g. “the application can do XYZ”
URI	Uniform Resource Identifier – An identifier of a unique resource within a system, usually utilized as a web URL component
URL	Uniform Resource Locator – A string that represents the location of a resource within a system, usually utilized as a website link to inform the site of which resource one wishes to access
VSM	Value Stream Mapping – See D3.6 representing LL2
vX	Version X – A numerical versioning system with X specifying the sequential version of an asset
WP	Work Package – A document detailing the work that needs to be carried out by each partner of a project

1 Executive Summary

The first version of the blockchain related deliverables of ICONET was aimed at setting the precedence of its successors by establishing certain baselines with regards to how the ICONET blockchain solution's development would take place. It outlined the blockchain solution any developments should be based on, the requirements of the said implementation under the context of PI and finally what an alpha implementation should look like. As a result, an alpha implementation of the blockchain was provided along with the first version that showcased the capability of establishing a basic SLA and associating it with a PI container throughout its journey.

The second version of the deliverable was geared towards exploring how the solution can be expanded to accommodate for the use cases of the Living Labs in a more hands-on approach. To this end, inputs from the Living Labs were assimilated in the formulation of the report to define the functionalities that would be expected form the blockchain enabled system by the Living Labs as well as how these functionalities would actually be exploited in each testbed. In the end, a next version of the software was coded along with an externally accessible API which consumes ICONET's transport events to create, maintain and sever SLAs whenever necessary according to a set of rules provided during an order's creation.

This final version is meant to conclude the Ricardian contract related findings of versions 1 and 2 of the deliverable, by investigating the applicability of an automated dispute resolution system based on immutable data derived from the blockchain, in tandem with the formal terms of the Ricardian contracts themselves. This trait would significantly reduce the cost incurred from going through legal processes to resolve disputes arisen from voided transport contracts in the PI world.

Specifically, the first point investigated was whether it is feasible to deviate from the Matryoshka Ricardian contract model applied in v2 and migrate to a Singleton model where each PI transport arrangement or order is accompanied by a single Ricardian contract. This type of segregation of logic would enable the dispute resolution system to be much more fine-tuned to the needs of each order and as such each dispute that comes from one.

Afterwards, supplementary on-chain data as well as off-chain data storable on the blockchain that can be used for the dispute resolution mechanism has been pinpointed. These data are crucial in the impeccable operation of the said mechanism, as the mechanism itself is not be able to assess the validity of the data in terms of its origin of generation, and as such it is up to the "data feed" of the mechanism to solely provide data acquired from the sources either directly or via an immutable storage channel, such as that of the blockchain.

The findings of these investigations have been assimilated to form a concrete dispute resolution mechanism which is able to automatically actuate the blockchain instance itself and severe an SLA contract through its authority as an approved dispute resolution automaton. Both the approval and dispute-based severance process are newly defined capabilities of the blockchain and as such, developmental activities on the blockchain itself needed to be carried out to properly fulfill these functionalities.

Once the complete solution was formed, test suites that replicate the Living Lab environments were created to simulate what a sample deployment use case would look like as well as how the system would perform under this use case. To properly assess the capacity of the solution, a stress-testing tool was once again used to bombard the API endpoints with hand-crafted and machine-generated payloads providing insight to tangible performance metrics.

Apart from the analytical and developmental activities relating to the blockchain aspect of ICONET included in this report, an in-depth inspection of the state-of-the-art PI and transport blockchain initiatives has been compassed to locate other projects that have experimented with blockchain technology deployed in the context of logistics. This inspection was executed to highlight the innovation of the ICONET project and to indicate whether other projects would be capable of utilizing the ICONET project outputs to their benefit.

The related effort for the above is outcome of the ICONET WP2, Task 2.4 "Blockchain mechanisms for secure and privacy-preserving distributed transactional ledgers", the subtasks concerning the realization of smart contracts & the blockchain specifications, and the related versioned deliverables 2.9 (v1), 2.10 (v2) and 2.11 (v3).

2 Introduction

This deliverable's purpose is to investigate an automated dispute resolution mechanism that arises from blockchain-enabled PI SLA contracts and replicate the system should it be possible. The mechanism's description is accompanied by what needs to be done at the blockchain as well as server level to ensure that enough data are available to the system and that the system operates in an autonomous way without the explicit assistance or input of an external human party. This deliverable serves as outcome of WP2 and particularly task 2.4 (Blockchain mechanisms for secure and privacy-preserving distributed transactional ledgers) led by the INLECOM Group (ILS Group). As supplementary research findings, the report also includes an analysis of what has been done in the space of PI and transport in general in relation to blockchain technology.

These findings are meant to distinguish the innovation aspect of the blockchain of ICONET and help paint a clearer picture of what differentiates the ICONET project blockchain initiative from other initiatives in the same field. This deliverable demonstrates the following key statements:

- The applicability of dispute resolution mechanisms in a fully autonomous way in the context of SLAs
- The close integration of the solution in a tangible use case under the LL of Antwerp
- The innovation of the blockchain initiative of ICONET

Numerous initiatives in the space of transport and logistics have been observed throughout the years with regards to applying blockchain technology in a yet-unseen fashion, however these initiatives limit themselves to traditional blockchain implementations and rudimentary use cases that do not yield any revolutionary findings. Instead, they tend to focus on the technology itself and not in how it can interface with the concept of logistics in a unique way. Even more so in the field of PI, as the experimental nature of PI has put off enterprises from attempting to apply blockchain tech to it as PI is a premature technology.

In ICONET, we aimed to break through this barrier and conceive a novel methodology via which blockchain technology can be meaningfully applied in the context of PI with the aid of other experimental technologies such as the Ricardian contracts which our solution is heavily based on. To supplement our findings, we also include any other initiatives that we believe fall in line with what we devised or come close to it to further strengthen

API to both conform to the new specification as well as be able to harness the power of the automated dispute resolution mechanism

3 ICONET Automated Dispute Resolution System

Automated dispute resolution systems (ADRS) have been a field of ongoing research[1] as it is meant to revolutionize the process via which end consumers would bring a breach of a specific term to the attention of companies and corporations in a swift, secure and scalable manner. These ADRS systems aim to streamline the disputing process using digital means to simultaneously cut down the costs incurred with a dispute as well as render the whole process much quicker.

