***Disclaimer***

The present document has been produced and approved by the <long ISGname> (<short ISGname>) 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.

ETSI GR ISG-PDL 006 v.0.0.5 (2020-09)

eorganizational proposal

**Group REPORT**

PDL INTER-LEDGER INTEROPERABILITY

*The GRs (ETSI Group Reports) are deliverables produced by Industry Specification Groups (ISG). GRs are written with the style of a Technical Report (TR), and represent the sole view of the ISG members.*

**The guidance text (green) shall be removed when no longer needed
or the skeleton without guidance text also available via the editHelp! website should be used.**

<

Reference

PDL-006 INTER-LEDGER INTEROPERABILITY

Keywords

Security, Conformity, Trust, Interoperability

***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 - NAF 742 C

Association à but non lucratif enregistrée à la

Sous-préfecture de Grasse (06) N° 7803/88

***Important notice***

The present document can be downloaded from:
[http://www.etsi.org/standards-search](http://www.etsi.org/standards-search#Pre-defined Collections)

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at <https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.

All rights reserved.

**DECT**TM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
**3GPP**TM and **LTE**TM 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.

Reproduction is only permitted for the purpose of standardization work undertaken within ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Broadcasting Union yyyy.

© Comité Européen de Normalisation Electrotechnique yyyy.

© Comité Européen de Normalisation yyyy.

© WIMAX Forum yyyy.

Contents

Intellectual Property Rights

Foreword

Modal verbs terminology

Executive summary

Introduction

1 Scope

2 References

2.1 Normative references

2.2 Informative references

3 Definition of terms, symbols and abbreviations

3.1 Terms

3.2 Symbols

3.3 Abbreviations

4 Why Interoperability between PDLs

5 Types of PDL Interoperability

5.1. Unidirectional

5.2. Bidirectional

6. PDL Interoperabilitiy tools

7. PDL Interoperability solutions

8. PDL Interoperability requirements ……………………………………………………………………

#

# Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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](https://ipr.etsi.org/)).

Pursuant to the ETSI IPR Policy, no investigation, 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.

# Foreword

*[ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)* [(](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)*[EDRs)](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx),*

This Group Report (GR) has been produced by ETSI Industry Specification Group <long ISGname> (<short ISGname>).

The present document is part <i> of a multi-part deliverable. Full details of the entire series can be found in part [x] [Bookmark reference].

# Modal verbs terminology

*[ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)* [(](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)*[EDRs)](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx),*

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](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

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

#

# Executive summary

[*ETSI Drafting Rules* (*EDRs)*](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)*,*

# Introduction

*[ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)* [(](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx)*[EDRs)](https://portal.etsi.org/Services/editHelp%21/Howtostart/ETSIDraftingRules.aspx),*

Enabling communication between different DLT is a challenge that can be resolved in favor 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 favor 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 this document is aligned with the definition of ISO/IEC 17788:2014 “information Technology -Cloud Computing-Overview and vocabulary” 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) from the European Commission (EC) had 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, NIFO (National Interoperability Framework Observatory) 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) 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

This document will describe 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

European Blockchain Services Infrastructure (EBSI)

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>

European Interoperability Framework (EIF)

“Full Text: <https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf>

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

## 3.2 Symbols

## 3.3 Abbreviations

API: Application Programming Interface

DLT. Distributed Ledger Technology

EBSI: European Blockchain Service Infrastructure

EIF: European Interoperability Framework

EC: European Commission

NIFO: National Interoperability Framework Observatory

PDL: Permissioned Distributed Ledger

# 4 Why Interoperability between PDLs:

 Motivation.

