ETSI GR PDL 006 V1.1.1 (2022-08)

Permissioned Distributed Ledger (PDL); Inter-Ledger interoperability

Disclaimer

The present document has been produced and approved by the Permissioned Distributed Ledger (PDL) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/PDL-006_Interop

Keywords
conformity, interoperability, security, trust

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Enabling communication between different DLT is a challenge that can be resolved in favour of scalability if interoperability is implemented with security, however the architecture, taxonomy and ontology of the DLT landscape is certainly very diverse and with a variety of technical issues and challenges that a lot of time and efforts are being invested in deploying approaches and solutions. This is in favour of the ecosystem as a whole. Priorities for multi-stakeholders are based on interoperability and cross-chain solutions for connecting the new era of internet.

The baseline for the present document is aligned with the definition of ISO/IEC 17788:2014 [i.19] whereby Interoperability is *"the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged"*.

The European Interoperability Framework (EIF) [i.2] from the European Commission (EC) had the first version adopted in 2010 between the new EU policies in the field of information technology with strong focus on openness and information management, data portability, interoperability governance, and integrated service delivery. Furthermore, National Interoperability Framework Observatory (NIFO) [i.13] produce a variety of documents with recommendations for policy makers, researchers, and business stakeholders with the latest developments on digital government and interoperability across Europe. On the other hand, the European Blockchain Services Infrastructure (EBSI) [i.1] is officially established with which inter-ledger interoperability will be a key ingredient for scalable business and connecting networks for cross-border communications. Actually, four use cases are applying on the top of EBSI and one of them is related to trusted data sharing which is a value for considering interoperability as a priority within the deployment of the European Digital Single Market.

1 Scope

The present document describes the key elements of interoperability to exchange information between different ledgers and to mutually use the information that has been exchanged.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] European Blockchain Services Infrastructure (EBSI).

NOTE: Available at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

[i.2] European Interoperability Framework (EIF).

NOTE: Available at https://ec.europa.eu/isa2/isa2_en/.

[i.3] EU SOFIE project.

NOTE: Available at https://www.sofie-iot.eu/.

[i.4] SOFIE inter-ledger implementation.

NOTE: Available at https://github.com/SOFIE-project/Interledger.

[i.5] Inter-American Development Bank (IADB): "Quantum Resistance in Blockchain networks".

NOTE: Available at https://publications.iadb.org/publications/english/document/Quantum-Resistance-in-Blockchain-Networks.pdf.

[i.6] ISO/TS 23635:2022: "Blockchain and distributed ledger technologies - Guidelines for governance".

NOTE: Available at https://www.iso.org/standard/76480.html.

[i.7] D. Lagutin, F. Bellesini, T. Bragatto, A. Cavadenti, V. Croce, Y. Kortesniemi, H. C. Leligou, Y. Oikonomidis, G. C. Polyzos, G. Raveduto, F. Santori, P. Trakadas, and M. Verber: "Secure Open Federation of IoT Platforms Through Interledger Technologies" - The SOFIE Approach. In Proceedings of European Conference on Networks and Communication (EuCNC) 2019. Valencia, Spain, 2019.

[i.8] R. Neisse, J. L. Hernandez-Ramos, S. N. Matheu-Garcia, G. Baldini, A. Skarmeta, V. Siris, D. Lagutin, P. Nikander: "An Interledger Blockchain Platform for cross-border Management of Cybersecurity Information". IEEE Internet Computing, pp. 1-11. IEEE, June 2020.

[i.9] D. Lagutin, Y. Kortesniemi, V. A. Siris, N. Fotiou, G. C. Polyzos and L. Wu.: "Leveraging Interledger Technologies in IoT Security Risk Management". Chapter in: Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection, pp. 229-246. now publishers, June 2020.

[i.10] European Interoperability Reference Architecture (EIRA).

NOTE: Available at https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/about.

[i.11] European Solution Architecture Template (SAT) in EIRA.

NOTE: Available at https://joinup.ec.europa.eu/sites/default/files/document/2019-06/Detailed-level%20Interoperability%20Requirements%20Solution%20Architecture%20Template%20%28DL%20SAT%29%20Design%20Guidelines.pdf.

[i.12] European Library of Interoperability Specifications (ELIS).

NOTE: Available at https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v110 and https://joinup.ec.europa.eu/collection/imaps-interoperability-maturity-assessment-public-service.

[i.13] National Interoperability Framework Observatory (NIFO).

NOTE: Available at https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/3-interoperability-layers#3.1.

[i.14] V.A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G.C. Polyzos: "Interledger Approaches", IEEE Access, vol. 7, 89948-89966, 2019. DOI: 10.1109/ACCESS.2019.2926880.

NOTE: Available at https://acris.aalto.fi/ws/portalfiles/portal/35799505/ELEC_Siris_Interledger_approaches_IEEEAccess.pdf

[i.15] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille: "Enabling Blockchain Innovations with Pegged Sidechains".

NOTE: Available at https://blockstream.com/sidechains.pdf.

[i.16] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2nd October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1724.

[i.17] EU Digital Single Market.

NOTE: Available at https://toop.eu/.

[i.18] WEF: "A Framework for blockchain Interoperability 2020".

NOTE: Available at http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf.

[i.19] ISO/IEC 17788:2014: "Information technology — Cloud computing — Overview and vocabulary".

[i.20] barrywhiteHat's zkrollup.

