ETSI GR PDL 018 V1.1.1 (2023-04)

Permissioned Distributed Ledger (PDL); Redactable Distributed Ledgers

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI GR PDL 018 V1.1.1 (2023-04)
https://standards.iteh.ai/catalog/standards/sist/96b7cbad-ce61-4d18-a229-5967510deb65/etsi-gr-pdl-018-v1-1-1-2023-04

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-0018_redactable_DL

Keywords
PDL, privacy

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

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

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 2023.
All rights reserved.

Contents

ETSI STANDARD PREVIEW
https://standards.iteh.ai/catalog/standards/sist/...

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

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

https://standards.iteh.ai/catalog/standards/sist/96b7cbad-ce61-4d18-a229-5967510deb65/etsi-gr-pdl-018-v1-1-1-2023-04

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.

1 Scope

The present document describes the definition of redactable distributed ledgers, presents use cases where redactable distributed ledgers are useful, and assesses existing solutions of redactable distributed ledgers. The present document also discusses potential standardization areas for enabling, managing, and using redactable distributed ledgers.

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.

iTeh STANDARD PREVIEW
ETSI GR PDL 018 V1.1.1 (2023-04)
https://standards.iteh.ai/catalog/standards/etsi-gr-pdl-018-v1-1-1-2023-04

[i.1] D. Zhang, J. Le, X. Lei, T. Xiang, and X. Liao: "Exploring the Redaction Mechanisms of Mutable Blockchains: A Comprehensive Survey", International Journal of Intelligent Systems, vol. 36, no. 9, 2021, pp. 5051-5084.

[i.2] G. Ateniese, B. Magri, D. Venturi, and E. Andrade: "Redactable Blockchain - or - Rewriting History in Bitcoin and Friends", 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 2017, pp. 111-126.

[i.3] Y. Sompolinsky, S. Wyborski, and A. Zohar: "PHANTOM GHOSTDAG: A Scalable Generalization of Nakamoto Consensus", In Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT '21). Association for Computing Machinery, September 2, 2021, New York, NY, USA, 57-70.

[i.4] IoTA 2.0 Research Specificaiton, June 4, 2021.

[i.5] M. Mehar, et al.: "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack", Journal of Cases on Information Technology (JCIT), 21(1), pp. 19-32, November 26, 2017.

[i.6] ETSI GR PDL 004: "Permissioned Distributed Ledgers (PDL); Smart Contracts; System Architecture and Functional Specification".

[i.7] ETSI GS PDL 011: "Permissioned Distributed Ledger (PDL); Specification of Requirements for Smart Contracts' architecture and security".

[i.8] I. Puddu, A. Dmitrienko, and S. Capkun (2017): "μChain: How to Forget without Hard Forks".

[i.9] D. Deuber, B. Magri and S. A. K. Thyagarajan: "Redactable Blockchain in the Permissionless Setting", 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 124-138.

[i.10] K. D. Richard: "A Data Structure for Integrity Protection with Erasure Capability", NIST Cybersecurity Whitepaper, May 20, 2022.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

hashing collision: scenario where two different input messages get the same hashing value using the same hashing function

Redactable Distributed Ledger (RDL): distributed ledgers where the stored content or objects can be modified with consensus through certain redaction operations

NOTE: A survey on mechanisms for mutable blockchains is presented in [i.1].

redactable objects: objects on distributed ledgers with the redaction property

redaction: property for supporting changes to one or multiple objects on distributed ledgers

redaction operations: actions or operations to change redactable objects on distributed ledgers

NOTE: To modify, to delete, and/or to insert one or multiple redactable objects on distributed ledgers.

Trapdoor-Controlled Hash (TCH): hashing scheme with two modes:

1) collision-free one-way hashing without using a trapdoor key to map an input message to a unique hashing value, which is the typical mode in traditional collision-free hashing schemes; and
2) using a trapdoor key to cause a hashing collision (i.e. to cause the same hashing value for two different input messages)

NOTE: Chameleon hash, as described in [i.2], is an example of trapdoor-controlled hash schemes.

Trapdoor Key (TK): secret key that allows the owner of this secret key to generate a hashing collision for two different input messages

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/96b7cbad-ce61-4d18-a229-5967510deb65/etsi-gr-pdl-018-v1-1-1-2023-04

3.2 Symbols

Void.