* + 1. Different sectors complementary services
		2. Third party auxiliary services (Access control, etc.)
		3. Different Jurisdictions (Cannot share a PDL)
		4. Business or personal Privacy issues (Idem)
		5. Antitrust
		6. Regulatory/Lawful access obligations
		7. Business secrets
* exploit different properties of each ledger, lowering cost and latency, better security and privacy (due to GDPR we can not store personal data in public ledgers), etc.
* Transferring and/or trading (or exchanging) value between chains
* Transferring information or generic messages between chains
* Allowing different tradeoffs between trust and cost
* Different levels of privacy
* Increasing the overall scalability and functionality

Combining two or more DLTs using interledger 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.

This document will envision the scenarios for multiple ledgers and distinguishing from this 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 section it is an introduction for a cross-chain or inter-ledger interoperability scenario.

#

Figure 1 EXAMPLE OF NON INTER-LEDGER INTEROPERABILITY

As per the Figure 1, there is just one ledger, in this scenario it is a type of interoperability out of the scope of this document. Serve as illustrative, that functional components, sometimes security functional components others minimal functional components or simply optional functional components, are able to provide intra-chain interoperability, inside the PDL for a completeness of the DLT.

6. TYPES OF PDL INTEROPERABILITY

6.1. UNIDIRECTIONAL

1. 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)
2. 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 interest. As per the 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 (Tooba would contribute this side)



Figure 3 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. (Christophe will contribute this side with a use case)

6.2. BIDIRECTIONAL:

1. A PDL can change the status of some registries of another PDL and vice versa but the same kind of registry can only be changed by one of them.

 ii. Two PDL share the value/status of one or more registries. Any change in any PDL triggers a change in the other PDL.

# 7. PDL INTEROPERABILITY TOOLS:

1. Through APIs or Tooling (as depicted in PDL-003)
2. Through dedicated application (to discuss whether this is interoperability)
3. Through an inter-PDL dedicated application developed for automation of interoperability. This is the case when the two ledgers are not accessible by a single ‘user’.

7.1. APIs or Tooling: as depicted in PDL 03

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), 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 interledger 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 interledger 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.

Note: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

7.3. Sidechains

7.4. Layered value transfer protocols

7.5. Bridging

7.6. Apps for interoperability

7.7. Ledger-of-Ledger

# 8. PDL INTEROPERABILITY SOLUTIONS

8.1. Direct interoperability

8.2. Auxiliary PDL

1. The auxiliary PDL contains part of the information of third party PDLs for the shake of interoperability between those third PDLs
2. The auxiliary PDL is the consolidation of third party PDLs (and the reference for disputes?)

In the EU SOFIE[[1]](#footnote-1) project, interledger is used in various ways [Lag19]. For example, agricultural supply chain use case stores hash of private transactions to public ledger using interledger, to provide immutability for private transactions and help with dispute resolutions as described in Section 5.1. 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 interledger 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, interledger is useful for any kind of situation where trust, transparency, and automation is required between multiple parties. These include sharing cybersecurity information [Nei2020] or automating disclosure of software vulnerabilities [Lag2020].

SOFIE project has released an interledger implementation[[2]](#footnote-2) written in Python supporting Ethereum, Hyperledger Fabric, and Guardtime KSI ledgers. The implementation connects any two ledgers: after a certain trigger occurs on one ledger, the transaction is sent to another ledger.

[Lag2019] 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.

[Nei2020] 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.

[Lag2020] 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.

* SOFIE Interledger use cases
	+ food-supply-chain:
		- storing hashes of transactions (of a private ledger, even db) to a public DL
		- hierarchical DLT solutions
	+ context aware mobile gaming ecosystem
* SOFIE Interledger component implementation

# 9. PDL INTEROPERABILITY REQUIREMENTS

9.1 Who will interoperate with

9.2. What information do you need to exchange

9.3. Which are the operations allowed

9.4. Traceability

9.5. Future-proof

9.6. Minimal viable governance

1. ***<https://www.sofie-iot.eu/>***  [↑](#footnote-ref-1)
2. ***<https://github.com/SOFIE-project/Interledger>***

 [↑](#footnote-ref-2)