NOTE: Available at https://github.com/barryWhiteHat/roll_up.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ABBs	Architecture Building Blocks
API	Application Programming Interface
DL SAT	Detailed Level interoperability requirements Solution Architecture Template
DLT	Distributed Ledger Technology
EBSI	European Blockchain Service Infrastructure
EC	European Commission
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EIS	European Interoperability Strategy
ID	IDentifier
ILP	Inter-Ledger Protocol
IoT	Internet of Things
NIFO	National Interoperability Framework Observatory
OOP	Once and Only Principle
PDL	Permissioned Distributed Ledger
SAT	Solution Architecture Template
SLA	Service Level Agreement
URL	Uniform Resource Locator
V2X	Vehicle-to-everything

4 Why Interoperability between PDLs

Combining two or more DLTs using inter-ledger mechanisms allows a different tradeoff in terms of trust and cost, allows different levels of privacy, and can increase the overall scalability and functionality. A higher or wider-scale trust requires a larger network with more nodes and/or a more demanding consensus model. This is the case of public ledgers, which results in a higher computation cost, hence monetary transaction cost, and higher transaction delay compared to permissioned DLTs. Hence, transactions requiring a higher level of trust can be recorded on a public blockchain, whereas transactions which occur frequently but for which a lower level of trust is sufficient can be recorded on a permissioned DLT. Utilizing permissioned DLTs can support higher privacy, since all transactions on a public blockchain are public. Hence, data can be stored in permissioned DLTs for privacy, whereas hashes of the data stored on permissioned DLTs can be periodically stored on public blockchains to ensure immutability of the data. Finally, multiple permissioned DLTs can be combined with a public blockchain to exploit transaction locality, hence achieve scalability, while also allowing the permissioned DLTs to support different consensus models and programming functionality.

The present document envisions the scenarios for multiple ledgers and distinguishing from the present document considerations intra-chain or inside the same PDL which allows interoperability between applications but do not communicate with other PDL. Although it is a very important dimension of the interoperability which is part of the intrinsic mechanism of the PDL, in this clause it is an introduction for a cross-chain or inter-ledger interoperability scenario.

5 What is not Interoperability between PDLs

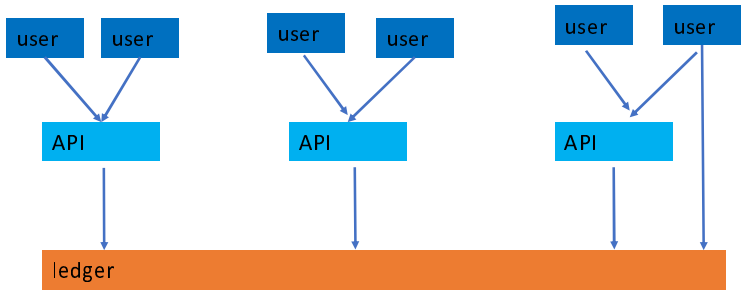


Figure 1: Example of non inter-ledger interoperability

Within the figure 1 the scenario represents a type of interoperability which is out of the scope of the present document. With different components operating in the same ledger with which interoperates each others inside the PDL.

6 Types of PDL Interoperability

6.1 Unidirectional

6.1.1 Description

A PDL receives information from other(s) blockchains (PDLs or not) to update their status (i.e. an oracle blockchain pushing information to a PDL).

A PDL sends information to others blockchain (PDLs or not) (i.e. a PDL updates the status of a delivery to vendor/procurement PDLs).

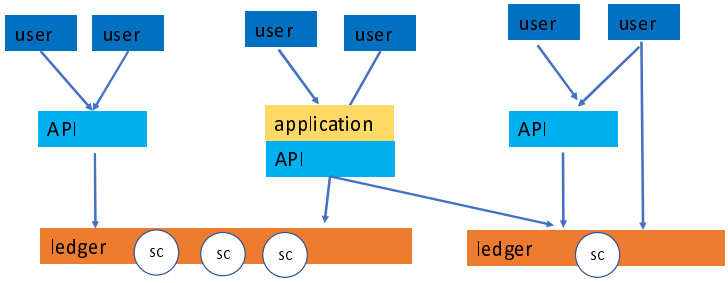


Figure 2: Example one of inter-ledger interoperability

In this basic scenario there are two ledgers whereby interoperate between them, one PDL is exchanging information with other PDL to mutually use such information in a perfected and common interest. As per figure 2, the two ledgers represent two different PDL which make via Gateway or API an interoperability approach, but there are a variety of approaches. Independent ledgers into a same scenario can approach from a key-parameters which are recommended to be in every ledger.

When one PDL takes information from another PDL or an external data source following considerations are recommended:

1) Data Integrity: data feed to the ledger needs to be authenticated, guarantee from the source may be attached to prove the integrity of the data.

2) Data Security: ensure the prevention of attacks such as eavesdropping and man-in-the-middle attack.

3) Data format: ensure the data is in the format compatible to the PDL.

6.1.2 Data Integrity

When data is fed to the PDL, it is written to the PDL for eternity. Hence its integrity and authenticity is of prime importance. Moreover, if this data is required to execute further Smart Contracts and invoke other chained transactions this may result in wrong executions. For example, if a Smart Contract is programmed to pay to some customer, and wrong recipient information is fed to the contract then the customer would be different and would not satisfy the performance because of the integrity of the data. In another example, if a malicious party tampers a bid to be entered to a PDL, and the bid value, can feed the wrong bid to the ledger.

6.1.3 Data Security

The data entered in a PDL needs to be secured from cyber attacks such as man-in-the-middle attack and eavesdropping. For example, if a bid is placed by a PDL and to another PDL, it is essential to secure such information exchange.