3.1 ICONET ADRS Workflow

ADR systems have seen increasing demand in the ever-increasing digital world of e-commerce, however we believe that such systems would have implications on other fields of digital technology as well, such as that of ICONET. To that extent, we have identified that an ADRS would be an ideal supplement to our blockchain implementation of an SLA tracking mechanism as SLAs are already being terminated and validated with blockchain-based data in our solution.

With the addition of an ADRS it would be possible to further utilize on-chain data associated with a PI container and subsequently an SLA to verify whether the SLA has indeed been broken in case of a dispute that may arise from a party claiming that the SLA was unmet due to the condition that a package arrived in for instance. If the claim included a parameter that was tracked on the package but was not a terminate-able term of the SLA, it will be instantly verified on chain and the dispute's outcome would be automatically carried out.

As an example, a container may be tracking both the humidity and temperature the package(s) is / are placed in. An SLA may be specified with regards to the temperature range; however the descriptive contents of the SLA may mention that the package should be kept in a non-humid state within a pre-defined range that renders the purveyor of the services eligible for a partial refund rather than a cancellation of the service. If the recipient proceeds to claim that this SLA was not followed, he / she would be directed to include the exact term of the SLA he / she wishes to dispute.

Afterwards, two pathways can occur. One would be the SLA term that was specified was a secondary term that was not actively tracked as a terminate-able term. In this case, the metrics stored on the blockchain would be compared to the permitted ranges of the SLA and the outcome of the dispute would be immediately carried out, with a pending action either by automated services or human intervention to carry out the pending actions of the disputes' outcome, such as a partial refund.

The other pathway would be in the case the selected SLA term does not correlate with a measurement tracked by the IoT equipped container. In such a case, the case would be put into a pending state that would require a human to look at the case and validate based on the provided blockchain-certified information as well as any on sc[illegible]

This is completely avoided in the ICONET project as the remediation aspect of a dispute always involves the human element to avoid any type of over- or under-estimations of values involved in the disputes. As such, the system is only responsible for gauging the data it is provided with and impartially providing an outcome on whether the contested claim stands true or not purely based on the data it is provided with.

The rationale behind moving forward with an ADRS is that we foresee disputes arising from SLAs to have a significant impact on the lead time of the resolution of such a typical dispute. Pre-PI, transport and logistics use traditional pen-and-paper contracts meaning that disputes seldomly arise and may be dealt with offline as the contracts are few and under rudimentary terms. In ICONET, we introduce the automation of the generation of such contracts, consequently increasing the “contract” throughput a party possesses in the PI and as an inevitable outcome of that the number of disputes increase.

This increase in disputes needs to be dealt with via a similarly automatic way to avoid solving an issue and introducing another, a common problem faced with experimental state-of-the-art solutions. During our research for the management of the SLAs lifecycle, inclusive of the dispute phase as well as the finalization phase, we identified a posteriori research done on the management of SLAs[3] and they attempted to introduce a similar QoS monitoring service that would alter the SLAs, however they limited their scope to agreements rather than legally enforceable contracts, like Ricardian ones.

Interesting to note, however, is the similarity between the Matryoshka Ricardian contract model we applied in ICONET and the “frame SLA” format mentioned in the aforementioned source which acts as a superset SLA that other SLAs derive from akin to how Ricardian contracts can be derived from a “parent” Ricardian contract using the Matryoshka model.

3.3 Technical Specification of ADRS

As the ICONET ADR system will operate on the blockchain itself, certain abstractions need to be applied to how it will operate as well as what data it will need to decisively produce a satisfactory decision on any dispute it may be provided with. First, the system itself will simply be reduced to a simple state machine that will have one of the following states:

- Contested: The dispute has just been submitted and is being assessed. The assessment phase is important as the action of retrieving the correct data of a PI container is an asynchronous operation due to the distributed operation of a blockchain.
- Valid: The concerns raised in the dispute and the selected SLA terms were in fact breached based on the evidence that was collected from the immutable blockchain IoT measurement data.
- Invalid: The concerns raised in the dispute and the selected SLA terms were not breached based on the evidence that was collected from the immutable blockchain IoT measurement data.
- Indecisive: The ADR system is unable to provide an outcome for the case as it lacks the necessary data and / or context and as such, human intervention is necessary to assess the situation.

One can infer from the aforementioned states that the ADR tool is expected to run within a short timeframe from the conclusion of the service the SLA governs. As a result, we expect parties to follow up their Proof-of-Delivery requests on the Web Logistics Layer with an invocation of the ADR system if they believe that these terms have been breached. To delineate the workflow that can be deduced from these states, the following MSC diagram has been formed:

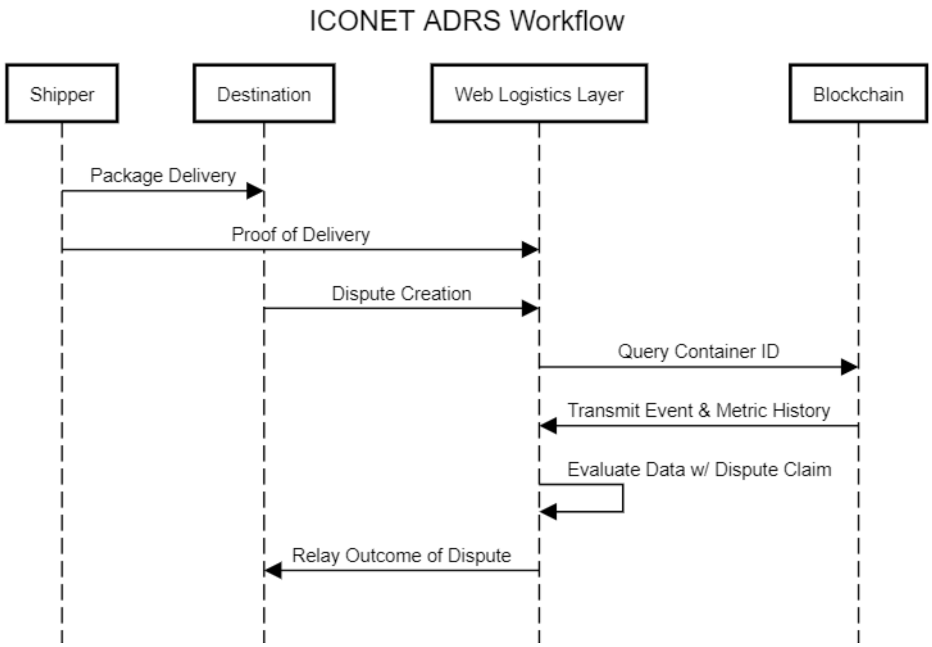

Figure 1 - ADRS Workflow

As a matter of optimization, the previous version of the ICONET blockchain did not store any measurements that were associated with a container that had no SLA applied on them as a matter of optimization and reduced data usage. To properly supply the ADR system with the abundance of information it requires, we revised the IoT measurement consumption endpoint of the blockchain to properly associate a PI container with all its data feeds provided that properly authorized parties relayed those data feeds to the blockchain.