3.3 Abbreviations

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

DAG	Directed Acyclic Graph
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
ISG	Industry Specification Group
PDL	Permissioned Distributed Ledger
PK	Public Key
PKi	Public Key i
RDL	Redactable Distributed Ledger
TCH	Trapdoor-Controlled Hash
TK	Trapdoor Key
TXN	Transaction

4 Introduction to Redactable Distributed Ledger

4.1 Introduction

Distributed Ledger Technology (DLT) systems have been evolving.

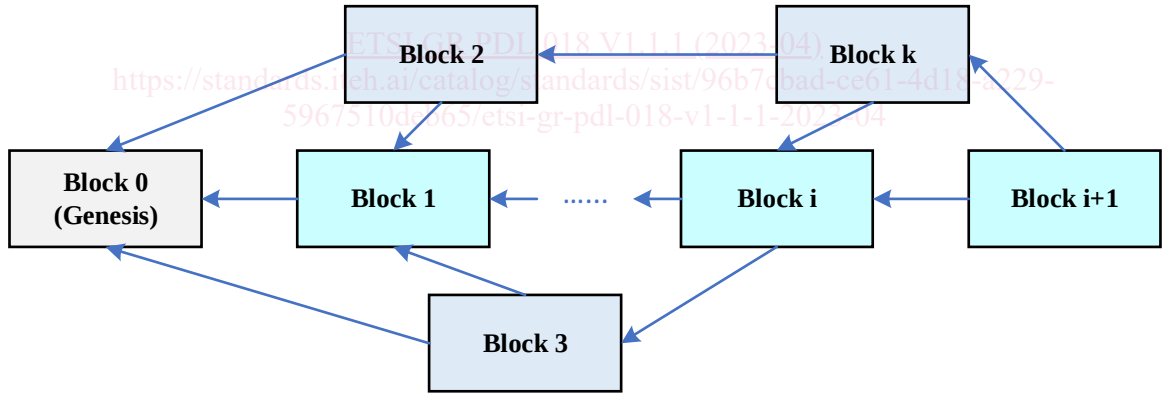
EXAMPLE 1: Distributed ledgers can be formed in different structures as illustrated in figure 4.1-1, such as blockchain (e.g. Bitcoin™, Ethereum™, Hyperledger Fabric™), block Directed Acyclic Graph (DAG) (e.g. PPHANTOM as described in [i.3]), and blockless DAG (e.g. IoTA as described in [i.4]). In general, DLT brings unique characteristics and advantages such as immutability, transparency and decentralization.

1) **Blockchain:** A linear topology with a set of chained blocks starting from the first genesis block. Each block (except the genesis block) has one and only one parent block.

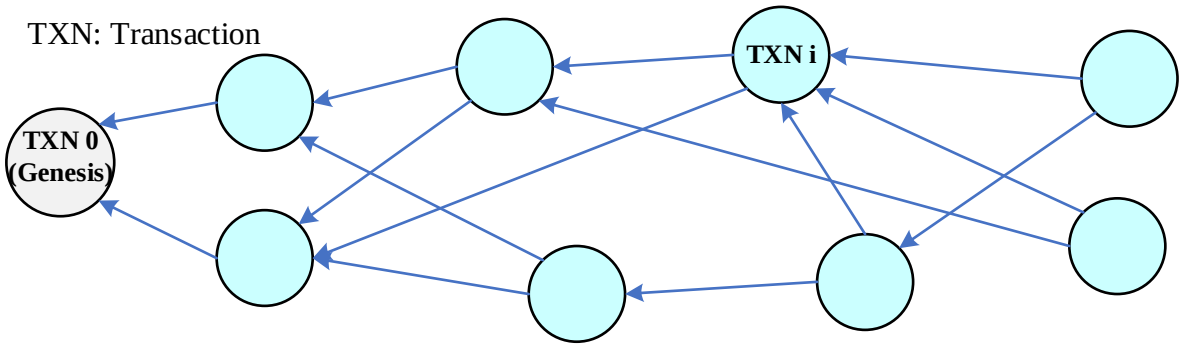
2) **Block DAG:** Blocks are organized in a DAG, where each node represents a block. Usually, each block (except the genesis block) has more than one parent blocks. Two or more blocks are connected if the corresponding two nodes are connected in the DAG.