6.1.4 Data Format

Two ledgers need to understand each other, that is to say that Data exchange between a PDL and another PDL or storage follow a compatible format. Following a mutually agreed scheme for PDL may also help with automated chained executions of the contracts where several Smart Contracts are involved in a chained execution process.

6.1.5 Standard Fields for PDL Interoperability

When interoperating between a PDL and another PDL (unidirectionally), the following fields may be considered as essential.

1) **PDL Identifier:** Every PDL should have an Identifier - this will help in recording the identity of the ledger in the Gateway (see next clause).

2) **Node Identifier:** A unique Node Identifier corresponding to their PDL. For example, a PDL Identifier XY can have a Node with Identifier XY123.

3) **Shareable Data Fields:** Every PDL, when they want to share their data in the future should specify the fields to the Gateway and the fields they do not intend to be shared may not be revealed to the Gateway at all for security reasons.

Referenced architecture for Unidirectional PDL access:

1) The PDL, intending to access data from the other PDL/storage, makes a request to the Gateway. This Gateway is a trusted entity by both PDLs and includes its own storage with Smart Contracts. This Gateway maintains all the records of shareable data between the PDLs, for example, some PDLs may not prefer to share certain details, will not reveal those fields to the Gateway. Smart Contracts stored by the Gateway, may be maintained in another PDL or trusted data storage and depend on the resources available.

2) The PDL requesting for data may include the following details in the request:

   a) Its own (PDL) Identity; may be public key.

   b) PDL Identity they are requesting data from.

   c) Data fields they require.

   d) Duration for which need access.

3) The Gateway checks the requesting PDL credentials in their own records and verifies the access rights; if all matches provide the keys and grants the access. A Smart Contract is executed at this stage and records the details of requesting data and the requester.

NOTE: A Smart Contract will execute in both the cases (accepting or rejecting) the data request to keep record of all the requests.

4) Using the keys PDL1 can access record from PDL2.

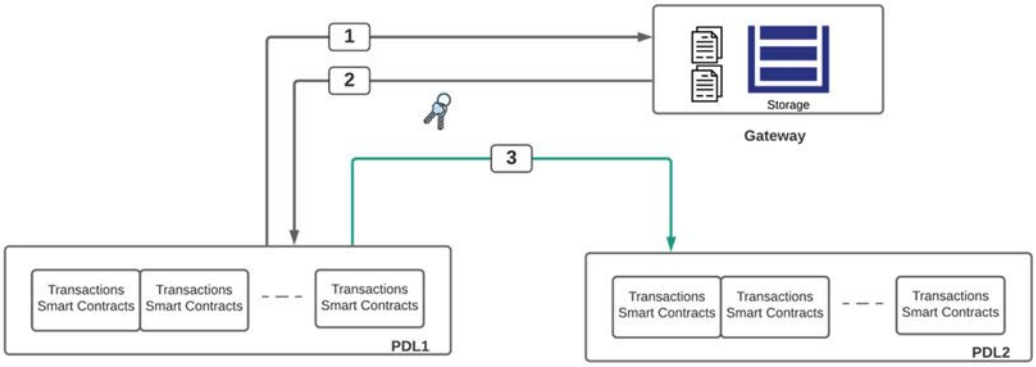


Figure 3: Example with simple scenario of interoperability between two PDL (faster procedure)

6.1.6 Security Considerations

The major security consideration here is the single point of failure for a Gateway. This means that if the Gateway is compromised, the malicious party can take over the system and issue the keys to themselves or possibly to other malicious parties.

The solution (figure 4) can be used instead of saving all the information such as readable data fields the Gateway actually asks from the ledger for permission for PDL1 to access PDL2. The PDL2 decides after running consensus and sends the accept/reject signal to the Gateway by executing a Smart Contract in the Gateway Ledger which subsequently issues keys to PDL1 (i.e. the requesting ledger).

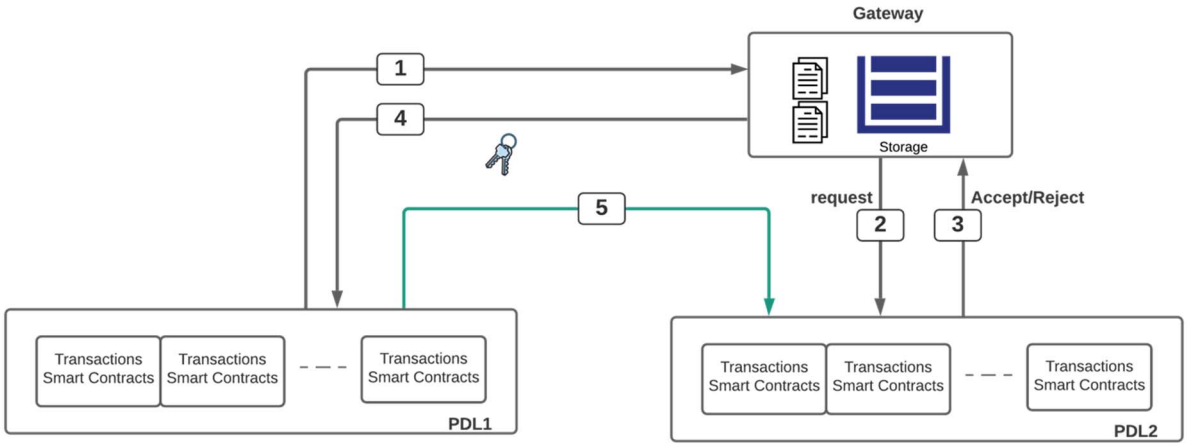


Figure 4: Example secured interoperability between 2 PDL (Live verification)