Afterwards, additional members were added to the data structure of an SLA to enable the linkage of an ongoing dispute. This linkage occurs via a SHA-256 hash of the timestamp the dispute has arisen, the term it concerns and the ID of the container and / or products it was in effect for. Afterwards, the data structure of a dispute was defined.

The data structure of a dispute would need to be able to attach to it an arbitrary amount of information as even during the “Indecisive” state of a dispute any material concerning it would need to be passed through the blockchain to ensure that an auditable history of actions regarding the dispute is retained. As was expressed in the version deliverables preceding this report, it is inefficient to store complex data structures and arbitrary-length data on the blockchain due to its nature. For this purpose, we once again propose a hash-based approach where the actual data regarding the dispute are stored in an off-chain repository and the dispute itself possesses a link to the location of the data via a direct link or ID and the hash of the said data is kept in sync on the “Dispute” blockchain data entry.

The “Dispute” data structure itself possesses numerous fields that are meant to help the blockchain system retain the dispute’s state between invocations of the functions concerning it.

Specifically, an enum field is kept to represent the latest state of the dispute, a textual field is kept to identify which containers and / or products it concerns, a hash-map field is kept that maps dispute material hashes to corresponding links of the locations they are stored in and finally, a textual field is once again kept to indicate the responsible party of a dispute. To ensure GDPR compliancy, this is merely an identifier of the person that is assigned on the dispute and contains no identifiable information whatsoever essentially forwarding GDPR compliancy to the company’s user database and identification solution.

These changes brought the introduction of new transaction types at the blockchain level as well, as the blockchain itself distinguishes transactions based on an identifier of the transaction type the initiator of a transaction wishes to invoke. For the purposes of ICONET, we utilize a sequentially increasing positive integer to represent the transaction types as the total number of types is smaller than 256 and as such, a single byte representation of a number can cover the full breadth of transactions ICONET boasts.

A separate activity that needed to be done on the existing blockchain infrastructure was to convert the Ricardian contract generation mechanism from the Matryoshka model to a singleton model, as mentioned in D2.10. The conversion was straightforward; first, the Matryoshka “parent” contract needed to be converted into a template and then, a function that applies the input variables on the template document needed to be coded. To prevent duplication of effort, this activity was carried out in Chapter 5 of the deliverable.

4 Web Logistics OLI Layer Adaptations

The ADRS described in Chapter 3 posed certain changes to the underlying blockchain implementation that have consequently altered the data structures and associated query and submit actuation transactions on the blockchain itself. The change was necessary since dispute states and dispute themselves needed to have some form of on-chain representation to render them non-malleable with a comprehensive audit trail to prevent malicious or accidental overwriting of crucial data associated with one.

To complement these changes, new endpoints need be devised on the Web Logistics OLI layer's server to support these new types of capabilities and be able to process and return to callers the renewed data structures. These endpoints were coded in full accordance with the design paradigm of RESTful APIs, as was the initial version of the server, and documentation surrounding the purpose of each endpoint was also provided in the form of a swagger file that is aimed to be easily digestible by any party that wishes to integrate the ICONET Web Logistics OLI Layer API and blockchain capabilities.

Additionally, the Pub-Sub infrastructure defined in version 1 of this deliverable was expanded to enable subscription to any disputes that require human actions. We envision the subscription pattern in contrast to the polling pattern to be much more efficient in the context of the ADR system as disputes can occur at any given point in time and it is crucial that the responsible parties are informed in the most seamless and automatic way possible reducing the time between the creation of the dispute and its resolution.

The data structures defined in Chapter 3 and particularly the "Dispute" data structure needed to be re-defined in JSON terms albeit with certain characteristics changed to encompass the data transformations that occur at the Web Logistics service. These transformations exist solely to aid other developers in extracting the data they are going for from a specific dispute in a straightforward fashion.

In total, 4 new endpoints were devised whereas 2 endpoints were updated to reflect the changes conducted in Chapter 3. The changes and additions were relayed to the partners of the project accordingly to aid in any additional integration activities that were deemed necessary on their services. To illustrate these changes, the OLI layer interaction diagram of ICONET was updated to reflect the additional endpoints and depict how a typical dispute creation and resolution would look like:

