ETSI GR PDL 018 V0.0.2 (2022-09)

Redactable Distribued Ledgers

***Disclaimer***

The present document has been produced and approved by the Permissioned Distributed Ledger 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.

**Group Report**

Reference

DGR/PDL-018\_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:
<http://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](http://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>

***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***

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

© ETSI 2022.

All rights reserved.

Contents

Intellectual Property Rights 4

Foreword 4

Modal verbs terminology 4

1 Scope 5

2 References 5

2.1 Normative references 5

2.2 Informative references 5

3 Definition of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 6

4 Introduction to Redactable Distributed Ledger 6

4.1 Introduction 6

4.2 Issues with Immutable Ledgers 6

4.3 Redaction Operations 6

5 Use Cases for Redactable Distributed Ledgers 6

5.1 Introduction 6

5.2 Self-Sovereign Identity (SSI) 6

5.3 Metaverse 6

5.4 Wireless and Mobile Networks 6

6 Existing Solutions of Redactable Distributed Ledger 7

6.1 Introduction 7

6.2 Chameleon Hash (CH) 7

6.3 CH-based Redactable Blockchain 7

6.3.1 Blockchain Redaction Process 7

6.3.2 Blockchain Redaction Management 7

6.4 Policy-based Redactable Blockchain 7

6.5 Redaction Using New Block Structures 7

6.6 Comparisons among Existing Redactable Blockchain Schemes 7

7 Potential Issues with Redactable Distributed Ledger 7

8 Conclusions and Next Steps 7

History 8

# 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](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.

# 1 Scope

This document will describe the definition of redactable distributed ledgers, presents use cases where redactable distributed ledgers are useful, and assesses existing solutions of redactable distributed ledgers. This 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.

[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, doi: 10.1109/EuroSP.2017.37.

[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 (https://doi.org/10.1145/3479722.3480990)

[i.4] S. Popov, “The Tangle,” White Paper Version 1.4.3, April 30, 2018 (http://www.descryptions.com/Iota.pdf)

[i.5] R. Kuhn, “A Data Structure for Integrity Protection with Erasure Capability,” NIST Cybersecurity Whitepaper CSWP 25, May 20, 2022 (https://csrc.nist.gov/publications/detail/white-paper/2022/05/20/data-structure-for-integrity-protection-with-erasure-capability/final)

[i.6] 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 (https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3014782).

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

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

**Chameleon Hash:** A 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).

**Hashing Collision:** The scenario where two different input messages gets the same hashing value using the same hashing function.

**Redaction:** A property for supporting changes to one or multiple objects on distributed ledgers.

**Redactble Objects:** The objects on distributed ledgers with the redaction property.

**Redaction Operations:** The actions or operations to change reactable objects on distributed ledgers.

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

**Redactable Distributed Ledgers:** Distributed ledgers that can be changed with certain redaction operations.

**Trapdoor Key:** A secret key that allows the owner of this secret key to generate a hashing collision for two different input messages.

## 3.2 Symbols

Void.

## 3.3 Abbreviations

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

CH Chameleon Hash

DAG Directed Acyclic Graph

DAO Decentralized Autonomous Organization

ETSI European Telecommunications Standards Institute

EU European Union

GDPR General Data Protection Regulation

PDL Permissioned Distributed Ledger

RDL Redactable Distributed Ledger

TXN Transaction

# 4 Introduction to Redactable Distributed Ledger

## 4.1 Introduction

Editor’s Note: This part could be reduced, especially if other sections 5 & 6 is not significantly longer than section 4 or if the details of those ledger structures can not be efficiently covered in sectoons 5 and 6. Check if there is any differences among those structures from redaction perspective.

Distributed Ledger Technology (DLT) systems have been evolving. For example, distributed ledgers can be formed in different structures as illustrated in **Figure 4.1-1**, such as blockchain (e.g., BitcoinTM, EthereumTM, Hyperledger FabricTM), block Directed Acyclic Graph (DAG) (e.g., PPHANTOM [i.3]), and blockless DAG (e.g., IoTA [i.4]), and block matrix [i.5]. In general, DLT brings unique characteristics and advantages such as immutability, transparency, and decentralization.