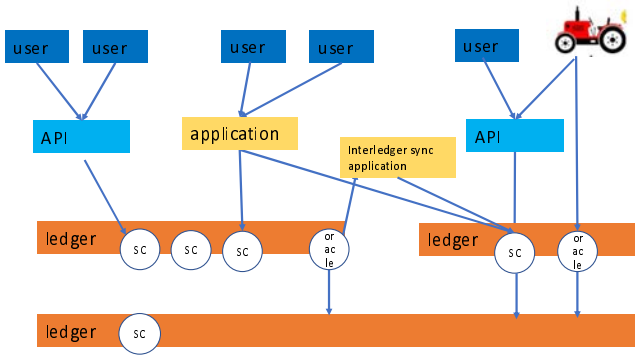


Figure 5: Example two of inter-ledger interoperability

In this scenario there are three ledgers that consolidate a common ledger as part of one PDL. Hence inter-ledger interoperability can occur between ledgers within a same PDL or between various PDL.

The architectural model may vary from the scenario but there are three common facets for the inter-ledger interoperability which are unidirectional in the schema of figure 5:

a) Immutable ledger: transaction record's facet.

   It represents the transactions distributed ledger whereby the replication is unstoppable between all the nodes and consolidate the validation and represent the source of truth for the PDL.

b) Services and application ledger: Inter-ledger interoperability's facet.

   It represents the utilities and facilities that provide interoperability within the PDL between the different ledgers and it is normally composed of a minimal functional components such as Smart contracts and APIs that interact, usually, with a Gateway between ledgers in accordance with the particular performance.

c) User's Access Management: Behavioural facet.

   It represents the accessibility to consumers and users, and may vary between different architectural models whereby could be from different perspectives such as observing and reading the immutable ledger and/or using the services and application ledger.

   In this scenario there are a variety of entities which require a minimal identification and authentication to produce effects within the PDL, however no permissions to users that are just reading the immutable ledger, making analytics in that ledger and or researching activities but are not able to execute transactions without permissions and authorizations which are duly in conformance with the services and applications ledger and the governance dependency of the PDL.

   This scenario does usually provide oracles which are able to enhance the ledgers and contribute the performance between the services and application ledger with the immutability ledger for processes of verification and/or fraud detection by increasing the ability to be obliterated, which represents that the attributes of the PDL provides documentary completeness.

6.2 Bidirectional

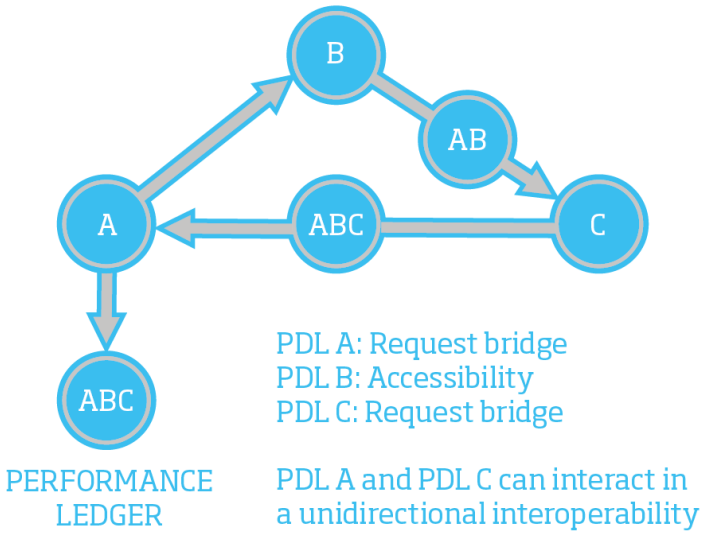
The main challenge of bidirectional interoperability is the synchronization of all ledgers involved; the essential scenario represents the interoperability between distributed ledgers whereby the administrative domain is decentralized.

Simple ledger can relay in a variety of layers and a variety of PDL can coexist for a same industry whereby PDLs consolidate their flow and registries in an immutable ledger that reflects the status of both PDLs is valid.

Directionality is independent of direct or indirect techniques, which means that unidirectional approaches can be direct or indirect techniques and at the same time a variety of techniques can be applicable for direct or indirect considerations of bidirectional interoperability.

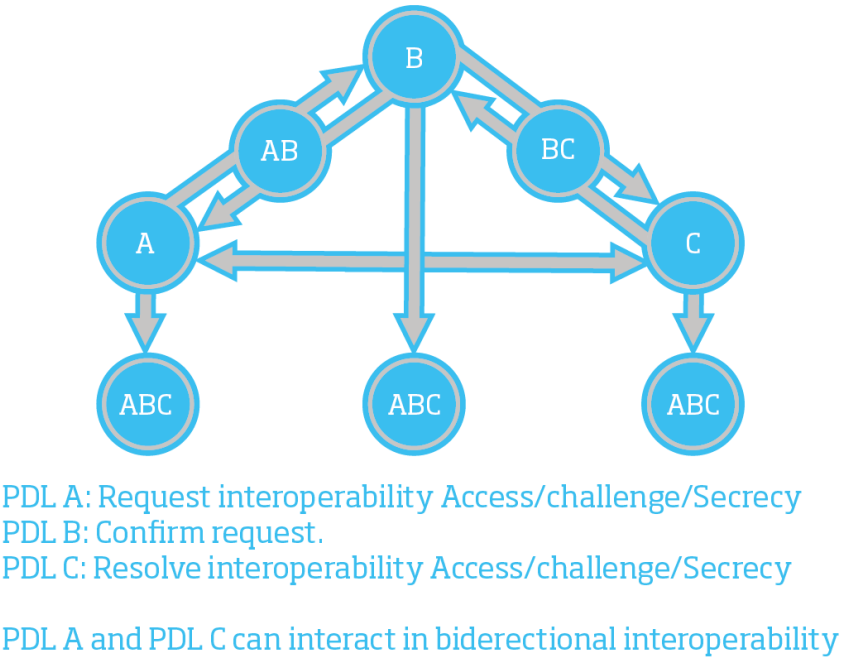
Whereas A is a PDL looking for interoperability, B is another PDL for interoperability or an application (API, Gateway API, etc.) for interoperability, which some of those tools or auxiliary mechanism are described in the present document, and C is another PDL which is requested for interoperability or is looking for interoperability with PDL A.