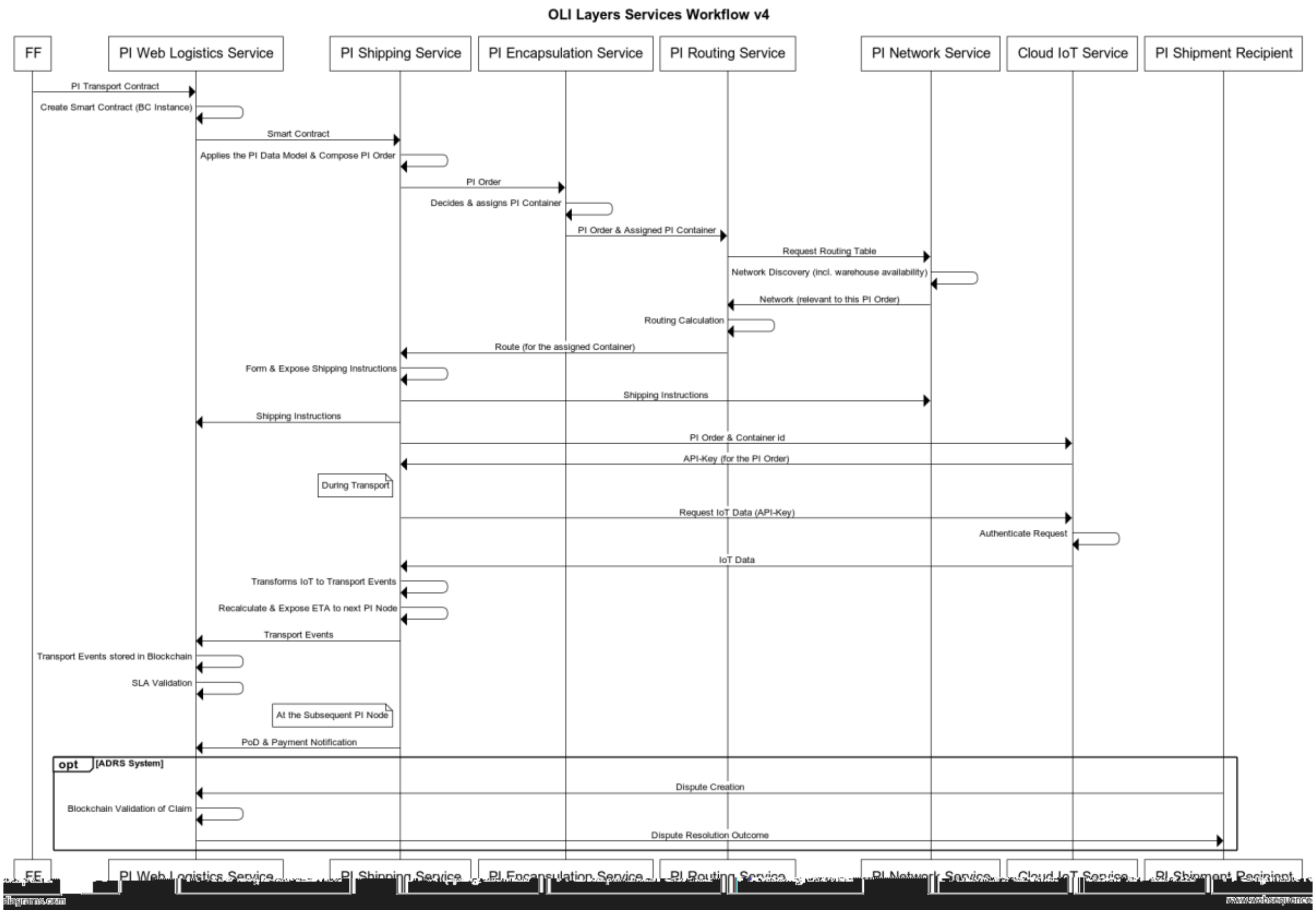

Figure 2 - OLI Layers Services Workflow w/ ADRS System

As observed above, newfound interactions between the Web Logistics layer and the final recipient of a PI shipment can be observed to fulfill the requirements of the ADR system. These interactions are meant to be done in an asynchronous fashion and do not necessary reflect system-aided instructions, as the initiation of a dispute must be done via a human action from the contester of the dispute.

The ADR system is meant to replace traditional legal processes that are involved in the case of disputes, however it should also be capable of performing admirably under a heavy load, as the influx of disputes is expected to increase as the PI becomes more and more interconnected and more contracts are needed to be formed dynamically between the various parties of PI cooperating since cooperation is an integral aspect of PI.

5 PI Corridor Living Lab Scenario and Assessment

The Living Lab of P&G, which is the second LL of the ICONET project, was chosen as the ideal candidate for the definition of a blockchain-eccentric scenario involving customized Ricardian contracts, an application of the ADR system and blockchain-enabled interaction with the Web Logistics OLI layer. For this purpose, close collaboration between ILS, the blockchain lead of the project, and P&G was necessary to exchange the appropriate information and materials needed to make the scenario come to fruition.

To re-iterate, in the second version of the deliverable we described a use case whereby PI Packet turbulences where measured and relayed to the smart contracts for cross-check with the pre-agreed SLA terms and, where applicable, the SLAs where severed and the responsible parties notified via the subscription endpoint of the then-latest Web Logistics API. This was meant to replicate a close-to-reality scenario of what the P&G living lab entails, however it was slightly more generic than what is necessary to properly apply the complete ICONET blockchain solution detailed in this report.

For this version, we specifically reached out to P&G to get hold of what the typical legal contract they form with a transporter is so as to replicate it accordingly in Ricardian contract terms. The conversion was done using manual techniques and attempted to correlate actions that are included in the legal contract and actuated by the blockchain in a computer-friendly format to aid in the consumption of the contract by the Web Logistics OLI layer.

The terms regarding compensation as well as SLAs were also templated to allow their dynamic placement, ensuring that no type of transformation between a legal contract and a Ricardian contract would be necessary for typical use cases. To that end, a small tool was coded that consumes a set of numerical and Boolean inputs and generates the corresponding textual file as well as PDF of a Ricardian contract. The numerical inputs are used for depicting limits of measurements whereas the Boolean values state which optional terms are to be included or not as well as what terms are grounds for SLA severance. Underneath, the tool utilizes markdown representation which is subsequently converted to PDF format via an HTML renderer.

As a next step, the Ricardian contract generation tool was coupled with the endpoint of the Web Logistics layer that consumes the PI Order data model defined in D2.1 to automate the process of generating a Ricardian contract. A hashing algorithm is then applied on the generated Ricardian contract, specifically the SHA-256 algorithm[4] , and the digest of the hash is attached to the SLA entity on the blockchain.

At this point, the Ricardian contract is meant to be stored in some form of historical storage that is accessible by both the owner and the user of the service the SLA describes. For this purpose, any off-chain storage solution would suffice and can be done in either of the two following ways: returning the generated Ricardian contract to the PI Shipping Service OLI layer when the request is completed or storing it locally on the Web Logistics layer and enabling parties to query it via the identifier returned by the initial generation request. For the demonstration purposes of ICONET, we opted for the second approach as it was much faster to simply store the generated Ricardian contracts locally.

Throughout the PI Order's trip, any measurements attached to it are tended to on the blockchain and an auditable and immutable history of them is stored on-chain to aid the ADR tool. Should a PoD signal be sent to the blockchain, active tracking of the SLA concludes and any subsequent measurement that is provided regarding the SLA is disregarded as the SLA is no longer active beyond the timestamp of the PoD. From this point onwards, it is possible to raise a dispute by the corresponding endpoint of the Web Logistics layer.