3) **Blockless DAG:** Transactions are directly organized in a DAG, where each node represents a transaction. Usually, each transaction (except the genesis transaction) has more than one parent transactions. Two or more transactions are connected if the corresponding two nodes are connected in the DAG.

(a) Blockchain



(b) Block DAG



(c) Blockless DAG

Figure 4.1-1: Structures of Distributed Ledgers

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI GR PDL 018 V1.1.1 (2023-04)
https://standards.iteh.ai/catalog/standards/sist/96b7c...ad-ce61-4d18-a229-5967510de365/etsi-gr-pdl-018-v1-1-1-2023-04

DLT-based solutions are usually characterized by being immutable, tamper-proof, and decentralized, making them outperform centralized counterpart systems. Such unique characteristics of DLT fit perfectly with any decentralized applications, where trust is an issue.

EXAMPLE 2: Blockchain guarantees the integrity and security of financial transactions in the economic sector by preventing double-spending frauds and protecting users' assets from being tampered with.

4.2 Limitations of Immutable Ledgers

The unique characteristics of DLT (especially immutability) could be misused and lead to potential issues. Figure 4.2-1 illustrates some potential limitations of immutable ledger structure:

1) Information published by users on distributed ledgers may become sensitive and create privacy concerns in the future, especially in public DLT systems. Such privacy-concerned information cannot be removed from distributed ledgers due to their immutability, therefore contradicting "the right to be forgotten" associated with General Data Protection Regulation (GDPR).

2) Misinformation could be added to the distributed ledgers by attackers and stay there forever.

3) Crypto criminals and hackers can inject illegal contents forbidden by national or international laws into distribute ledgers, which cannot be removed.

4) Bogus smart-contracts, and more specifically bogus Decentralized Autonomous Organization (DAO) smart-contracts, can be exploited and immutability limits the ability to rectify such problems. E.g. DAO applications, the most significant smart contract applications in the Ethereum™ platform, are another example of immutability misuse. Hackers and crypto criminals discovered logical flaws and vulnerabilities in DAO smart contracts that led to transferring over US$ 120,3 million worth of Ethereum™ coins to their accounts as reported in [i.5], which could have been avoided if such flawed smart contracts had been modified. This problem was semi-cured by hard forking Ethereum™ blockchain back in 2016 to delete the attackers' transfer transactions.

5) Finally, immutability unavoidably causes a scalability issue in maintaining the append-only and ever-growing chain-length of distributed ledgers.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI GR PDL 018 V1.1.1 (2023-04)
https://standards.iteh.ai/catalog/standards/sist/96b7cbad-ce61-4d18-a229-

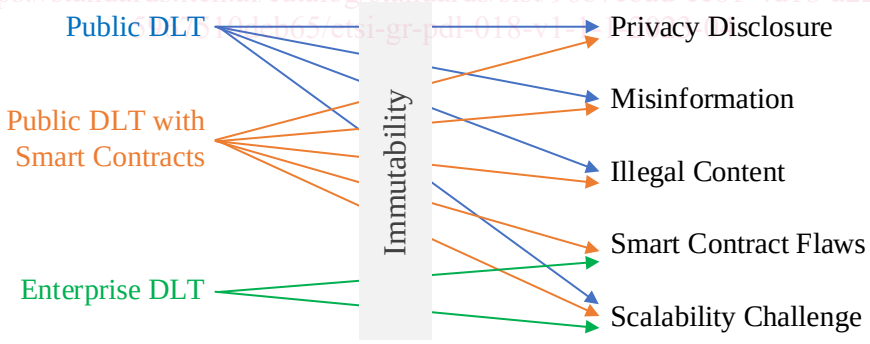


Figure 4.2-1: Potential Limitations with Immutable Distributed Ledgers

4.3 Redaction Operations

4.3.1 Introduction

Redaction operations could be different for different structures of distributed ledgers,. Even if it is possible to apply the same redaction operation on different distributed ledger structures, the complexity and implications of the redaction operation could still be different.

4.3.2 Redaction Operations for Blockchain

4.3.2.1 Types of Blockchain Redaction Operations

Redaction operations for blockchain-based distributed ledgers are: transaction-level redaction operations, single-block-level redaction operations, and multiple-block-level redaction operations.

4.3.2.2 Transaction-Level Redaction Operations

4.3.2.2.1 Changes Caused by Transaction-Level Redaction Operations

These redaction operations aim to impose changes on one or multiple existing transactions being included in an existing block and/or add new transactions. The modification of these transactions within the same block will automatically change:

1) the fingerprint (e.g. the Merkle tree root) of all transactions;
2) the content of this block; and
3) the hash value of this block.