Within the diagrams, it is visible to compare the scenarios whereby, and independently if it is direct or indirect techniques, various PDLs make interoperability, as shown in the two following scenarios.



NOTE: The same kind of registry can only be changed by one of them.

Figure 6: A PDL can change the status of some registries of another PDL and vice versa



NOTE: Any change in any PDL triggers a change in the other PDL.

Figure 7: Two PDL share the value/status of one or more registries

7 PDL interoperability tools

7.1 APIs or Tooling: as depicted in EIRA

The European Interoperability Reference Architecture (EIRA) was created and is being maintained in the context of the New European Interoperability Framework and National Interoperability Framework Observatory ISA2 program [i.13] as part of the European Interoperability Strategy (EIS). With these key instruments, the European Interoperability Framework (EIF) [i.2] is endorsed by the European Commission and is composed of an Interoperability governance with four layers.

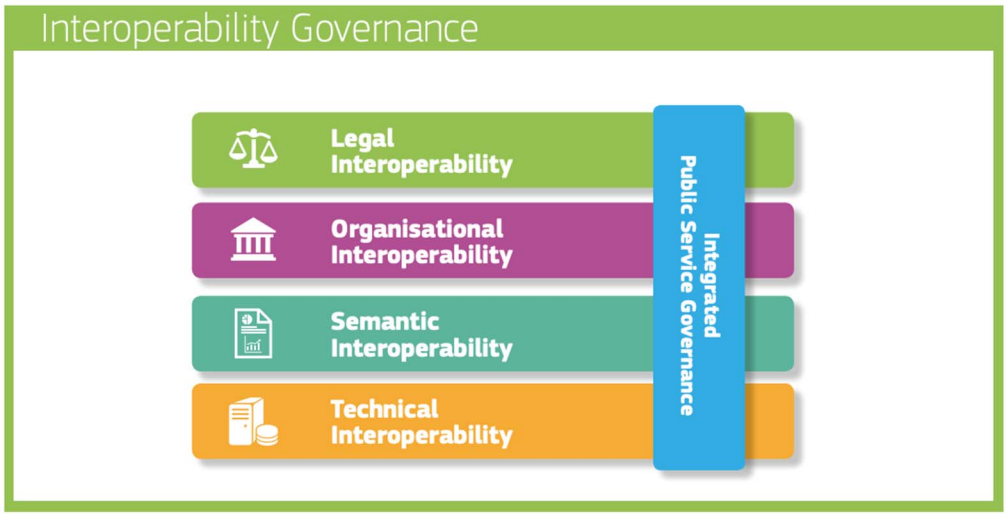


Figure 8: Interoperability Governance in NIFO [i.13]

The interoperability requirements solutions compose an approach via Detailed Level interoperability requirements Solution Architecture Template (DL SAT) which, through a design guidelines, offers specification extending to EIRA providing solution architects in a specific solution domain in a form of a template that can be used to design related solutions. Any Solution Architecture Template (SAT) [i.11] in EIRA contains:

- Principles and requirements.
- Goal and description of supported functionalities.
- A sub-set of the EIRA core Architecture Building Blocks (ABBs) covering the four EIF layers.
- A set of specific ABBs extending EIRA's views enabling specific functionalities to be provided by implementations derived from SAT.
- The interoperability specifications of selected ABBs.

In addition the Design guidelines for SAT provide a comprehensive number of guidelines such as narrative, motivation, minimal attributes for the interoperability specifications such as ID, dct:type, dct:publisher, dct:modified, eira: url, eira:identifier and eira:body. See [i.11].

The lifecycle model of this solutions-based architecture in the European framework is named SAT: plan, build, deliver and run. This model facilitates the semantic and technical views with a legal and public policy view where different domain specific application services and components as well as the PDL can create a blueprint top-down by ensuring the organizational part with cohesive outcome for interoperability.

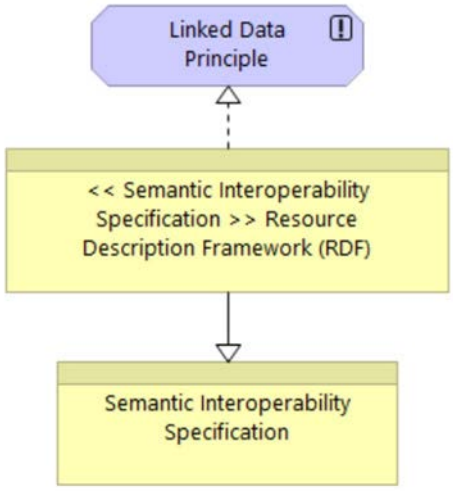


Figure 9: Semantic Interoperability in PDL

An Example of a Resource Description Framework as implementation of Semantic Interoperability Specification which has a principle attached (the Linked Data Principle) in the EIRA DL SAT.

A complete toolkit and libraries are released with their components at the EIRA Library of Interoperability Specifications (ELIS) [i.12] which display: Architecture Building Blocks, specification name, domain and URLs of the interoperability specification.