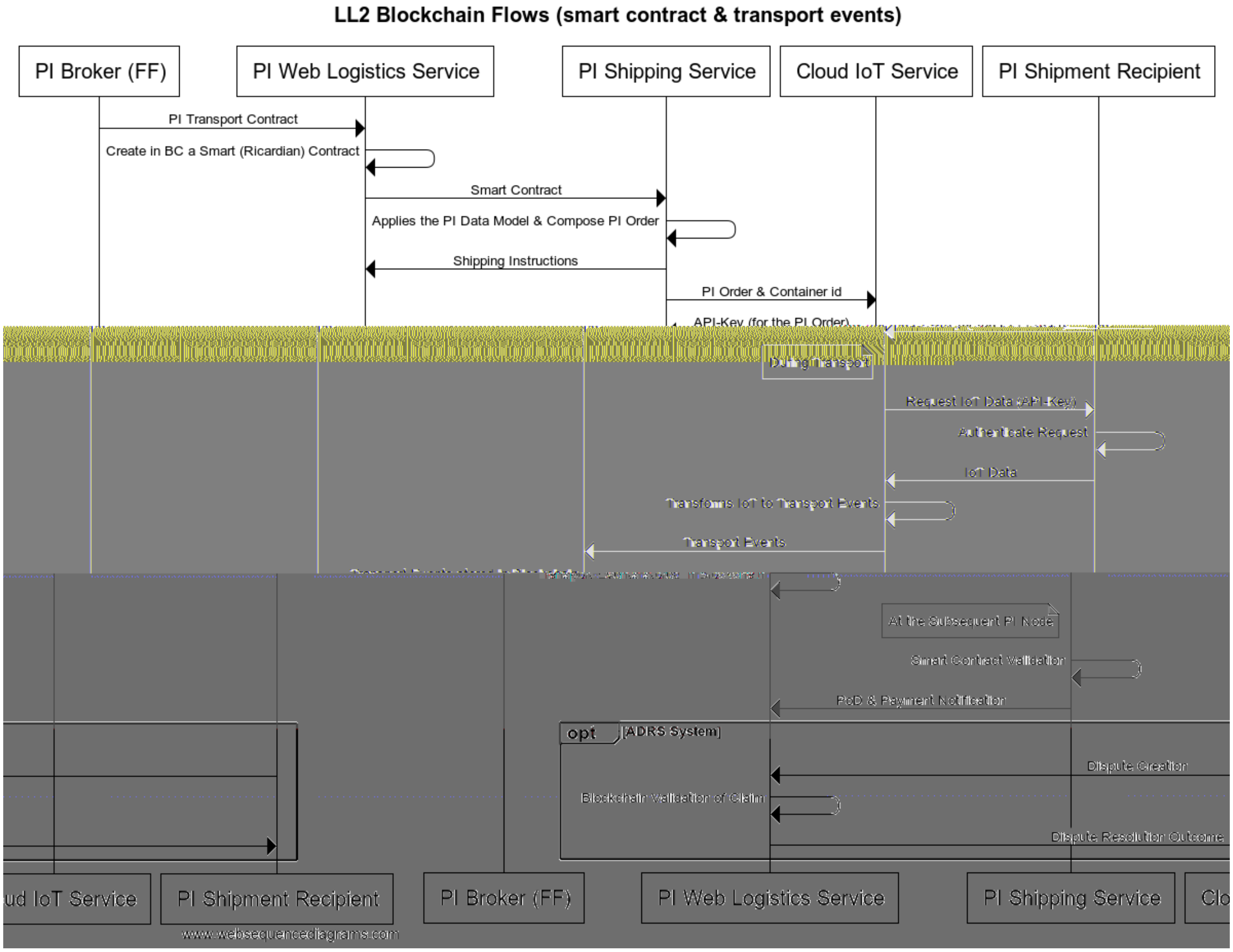

Figure 3 - ADRS within Workflows of PI Corridor LL

The dispute raising process is meant to be done by the PI Shipment's recipient in the P&G case, as they would be the final owner of the items concerned in the PI Orders and would be responsible for assessing that the service was carried out properly. Should a discrepancy occur, they are meant to contact the Web Logistics layer via the "/contract/:id/dispute" endpoint and raise a dispute, where ":id" should be replaced with the ID of the PI Container they wish to raise a concern for. At this stage, the workflow described in the "ADRS" tag takes place. Should the outcome require human interaction, any processes that have subscribed to the Web Logistics dispute notification endpoint will be properly pinged to communicate with the responsible persons of resolving or remediating the dispute.

To further illustrate our case, we contacted P&G and requested them to provide us with indicative metrics of what contracting requirements they presently face as well as what the projected increase in those requirements would be should PI be applied to its full extent. Using those metrics, we devised test suites that indicate how the system performs in the scenario of P&G.

The test case in conjunction with the feedback gathered from P&G has demonstrated that the blockchain-enabled Ricardian contract generation solution is a viable implementation of an autonomous SLA management system that covers all lifecycles of an SLA up to the point of dispute resolution with the aid of the ADRS.

We believe that the blockchain activities of ICONET in the realm of PI will act as the boost platform for other initiatives to flourish, as we believe the work done in ICONET can pave the way for more blockchain initiatives to take place that target PI as their application bed.

6 PI Driven e-Commerce Living Lab Scenario and Assessment

The Living Lab of SONAE is another Living Lab of ICONET that was assessed as a candid testing ground for the complete blockchain solution of ICONET. SONAE was extensive in the material they offered to assist our endeavors in defining a lab-fit scenario by offering us sample legal contracts with expansive materials and multiple pre- and post-conditions that they imposed on orders made on the LL. Their close collaboration bore fruition to concrete Ricardian contract-esque definition of the terms laid forth in their sample contracts, enabling us to inspect how real terms reflect themselves in Ricardian contracts.

In the second version of the deliverable we described a use case of SONAE whereby their complex network of PI hubs, inclusive of dark-stores, convenience stores and SONAE central warehouses, dynamically calculated new routes for their shipments based on situational information such as road closures and construction work. To this end, we proposed the incorporation of the Ricardian-based SLA contracts to the route-calculation mechanism to factor in the time deviation from the original order assumption and properly select the optimal route options based on these conditions.

Within this version, we expand upon the original use case to curate it more towards the automatic arbitration mechanism and its applicability in the context of SONAE. Since the original scenario hinted at the exploitation of the Matryoshka model, this scenario will also assess the performance difference in generating a new Ricardian contract per order instead of a singular one. This impact assessment is crucial in evaluating which version of the ICONET blockchain solution would be more beneficial for which scenario.