4.3.2.2.2 Scope of Transaction-Level Redaction Operations

Transaction-level redaction operations include:

1) modification of an existing transaction, which could be any one or multiple fields of the existing transaction;
2) removal of an existing transaction from the corresponding block;
3) insertion of a new transaction to an existing block;
4) modification of more than one existing transaction from the corresponding block;
5) removal of more than one existing transactions from the corresponding block; and
6) insertion of multiple transactions to an existing block.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI GR PDL 018 V1.1.1 (2023-04)
https://standards.iteh.ai/catalog/standards/sist/...d18-a229-5967510deb65/etsi-gr-pdl-018-v1-1-1-2023-04

4.3.2.3 Single-Block-Level Redaction Operations

These redaction operations are used to change an existing block or introduce a new block. The change of the existing block will change the hash value of the existing block. The introduction of new block needs to deal with how to maintain the hash-based blockchain structure. Single-blockchain-level redaction operations include:

1) modification of non-transaction-related fields of an existing block;
2) removal of an existing block; and
3) insertion of a new block to an existing blockchain (not to append the new block to the existing blockchain).

4.3.2.4 Multiple-Blocks-Level Redaction Operations

These redaction operations are used to introduce changes related to multiple blocks, such as:

1) removal of multiple existing consecutive blocks;
2) removal of multiple existing non-consecutive blocks, which will essentially be using "Single-Block-Level Redaction Operations";
3) insertion of multiple new blocks in a consecutive order to an existing blockchain (not to append blocks to existing blockchain); and
4) insertion of multiple new blocks in a non-consecutive order to an existing blockchain (not to append blocks to existing blockchain).

4.3.3 Redaction Operations for Block DAGs

4.3.3.1 Types of Block DAG Redaction Operations

Redaction operations for a block DAG are similar to redaction operation to a blockchain and include the following: transaction-level redaction operations, single-block-level redaction operations, and multiple-block-level redaction operations.

4.3.3.2 Transaction-Level Redaction Operations

They are the same as transaction-level redaction operations for a blockchain as descried in clause 4.3.2.2.

4.3.3.3 Single-Block-Level Redaction Operations

These redaction operations are used to change an existing block or introduce a new block. Each node on a block DAG represents an existing block. Since an existing block in a block DAG may be a child node of multiple parent nodes and/or a parent node of multiple child nodes, to change an existing block or to insert a new block needs to consider any impact and implications to its child and/or parent nodes. Blockchain-level redaction operations for a block DAG include:

1) modification of non-transaction-related fields of an existing block;
2) removal of an existing block; and
3) insertion of a new block to the existing block DAG (not to append the new block to the existing block DAG).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.3.3.4 Multiple-Blocks-Level Redaction Operations

These redaction operations are used to introduce changes related to multiple blocks, such as:

1) removal of multiple existing connected blocks;
2) removal of multiple existing non-connected blocks;
3) insertion of multiple new blocks in a connected sub-graph to an existing block DAG (not to append blocks to existing block DAG); and
4) insertion of multiple new blocks in a non-connected way to an existing block DAG (not to append blocks to existing block DAG).

ETSI GR PDL 018 V1.1.1 (2023-04)
https://standards.iteh.ai/catalog/standards/sist/96b7cbad-ce61-4d18-a229-

4.3.4 Redaction Operations for Blockless DAGs

Redaction operations for blockless DAGs are transaction-level only, since transaction is the only object unit in a blockless DAG. Each node on a blockless DAG represents an existing transaction. Since an existing transaction in a blockless DAG may be a child node of multiple parent nodes and/or a parent node of multiple child nodes, when changing an existing transaction or inserting a new transaction any impact and implications to its child nodes and/or parent nodes needs to be considered and addressed.

The following redaction operations are possible for a blockless DAG:

1) modification of an existing transaction, which could be any one or multiple fields of the existing transaction;
2) removal of an existing transaction from the current blockless DAG;
3) insertion of a new transaction to the current blockless DAG;
4) modification of multiple connected transactions from the current blockless DAG;
5) removal of multiple connected transactions from the corresponding block; and
6) insertion of multiple connected transactions to the current blockless DAG (not to append them as leaf nodes).