The National Interoperability Framework Observatory (NIFO) [i.13] is one of the mechanisms in place by the European Commission, to monitor the implementation of the revised version of the European Interoperability Framework (EIF) [i.2] and help to foster the capacity building policy and modernization of public administrations. By doing so, it aims at becoming an online community of practice and the prime source of information regarding digital public administration and interoperability matter within Europe. NIFO is centring its functionalities as information observatory, assistance and support, and community practice.

Through this mechanism EU member estates and associated countries are getting through interoperability matters.

7.2 Atomic swaps

Different categories can use the same basic mechanism; for example, atomic swaps based on Hashed Time-Lock Contracts (HTLCs) are used in atomic cross-chain transactions for direct trading between two peers, in transactions-across-a-network (also referred to as payment networks), Inter-Ledger Protocol (ILP), and some bridging solutions. Hence, the difference between the categories with respect to their underlying mechanisms is not always absolute. However, at a higher-level the various categories differ in their initial application assumptions. Atomic cross-chain transactions target peer-to-peer trading between two parties that seek to exchange value. Transactions-across-a-network solutions and ILP generalize peer-to-peer transactions to payment networks, where payments are routed along paths that are comprised of off-chain payment channels. Bridging approaches target cross-chain transactions between existing ledgers. Sidechain approaches assume the existence of a main chain and support the transfer of value between the main chain and sidechains, which are regarded as subordinate to the main chain. Ledger-of-ledgers approaches introduce a new super-ledger with the goal of having multiple sidechain-like ledgers, which can also support the interconnection to existing ledgers, such as Ethereum and Bitcoin.

The various approaches differ in the reliability of performing inter-ledger operations. Specifically, if atomic cross-chain transactions are performed by a single entity, then this entity can be a single point of failure. On the other hand, bridging approaches, sidechains, and ledger-of-ledger approaches involve multiple nodes that implement the inter-ledger operations, hence their decentralized operation yields a high reliability. Finally, the reliability of approaches involving transactions-across-a-network W3C® ILP depend on the existence of redundant paths between the end nodes that wish to transact, see [i.14].

7.3 Sidechains

By distributing verification or by a better way to utilize the networks' available resources scaling solutions still remain with uncertainty because of the underlying protocol for interoperability. Off-chain protocols like sidechains or rollups implement alternative scaling approaching.

The term of sidechain [i.15] initially was used to validate data between two blockchains as a solution to interoperate for such verification. It was an interoperability solution to enable two blockchains to verify information about each other's progress via light-weight proofs. The intention was to allow bitcoins to be locked in Bitcoin and to be released in the other network (and vice versa) without trusting any intermediary with the funds. Nowadays the term sidechain is used to imply that an independent network in a PDL has a relationship with another network in another PDL and it is implemented with a bridge contract that allows digital assets to be moved from the PDL to another PDL.

Normally the practices are using three types of bridge contracts:

- Single organizational: single party has the custody.
- Multi-organizational: fixed set of independent parties have the custody.
- Crypto-economic: a dynamic set of parties determined by their weight in assets have the custody.

The bridge contract for sidechains does not verify the integrity of the other network and instead relies on a set of parties to attest the validation. The term rollup originates from work emerged on Plasma by barrywhiteHat's zkrollup [i.20], like a sidechain is an independent PDL network but the parties (sequencers) are responsible for providing evidence about the state of the other network to bridge the contract. It is an important difference although Rollup networks can retain the security of the main-chain but also consume more resources from the main chain which decreases the financial sustainability to transact on a rollup in comparison with a sidechain.

From the user perspective is recommended to check the security of the other network and costs before transacting in a public blockchain, however within a PDL is an enabler to interoperate with other PDL networks and can be unidirectional or bidirectional interoperability:

1) Example of sidechain: Polygon [i.15]

2) Example of Rollup: Arbitrum [i.15]

7.4 Layered value transfer protocols

There are several approaches with the priority to identify what or which is the value, and there could be layers of steps to achieve interoperability but some of them cannot provide value for an interoperability or transfer protocols. It is about optimizing the layered value protocols.

7.5 Apps for interoperability

An application of ledger interoperability is shown in figure 10, where an end-device (e.g. user equipment) can have service subscription with a network (i.e. home service provider) and the home service provider can have roaming Service Level Agreement (SLA) with visited network to serve the devices based on subscription (i.e. subscribed services which includes subscribed network slice) during roaming.