Since the material provided by SONAE was expansive in scope, we correlated the contracts provided by SONAE and the contracts provided by P&G to identify common grounds and speed up the manual conversion process. Additionally, automation was introduced in certain aspects of the terms to bring the contract generation speed down and in-line with what one would expect from a performant solution.

Once again, markdown-based templating techniques were applicated on the output Ricardian contracts to ensure that Ricardian contract generation format is uniform across both LLs. In detail, the terms regarding the expected time of arrival as well as the humidity measurement thresholds were converted to dynamic language using data-to-human-readable-format libraries, such as the computer unit 60000 in milliseconds being converted to “1 minute” in the Ricardian contract terms. Although the libraries utilized convert units to humanly readable English text, it is possible to introduce multilingualism by applying internationalization, or i18n, libraries. Certain data-to-human-readable-format libraries possess such capabilities built-in as well, such as the library used in ICONET for time-to-text conversion.

The integration steps with the Web Logistics layer described in Chapter 5 also apply to this LL as the code and material developed behaves in the same way as the code and material described in that chapter. The only adaptation that was necessary between the two was the keys of the string-to-boolean hash map of the Ricardian contract generation tool, as the terms that were converted to dynamically generated ones differ between the two LLs.

The aspect of maintaining Ricardian contracts was not described in Chapter 5 and is crucial to a system which is expected to perform at an enterprise scale. As with code, contracts themselves follow a revision approach where multiple versions of the same document are maintained historically and are constantly adapted to reflect the latest legal landscape. The same applies to Ricardian contracts as it is an inherent trait of legal contracts in general. The original and prototyped system of locally storing Ricardian contracts would not suffice in such a case as the necessary storage space would increase exponentially with time.

To demonstrate the adaptability of the blockchain solution, this issue is easily tackled by introducing a history of Ricardian contract hashes than associating a singular one with each PI Order. As an example, instead of a single textual field that represents the hash of a Ricardian contract, an array of objects each containing two fields, the former being the hash of the contract and the later the timestamp from which onwards the contract is in effect would suffice to fulfill the desired longevity of the ICONET blockchain solution. However, such an aspect is not in scope of the ICONET blockchain solution as the blockchain solution of ICONET is meant to be a prototype other projects build on and utilize as they see fit with care rather than as production-grade software.

To enhance the validity of the assumptions laid out in the SONAE scenario and to properly evaluate the performance of version 2 of the ICONET blockchain against the latest version, we utilized the test suite we had devised for the final LL of version 2 as it encompassed the full ICONET blockchain workflow.

The output of the same test suite applied in the new version can be found in the tables below:

Table 1 – PI Driven e-Commerce Latency Percentiles

Stat	2.5%	50%	97.5%	99%	Average	Standard Deviation	Max
Latency	14 ms	22 ms	345 ms	348 ms	43.2 ms	76.44 ms	360.69 ms

Table 2 - PI Driven e-Commerce Requests & Bytes per Second Percentiles

Stat	1%	2.5%	50%	97.5%	Average	Standard Deviation	Min
Requests per Second	100	100	241	328	231.3	71.22	98
Bytes per Second	29.2 kB	29.2 kB	70.3 kB	95.7 kB	67.5 kB	20.8 kB	28.6 kB

As evident by our findings, the latest version of the ICONET blockchain does suffer a deviation on the original computation time required to generate a Ricardian contract however this delay is negligible when compared to the newfound value the system provides via its ADR system.

7 Blockchain & Ricardian Research Initiatives in PI

Transport and Logistics have been identified as a trending test bed for blockchain-oriented solutions[5,6,7] as they demonstrate a relatively practical use case of where secure data sharing communication channels can have an impactful effect on otherwise non-blockchain processes. However, these initiatives limit themselves to very rudimentary processes that do not possess any intricate functionality and commit basic actions and non-essential data storage.

In detail, logistics-oriented research initiatives seem to investigate the vehicular aspect of the logistics network and how vehicles could be interconnected via a blockchain-enabled way[5], forming a new type of network system of vehicles based on blockchain. The proposed solution is focused on networking and exchange of vehicular information however rather than coordination and actuation on the data inflows of the blockchain.

Another initiative focuses on securing transport contracts via supply chain transparency through blockchain-enabled mechanisms[6]. The main goal of the research paper is to demonstrate that it is possible to improve contractual coordination under a data transparency scenario ensuring each party of the supply chain achieves the best contract arrangement possible. However, the research does not propose an implementable technology but rather acts as an explorative study on how it would achieve its purpose using descriptive terms. Additionally, it does not act in a similar fashion to our solution as it does not aim to replace the actual creation of the contracts but rather render their terms fairer.

In general, it appears there is an ongoing trend in using the distributed database model of blockchains as a means of gaining value for the solution it is used in. As another example, an initiative has been made that places the blockchain as a “distributed registry model” that would securely and auditably store information about the transport network’s state to aid in “insurance telematics applications”[7]. This is an interesting initiative, as it does relate to the legal aspect of transport and logistics and one can see that there is a movement towards using blockchain in conjunction with some form of legal process optimization.

The sole research paper that was identified during our research to capitalize on blockchain technology applied in the context of PI seemed to focus on the transparency of data, such as the “discharge of a container from a vessel” being immediately known by all the necessary stakeholders of the PI that need to act upon it. It revolved around the idea of hyperconnected logistics and stated that blockchain technology, once again as a shared secure data storage, can be used to “optimize capacity utilization” and “combine shipments to reduce costs and produce emissions compliant with (inter)national regulations”.

We were unable to find a mention of combining Ricardian contracts with neither basic logistics and transport, nor the concept of Physical Internet, validating our assumption that previous work has not been done on the subject and renders the blockchain-related outputs of the ICONET project as a priority.

On a more general note, Ricardian contracts applied in conjunction with blockchain technology are seen as an ongoing and rising trend, owing to the numerous benefits the code immutability blockchain technology provides. Production-grade projects have started close-knitting Ricardian contracts to their smart contract counterparts to facilitate the legality of their processes and aid in better classifying what they offer in a legal context.

