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

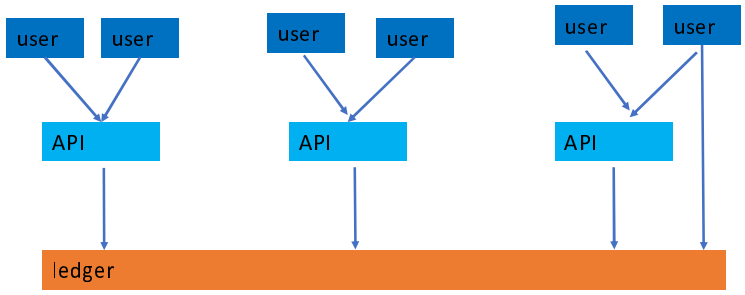

Figure 1: Example of non inter-ledger interoperability

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).

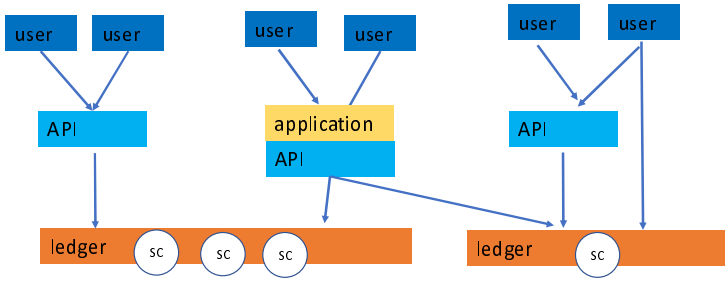

Figure 2: Example one of inter-ledger interoperability

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.

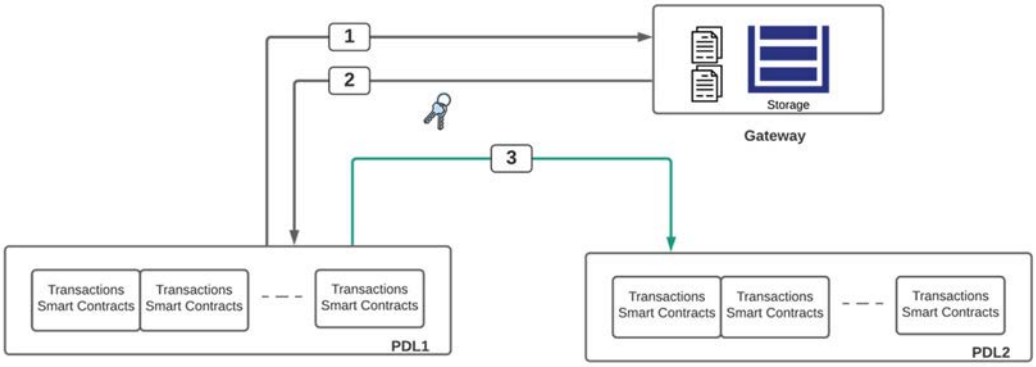

Figure 3: Example with simple scenario of interoperability between two PDL (faster procedure)

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).

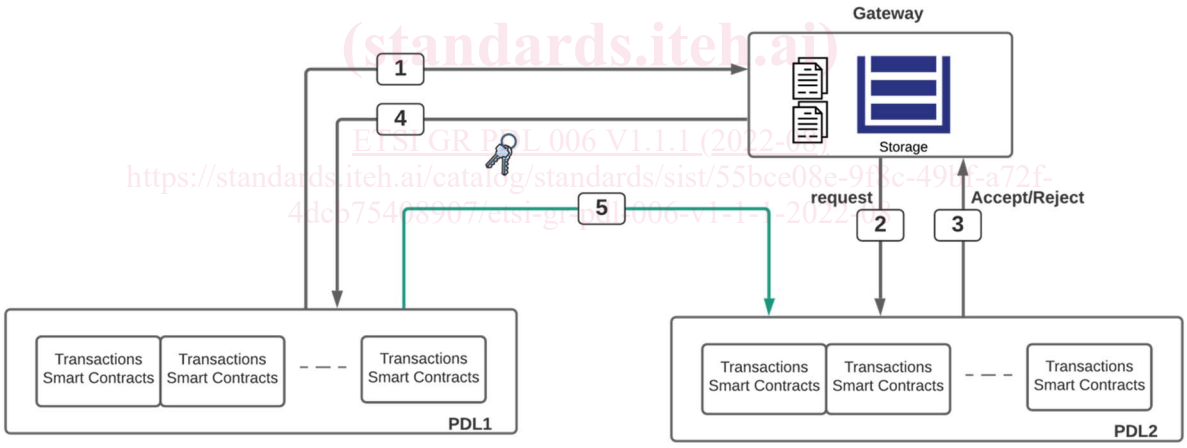

Figure 4: Example secured interoperability between 2 PDL (Live verification)

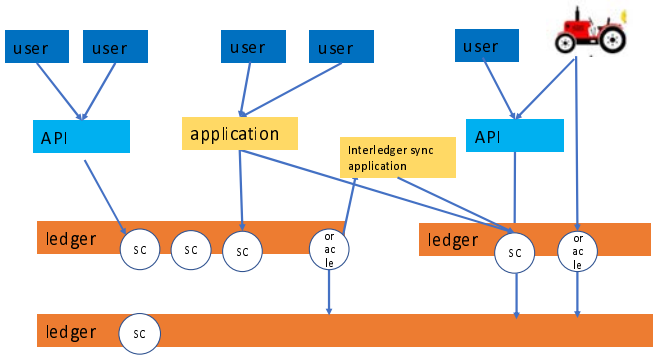

Figure 5: Example two of inter-ledger interoperability