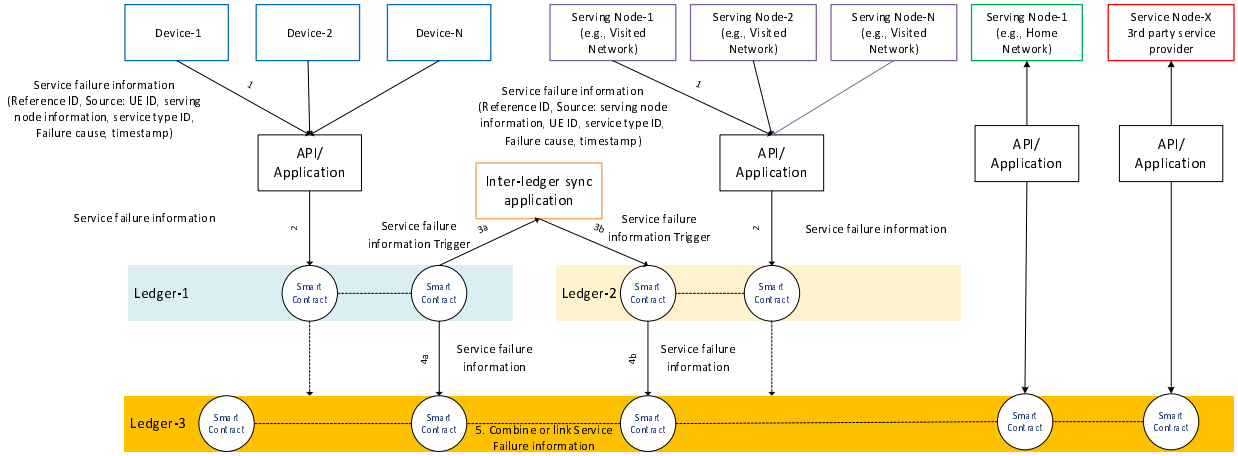


Figure 10: Trusted service failure reporting and handling using PDL with Ledger Interoperability

If the visited network rejects any service request from the device which is part of subscribed services, then the service failure related to a subscribed service can be notified by the device and serving network node(s) in a trust-worthy manner (i.e. the service failure report can be sent as a transaction to the preconfigured/designated application/API) to allow the home network node or any stakeholder to access the respective ledger and resolve the settlement and/or disputes if any raise related to roaming SLA. The steps shown in figure 10 are described as follows.

Precondition: A device requests service based on subscribed services and the serving node in the visited network rejects the requested service (i.e. can be any service such as related to a network slice according to the subscribed network slice) and provides a reference identifier which can be used for the service rejection reporting.

Step 1 The device generates a service failure report which can include reference id, the sender information (i.e. device id), service provider information (i.e. serving node and network id), service type information, failure cause, time stamp and any other required information.

Similarly, the serving node which rejected the subscribed service request can generate a service failure report which can include reference id, the sender information (i.e. serving node and network id), service receiver information (i.e. device id), service type information, failure cause, time stamp and any other required information. The device and the serving node can send the service failure report using any application/API by initiating a transaction to the reporting destination address locally configured.

The service type information can be specific to the type of subscribed service (for example, network slice related to a service such as massive IoT, V2X, etc.) requested by the device and rejected by the serving node.

Step 2 The service failure report transaction from the device and the serving node can be broadcasted to all validator nodes and after consensus can be added to the Ledger 1 (i.e. for device reporting) and Ledger 2 (i.e. for serving network node reporting) respectively.

Steps 3a-b A designated smart contract for Ledger-1 can send a trigger (either directly or via another smart contract responsible for ledger interoperability) related to the service failure information report to the configured Inter-ledger sync application. The Inter-ledger sync application can send the trigger to smart contract responsible for Ledger-2. The trigger can include reference id, sender information, serving node information and timestamp can be included.

Steps 4a-b The Smart Contract responsible for Ledger 1 can send the service failure report as a transaction to another destination address configured in the smart contract which may broadcast transaction to a set of validator nodes responsible for reaching a common consensus across all the involved stakeholders such as home network, visited network and 3rd party service providers and after a successful consensus the service rejection report related to the device is added as a block to another common consensus ledger (i.e. Ledger 3 shown in figure 10).

Similarly, the Smart contract responsible for Ledger 2, on receiving the trigger (as mentioned in step 3b) can fetch the block with reference id same as received in the trigger and send the service failure report information as a transaction and stores in ledger-3 which is built over a common consensus across all the involved stakeholders (i.e. Ledger 3 shown in figure 10).

Step 5 The smart contract in Ledger-3 on receiving the service failure report transaction related to the device from Ledger-1 (i.e. Step 4a) and the service failure report transaction related to the serving node from Ledger-2 (step 4b), adds as inter linked blocks using the reference id as the relation between the blocks. The smart contract stores the reference id, device ID and serving node information along with the block reference/identification of the ledger-3 in an online or offline ledger or storage to resolve future conflicts and settlements related to the financial and service level agreements.

Step 6 Required actions based on the complete service failure information (i.e. Service failure information from device and the serving node) can be taken during SLA evaluation or related conflict resolution. Further if a smart contract responsible for Ledger-3, if configured to report any trigger to the home serving node(s) or 3rd party service provider node(s), then the smart contract may trigger notifications related to the service failure information (i.e. reaching any threshold) via an API/Application.

7.6 Ledger-of-Ledger

Two or more ledgers can be combined into a unified ledger; such events are rare and may not be efficient due to latency computation and concurrency and challenges with a common consensus protocol for building blocks.

Challenges: operational based problems:

- Latency, access control, redaction (hidden data to enable privacy), algorithmic governance, permissions' strategy, node's computation power, synchronization performance time, etc.

Advantages:

- Discoverability, uniformed information in one place, ability to operate transportability and portability, forking, reduce of dependencies and correcting lack of democratization, increased value and trusted data, improve the credibility, etc.

8 PDL interoperability solutions

8.1 Direct interoperability (OOP (The Once and Only Principle)

The concept of the Once-Only Principle focuses on reducing administrative burden for individual and business, it is part of the Single Digital Gateway Regulation (EU) 2018/1724 [i.16] which promotes online access to every citizen and business need in order to get active in EU Countries. One of the innovative solutions developed is a generic federated architecture, developed in collaboration between the different Member States. The approach to federated architecture and building blocks reuses existing building blocks and components and integrates new elements in the European and participating States' ecosystem increasing a multi-disciplinary and intersectoral character of e-Government.

Basically, every business build with the Once Only Principle resolves around re-using data held by one administration, by providing it directly to another administration. It is a bidirectional relationship as required which port the data directly between peers. The Once and Only Principle is not and end in itself and it is part of a range of strategic initiatives at European level supporting cross-border digital public service provision for the Digital Single Market [i.17].