As a prime example, the OpenBazaar decentralized marketplace implementation features Ricardian contracts as the central liability tracking solution in the context of selling goods, as interparty liabilities are defined in the contracts. To avoid the generation of duplicate terms in each and every good listing on their solution, the project utilizes the Matryoshka model at its core, enabling easily extensible Ricardian contracts to be used for the listings.

Another relatively recent initiative that digests Ricardian contracts and attempts to introduce its developer base to them is the EOS project. EOS (stands for …?) itself is one of the most recent and strongest blockchains to date with regards to its market share and they have explicitly developed helper tools for usage by their developers to generate Ricardian contracts from smart contracts coded on their platform.

Both of these initiatives utilize a similar approach to the one we used in ICONET albeit vastly different concepts, restrictions and data models.

8 Conclusions & Work Ahead

Over the course of the report and based on the academic survey that was conducted to expose any research initiatives that express similarity with the blockchain aspect of ICONET we have determined that as of yet no analogous study has been done on the effects of blockchain technology in tandem with Ricardian contracts. While this may be a positive trait as it brings the ICONET project one step forward in state-of-the-art, it also comes with the negative side-effect of constraining the options of validating the assumptions made in the theoretical process of the solution.

We have attempted to bypass this limitation to the best extent possible by applying numerous good-faith practices during the theoretical groundwork that was laid out in version 1 and 2, such as extensively analyzing contemporary research papers on blockchain technology and Ricardian contracts thus selecting the ideal blockchain candidate and Ricardian contract formation methodology backed by tangible academic material. Each concept that was devised and brainstormed was subsequently either validated or invalidated by probing numerous online data sources of academic nature.

The implementation itself attempted to abstract itself as much as possible to ensure that it remains relevant in the coming years by using a conventional programming language and not limiting itself to the blockchain solution used underneath. The data structures defined are replicate-able in a variety of languages and were defined using ordinary language and data types rather than language-restricted structures.

The metrics utilized on the blockchain instance do not necessarily restrict themselves to the values described in the reports, as any type of measurement that can be represented with a numerical value can efficiently be stored on the blockchain, covering any future types of measurements that my arise as well. The ADR system developed in this report also takes advantage of this fact, generalizing the dispute resolution mechanism by simply judging the numerical data feeds and comparing them to the thresholds imposed in the Ricardian SLAs.

At first, the initial testbeds of the solution were defined from a theoretical perspective based on logical deduction from the traits of the LLs e.g. port of Antwerp is a port, so near large bodies of water and as such humidity may be a concern with the items being transported within. The performance metrics that were used and the cost savings, however, were based at times on actual data retrieved from data sources stemming from the LLs directly, such as Antwerp's influx of containers. As material costs differ from country to country, the indicative median values utilized in version 2 of the report were derived from calculating the median values of various location-agnostic online sellers to calculate a fair market value.

Afterwards, the LL of P&G was examined in depth as it appeared to be the ideal ground for a blockchain-eccentric ICONET scenario. P&G closely collaborated with ILS providing the necessary candidate contracts and materials required to build a deployable version of the ICONET blockchain solution that is curated for the P&G testbed. Using KPIs sanctioned by P&G and test suites that replicate the would-be production conditions of the P&G LL in both a pre-PI and PI context we were able to assess the impact of the blockchain solution of ICONET as well as the underlying ADR system.

The LL of SONAE was also investigated more towards the effects of the newfound blockchain functionality introduced in this report. Particularly, the computation time deviation was appraised between the Matryoshka Ricardian contract implementation and the per-order Ricardian contract implementation.

The LLs of the port of Antwerp and of Stockbooking were evaluated and after closer inspection deemed to not be the ideal grounds for analyzing the impact of the ADRS in depth as the former LL, after being reached out to for inputs, informed us that their contracts are generally long-term and not easily disclosable whereas the latter LL required adaptations to the workflow of the contracts as they were not traditional contracts for PI Orders but rather contracts that would be formed with new warehouses to expand their network.

The product of this report is meant to be consumed by other academic and non-academic blockchain initiatives in the context of PI as it amalgamates what other research activities have taken place in the space as well as finalize the definition of a prototype blockchain and Ricardian contract combination solution. Additionally, the developed solution itself can be potentially consumed by other tasks of ICONET should a beta integration of the blockchain system with the overall ICONET system be worthwhile. As indicated by version 2 of this report, Living Lab 2 has made use of the blockchain software developed via demonstrative examples that were developed in line with the expectations of the LL owner.

To summarize, the blockchain solution was finalized by being supplemented via an ADR system and its capabilities were demonstrated and evaluated via specific use cases relating to the P&G living lab as well as the SONAE living lab. To strengthen the innovation aspect of the blockchain, an exhaustive inspection of both past and ultramodern research papers was carried out to identify any potential papers that pose similarities to the blockchain research activities of ICONET and none were identified that make use of Ricardian contracts in the field of transport, logistics or PI.

Amendments to the blockchain implementation attached to this report may occur as the project progresses to accommodate for any prospective requirements that may arise in the future of the project.

9 References

[1] Palanissamy, Ayyappan, and R. Kesavamoorthy. “Automated Dispute Resolution System (ADRS) – A Proposed Initial Framework for Digital Justice in Online Consumer Transactions in India.” Procedia Computer Science, Elsevier, 27 Feb. 2020, www.sciencedirect.com/science/article/pii/S1877050920300958.

[2] Magiera, Siegfried, and Wolfgang Weiß. “Alternative Dispute Resolution Mechanisms in the European Union Law.” Alternative Dispute Resolution in European Administrative Law, 2014, pp. 489–536., doi:10.1007/978-3-642-34946-1_16.

[3] Marquezan, Clarissa Cassales, et al. “Runtime Management of Multi-Level SLAs for Transport and Logistics Services.” Service-Oriented Computing Lecture Notes in Computer Science, 2014, pp. 560–574., doi:10.1007/978-3-662-45391-9_49.

[4] Handschuh, Helena. “SHA Family (Secure Hash Algorithm).” Encyclopedia of Cryptography and Security, pp. 565–567., doi:10.1007/0-387-23483-7_388.

[5] Pournader, Mehrdokht, et al. “Blockchain Applications in Supply Chains, Transport and Logistics: a Systematic Review of the Literature.” International Journal of Production Research, vol. 58, no. 7, Nov. 2019, pp. 2063–2081., doi:10.1080/00207543.2019.1650976.