* Blockchain: A linear topology with a set of chained blocks starting from the first geneiss block. In other words, each block (except the genesis block) has one and only one parent block.
* Block DAG: Blocks are organized in a DAG. Usually, each block (except the genesis block) has more than one parent blocks.
* Blockless DAG: Transactions are directly organized in a DAG. Usually, each transaction (except the genesis transaction) has more than one parent transactions.
* Block Matrix: Blocks are organized in a matrix, where each column has some blocks and each row has some blocks. In other words, each block is indexed by a combination of a colum index and a row index.



(a). Blockchain



(b). Block DAG



(c) Blockless DAG



(d) Block Matrix

**Figure 4.1-1: Structures of Distributed Ledgers**

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. For example, 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 Issues with Immutable Ledgers

However, these unique characteristics of DLT (especially immutability) could be misused and lead to some potential issues. **Figure 4.2-1** illustrates the potential issues and limitations of immutable ledger structure.

* First, some information published by normal users on the distributed ledgers may become sensitive and cause privacy concerns in the future, especially in public DLT systems; however, such privacy-concerned information cannot be removed from the distributed ledgers due to its immutability, which prevents “rights to be forgotten” as described in General Data Protection Regulation (GDPR).
* Similarly, misinformation could be added to the distributed ledgers by attackers and stay there forever.
* Third, crypto criminals and hackers could inject into distribute ledgers illegal contents forbidden by national or international laws.
* Decentralized Autonomous Organization (DAO) applications, the most significant smart contract applications in the EthereumTM platform, are another example of immutability misuse. Hackers and crypto criminals discovered logical flaws and vulnerabilities in the DAO smart contracts that led to transferring over $120.3 million worth of EthereumTM coins to their accounts [i.6], which could have been avoided if such flawed smart contracts had been modified. This problem was semi-cured by hard forking EthereumTM blockchain back in 2016 to delete the attackers’ transfer transactions.
* Finally, the immutability unavoidably causes a scalability issue in maintaining the append-only and ever-increasing distributed ledgers.



Figure 4.2-1: Potential Issues and Limitations from Immutable Distributed Ledger

## 4.3 Redaction Operations

**Editor’s Note:** To discuss possible operations to redact/change/modify distributed ledgers: 1) modify a block; 2) Remove one or multiple blocks; 3) Insert one or multiple blocks; 4) modifty a transaction; 5) remove a transaction;

# 5 Use Cases for Redactable Distributed Ledgers

## 5.1 Introduction

Redactble distributed ledgers are useful for some applications asuch as self-soverign and disitributed identity, immersive experience, and future wireless systems.

## 5.2 Self-Sovereign Identity (SSI)

## 5.3 Immersive Experience

Editor’s Note: Need to well define “Metaverse”. May consider “immesive experience” or other terms/scenarios.

## 5.4 Wireless and Mobile Networks

# 6 Existing Solutions of Redactable Distributed Ledger

Editor’s Note: Need to be cautious and avoid advertising a particular solution.

## 6.1 Introduction

## 6.2 Chameleon Hash (CH)

## 6.3 CH-based Redactable Blockchain

### 6.3.1 Blockchain Redaction Process

### 6.3.2 Blockchain Redaction Management

## 6.4 Policy-based Redactable Blockchain

## 6.5 Redaction Using New Block Structures

# 7 Potential Issues with Redactable Distributed Ledger

## 7.1 Introduction

## 7.2 Comparisons among Existing Redactable Blockchain Schemes

# 8 Conclusions and Next Steps

Editor’s Note: Provide “recommendations” for next steps.

# History

|  |
| --- |
| **Document history** |
| v0.0.1 | 18 Jul 2022 | Creation of document, TOC and high-level content |
| V0.0.2 | 27 Sept 2022 | PDL(22)000\_125r2 |
|  |  |  |
|  |  |  |
|  |  |  |