8.2 Auxiliary PDL

- The auxiliary PDL contains part of the information of third party PDLs for the sake of interoperability between those third PDLs
- The auxiliary PDL is the consolidation of third party PDLs (and the reference for disputes?)

In the EU SOFIE project [i.3], inter-ledger is used in various ways, see [i.7]. For example, agricultural supply chain use case stores hash of private transactions to public ledger using inter-ledger, to provide immutability for private transactions and help with dispute resolutions as described in section 6.1. In context-aware mobile gaming use case, private ledger is used to store in-game assets used by the gamers. These assets can be traded in a public ledger between the gamers, but only if they are not active at the same time in the private ledger. The inter-ledger is used to guarantee that the state of the asset is changed in an atomic manner between the ledgers, and the asset can be active only in one ledger at time.

In a similar manner, inter-ledger is useful for any kind of situation where trust, transparency and automation are required between multiple parties. These include sharing cybersecurity information [i.8] or automating disclosure of software vulnerabilities [i.9].

SOFIE project has released an inter-ledger implementation [i.4]. The implementation connects any two ledgers: after a certain trigger occurs on one ledger, the transaction is sent to another ledger.

SOFIE Inter-ledger use cases:

- food-supply-chain:
  - storing hashes of transactions (of a private ledger, even database) to a public PDL:
    - hierarchical DLT solutions
  - context aware mobile gaming ecosystem
- SOFIE Inter-ledger component implementation

9 PDL interoperability goals/needs and recommendations

9.1 Who will interoperate with (checklist from WEF)

With the aim to enable PDL between other PDL, interoperability is explored by WEF [i.18] with a simplistic approach by questioning what platform is used or it is not chosen to simply enhance our communication protocols to application programming interfaces? In conclusion there is a checklist for interoperability recommended requirements from WEF based in three facets:

1) Business interoperability requirements;
2) Platform interoperability requirements;
3) Infrastructure interoperability requirements.

9.2 What information is exchanged

What a user wants in terms of exchange and what is allowed by the stakeholders.

There is a possible conflict between the requirements and capabilities. Capabilities are subject to technical feasibility and legal feasibility when it is a cross border there are concerns in terms of privacy laws and will make impossible not to attend the user's terms or avoid infringements in country's laws. And the stakeholders have to consider also the corporate law which naturally into a PDL a multi-jurisdiction is in nature and this is why it is recommended for the interoperability between PDLs to observer the data transport between countries and respect also the corporate networks to be accountable for user/consumer protection.

9.3 Which operations are allowed

Considering that a PDL can have a general purpose or specific purpose the range of operations allowed will be determined by the purpose of the network in the PDL. Furthermore, within a PDL there would be different layers which perform specific interoperability functionalities with dependencies from the directionality, sometimes are unidirectional dimensions to consolidate secure status to interoperate with or transmission or portability purposes to interoperate with, another situations perform bidirectionally with an in-put and out-put layer or with elements that are performed in a common ledger or replicated in its PDL. To decrease the uncertainty with the ability of interoperability is useful by providing some guidelines with the minimum security level for interoperability and maintaining a contingent program to anticipate vulnerabilities whereby by defining the operations allowed and the requirements to establish interoperability, it can enhance the certainty for interoperability.

9.4 Traceability and auditability

Events have to be traceable otherwise will not be able to cross-domain and the performance, integrity and authenticity of the interoperability has to be auditable. Keeping records/logs of transactions will allow to roll back in case of discrepancy.

Time-stamping consideration of the perfected interest between the two PDLs for interoperability is essential to ensure proper sequence of events.

It is recommended that the sequence of events has to pre-synchronize the atomic clock and other circumstances related to the configuration to mitigate risks and/or provide alternative responsive mechanism for interoperability.

9.5 Future-proof

The foreseen advent of quantum computers poses a threat on current PDLs, specifically in what relates to the vulnerability of digital signatures in transactions, and of the key-exchange mechanisms used for the communications among the nodes (see [i.5]). This obviously impacts inter-ledger activity and poses the additional risk of divergent solutions to address intra-ledger quantum vulnerability.

The current proposals on Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) are intended to address these potential vulnerabilities, and standards solutions are being produced for their application in general signature methods and communication protocols, including the convergence of key management interfaces. ETSI, IETF and NIST are specifically active in these fields, and it is recommended to follow their results in order to provide feedback on their applicability for intra- and inter-ledger PDL scenarios, and to incorporate and adapt these results as they become available.

9.6 Minimal viable governance

A PDL requires a clear definition on the lifecycle whereby the minimal viable governance guidance is going to be implemented: initialization, operation and termination. At the same time, it is necessary to make a perimeter on the context per each phase of the lifecycle where the roles and application's policies and rules are easy to audit and provide efficacy on the accountability.

Table 1: Inspired from ISO/TS 23635 [i.6] Guidelines for governance (ISO TC 307)

	INITIALIZATION	OPERATION	TERMINATION
Protocol context	Genesis Block, establishment of interoperability	Alteration rules (Forks, etc.)	Execution and validation
Application context	Accessibility and accountability	Discoverability, Auditability, availability, accountability, Syntactic Interoperability	Disposal, destruction or transfer
Data context	Establishment of data governance	Collection, Storage, Reporting, Semantic Interoperability	Disposal, archiving or destruction
Behavioural context	Organic functions and operations	Decision, Distribution, dispute resolution, Business Interoperability	Decommissioning and Disposal

History

Document history		
V1.1.1	August 2022	Publication