[6] Badzar, Amina. “Blockchain for Securing Sustainable Transport Contracts and Supply Chain Transparency - An Explorative Study of Blockchain Technology in Logistics.” Blockchain for Securing Sustainable Transport Contracts and Supply Chain Transparency - An Explorative Study of Blockchain Technology in Logistics, 1 Jan. 1970, lup.lub.lu.se/student-papers/search/publication/8880383.

[7] “Blockchain and Beyond.” International Transport Forum Policy Papers, 2018, doi:10.1787/bf31443f-en.

Annex I: Excerpt Addressing ST2.4.2

Sub-task 2.4.2 of ICONET's blockchain task 2.4 mostly concerned the theoretical and research activities that were carried out in the first version of this deliverable. To re-iterate, we analyzed the state-of-the-art blockchain solutions the market offered during the initiation of the deliverable.

What we identified was that the original blockchain solution that was heavily leaned towards in during the formation of the ICONET project lacked otherwise desirable traits of a blockchain solution for the realm of PI. We managed to find those traits in another blockchain solution that offered greater flexibility to the users of the technology at the expense of readily available functionalities.

As such, any blockchain work that was carried during the course of task 2.4 used the Tendermint framework specified in D2.9 and coded all types of functionalities from scratch, inclusive of how the state is managed, its structure as well as what types of transactions are supported.

To this end, the ICONET blockchain can be called a purpose-built blockchain in contrast to what would have been the result of using a readily available blockchain like Hyperledger Fabric or Quorum.

Annex II: D2.9 Summary

The objective of the D2.9 deliverable was to identify PI use cases, derived from the ICONET Living Labs, that blockchain could be applied on and describe the reasoning behind the research and programmatic steps taken during the solution's development. These programmatic steps were meant to describe the formation of smart contracts that also interact with PI-specific components such as "PI routing" and "PI packets".

Within the report we present the analysis and comparison of selected candidates from the state-of-the-art blockchain technological landscape with the purpose of defining the prime candidate for ICONET and the PI as a whole. The results of the analysis point towards the application of a purpose-built blockchain created upon the Tendermint consensus mechanism instead of a readily-available enterprise grade blockchain solution, such as the one referenced heavily during this project's conception, Hyperledger Fabric. The rationale behind this choice was that the Tendermint consensus engine provides a lot of freedom in the way the blockchain operates down to the block acceptance protocol, enabling us to create faster, more efficient mechanisms for the PI in comparison to the unnecessary computational overhead that exists in Hyperledger Fabric.

The potential application of blockchain technology on multiple use cases was researched with the goal of focusing on a single potential application within the report while simultaneously examining the available options. After correlating the various use cases identified, it became apparent that the dynamic allocation of space in PI Hubs for PI Packets was the most interesting and relevant use case to expand upon.

A notable output of that section was that the PI, as it is slowly but steadily evolving, already has and will open up more areas of interest for blockchain technology, as it is a heavily misunderstood technology, with actual benefits provided they are exploited in a correct manner. To fully capitalize on the benefits of blockchain technology, the automatic generation of Ricardian contracts was inspected within the report.

This inspection was on both a theoretical level, validating the assumption that it is legally possible to generate enforceable Ricardian contracts in a mechanical manner, and a practical level, showcasing the programmatic automation of a traditional PI contract translated to the vocabulary of a Ricardian contract.

Annex III: D2.10 Summary

The contents of the D2.10 report consume the outputs of the D2.9 blockchain deliverable of ICONET by expanding upon its findings and presenting a methodology via which it is possible to enhance the applicable value of the ICONET blockchain by associating Ricardian contracts with the ICONET blockchain's functions thus legally protecting and enforcing them.

Initially, the outputs of v1 of the deliverable are laid out and detailed as to how they will be consumed within this report. Specifically, the blockchain solution that will be used by ICONET is named, the Tendermint Consensus engine, along with the smart contract implementation of a dynamic speed limit for a packet flowing in the PI network and the corresponding LL use cases. These inputs were all justified under the pretense of Ricardian contracts to properly justify why Ricardian contracts were chosen as a means of empowering the functionality of the blockchain with legal affectability.

After the precedence was explained appropriately, the concept of Ricardian contracts is explained as well as their already-proven usability and smart contract correlation. Methodologies via which smart contracts can be linked to Ricardian contracts and vice versa were explored with the concept of PI in mind. These methodologies were then applied to each LL use case to highlight why and how Ricardian contracts are useful for the LLs with direct feedback and validation from the LL hosts.

Once the theoretical groundwork is complete, the practical programming steps taken were analysed and expanded in-depth. First, the legal enforce-ability of dynamically generated Ricardian contracts was conducted to conclude which types of Ricardian contracts ICONET will use. The candidate legal contract, after correspondence with the LL operators, was then identified and transformed to the prose necessary by smart contracts.

The implementation details surrounding the dynamic generation of these contracts based on parameterization of certain variables were subsequently written. Finally, workflows were described that map to each LL use case and indicate the resulting impacts of utilizing Ricardian contracts in existing scenarios. These workflows were tailored to the specifications of each LL and had been created by acquiring feedback from each LL participant.

Code that showcases these workflows and tests them while measuring key performance indicators was also provided to better gauge the impact of the proposed solution with tangible numbers as well as logical conclusions for immeasurable-mathematically indicators such as level of security. This report also contained tangible work that relates to the actual tracking of SLAs within the blockchain context per the specifications of ICONET as well as any supplementary information that was deemed necessary to include for the report to be considered complete.

Annex IV: Code Segment Disclosure

The newly created code of D2.11 was created to facilitate the ADRS as well as enhance the extent at which the Ricardian contracts of the project are utilized as well as how descriptive they are. In this effort, multiple contributions were procured by the LL partners of ICONET to define the model Ricardian contracts that would make sense in each respective LL's scenario. To this end, the LLs provided us with data in the form of confidential contractual documents which we consumed to produce their Ricardian contract counterparts.

While the code itself that manages the blockchain, which was disclosed in the previously versioned deliverables, is not restrained with regards to its disclosure, the Ricardian contracts and code segments that directly interact with terms contained therein are and must remain confidential per the instructions of the partners that provided them.

As a result, code segments are absent from this report to avoid any breach of confidentiality and to ensure that this deliverable can responsibly be disseminated in a public manner. The source materials can be distributed within the EU commission as part of the project's reviewing process and we are ready to respond to any such requests at will.