

ETSI GR PDL 032 V1.1.1 (2025-04)



Permissioned Distributed Ledger (PDL); Artificial Intelligence for Permissioned Distributed Ledger (<https://standards.iteh.ai>) Document Preview

[ETSI GR PDL 032 V1.1.1 \(2025-04\)](https://standards.iteh.ai/catalog/standards/etsi/6aab136d-e01a-486e-be02-7a182cbe6743/etsi-gr-pdl-032-v1-1-1-2025-04)

<https://standards.iteh.ai/catalog/standards/etsi/6aab136d-e01a-486e-be02-7a182cbe6743/etsi-gr-pdl-032-v1-1-1-2025-04>

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-0032_AI_4PDL

Keywords

artificial intelligence, identity, PDL, scalability,
security

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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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 2025.
All rights reserved.

Contents

Intellectual Property Rights	8
Foreword.....	8
Modal verbs terminology.....	8
Executive summary	8
Introduction	9
1 Scope	11
1.1 Description	11
1.2 In scope	11
1.3 Not in scope of the present document	11
2 References	12
2.1 Normative references	12
2.2 Informative references.....	12
3 Definition of terms, symbols and abbreviations.....	19
3.1 Terms.....	19
3.2 Symbols.....	21
3.3 Abbreviations	21
4 Enhancing PDL security using AI-based methods.....	22
4.1 Introduction	22
4.2 AI-Powered Anomaly Detection and Threat Identification in Real-Time.....	23
4.2.1 Problem statement	23
4.2.2 Using AI for Anomaly Detection and Real-Time Threat Detection	23
4.2.3 Real-Time Monitoring and Analysis	23
4.2.4 Pattern Recognition and Behavioural Analysis	24
4.2.5 Adaptive Threat Detection.....	24
4.2.6 Automated Response Mechanisms	24
4.3 Enhanced Fraud Detection through Machine Learning Algorithms.....	24
4.3.1 Problem statement	24
4.3.2 Using AI to detect fraud.....	25
4.3.3 Sophisticated Pattern Analysis.....	25
4.3.4 Anomaly-Based Fraud Detection.....	26
4.3.5 Predictive Fraud Analytics.....	26
4.3.6 Continual Learning and Improvement	26
4.3.7 Reduced False Positives.....	27
5 Smart contract optimization using AI.....	27
5.1 Introduction	27
5.2 AI-Driven Smart Contract Code Analysis and Optimization	27
5.2.1 Problem statement	27
5.2.2 Using AI to handle such challenges.....	27
5.2.3 Static Code Analysis.....	28
5.2.4 Performance Optimization.....	28
5.2.5 Security Enhancement	29
5.2.6 Code Generation and Refactoring.....	29
5.2.7 Natural Language Processing for Documentation	29
5.3 Automated Testing and Verification of Smart Contracts	30
5.3.1 Problem statement	30
5.3.2 Tools for Improving reliability and reducing the risk of errors	30
5.3.3 Automated Test Case Generation	30
5.3.4 Fuzzing and Mutation Testing	31
5.3.5 Formal Verification.....	31
5.3.6 Symbolic Execution.....	31
5.3.7 Continuous Integration and Deployment	31
5.3.8 Learning from Past Vulnerabilities.....	31

6	AI-Enhanced Consensus Mechanisms in Permissioned Distributed Ledger Systems	32
6.1	Consensus mechanisms for PDL functionality.....	32
6.2	AI-enhanced consensus algorithms for faster and more efficient agreement	32
6.3	Adaptive consensus mechanisms based on network conditions	33
7	Data analytics and insights using AI	33
7.1	Introduction and problem statement	33
7.2	Analysing Large Volumes of Transaction Data for Valuable Insights using AI	34
7.2.1	AI's capabilities to handle large volumes.....	34
7.2.2	Pattern Recognition and Trend Analysis	34
7.2.3	Anomaly Detection	34
7.2.4	Customer Segmentation and Personalization	35
7.2.5	Predictive Analytics	35
7.2.6	Real-time Processing and Decision Making	35
7.3	Predictive Analytics for Business Intelligence	35
7.3.1	Predictive Analytics capabilities of AI	35
7.3.2	Customer Behaviour Prediction	35
7.3.3	Sales Forecasting	36
7.3.4	Risk Assessment and Management.....	36
7.3.5	Demand Forecasting	36
7.3.6	Trend Analysis and Market Prediction	36
7.3.7	Operational Efficiency Optimization	36
7.3.8	Customer Lifetime Value Prediction	37
8	Privacy-preserving techniques using AI.....	37
8.1	Introduction and problem statement	37
8.2	Developing Advanced Privacy-Preserving Computation Methods using AI	38
8.3	Homomorphic Encryption and Secure Multi-Party Computation	38
8.4	Federated Learning	39
8.5	Differential Privacy in Machine Learning.....	39
8.6	Generative Adversarial Networks (GANs) for Synthetic Data.....	40
9	AI Tools for Network Optimization	41
9.1	Problem statement	41
9.2	Network Performance and Resource Allocation	41
9.3	Predictive Maintenance of Network Nodes.....	42
9.4	AI-Driven Network Topology Optimization	43
9.5	Intelligent Data Sharding.....	43
9.6	AI-Enhanced Network Security	43
9.7	Energy-Efficient Network Operations.....	44
9.8	AI-Powered Network Congestion Management.....	44
9.9	Adaptive Protocol Optimization.....	44
10	Governance and compliance using AI.....	45
10.1	Introduction and problem statement	45
10.2	AI Assisted Governance Rules and Compliance Checks Enforcement	45
10.3	AI Assisted Automated Auditing and Reporting	46
10.4	AI-Enhanced Governance Participation	47
10.5	Regulatory Compliance Monitoring	47
10.6	Intelligent Dispute Resolution.....	48
11	Identity management using AI	48
11.1	Introduction and problem statement	48
11.2	AI-Enhanced Identity Verification and Management Processes	49
11.2.1	AI-Powered Facial Recognition.....	49
11.2.2	AI-Powered Document Verification System	49
11.2.3	Anomaly Detection: AI-Powered Behavioural Biometrics for Continuous Authentication	49
11.3	Additional Scenarios and Examples	49
11.3.1	Federated Identity Management	49
11.3.2	Adaptive Access Control	50
11.3.3	Identity Recovery and Remediation.....	50
11.3.4	Decentralized Identity Verification.....	50
11.3.5	Cross-Chain Identity Management	50

12	AI-Assisted PDL Interoperability	51
12.1	PDL Interoperability in the context of AI - problem statement.....	51
12.2	AI-Facilitated Cross-Chain Communication and Data Exchange	51
12.3	Smart Routing of Transactions Between Different Ledgers.....	52
13	AI based PDL Scalability solutions.....	52
13.1	Problem statement	52
13.2	Developing More Efficient Scaling Solutions using AI.....	52
13.3	Dynamic Sharding Based on Network Traffic and Usage Patterns.....	53
14	Conclusion and Recommendations	53

Annex A: List of AI-tools referenced in the present document with brief descriptions and application for PDL55

A.1	Examples related to clause 4 (Enhanced security)	55
A.1.1	Examples of AI Algorithms for Continuous Monitoring.....	55
A.1.1.1	Temporal Graph Convolutional Networks (TGCNs).....	55
A.1.1.2	Federated Attention Mechanism with Differential Privacy	55
A.1.1.3	Hierarchical Long Short-Term Memory Networks with Adaptive Thresholding.....	56
A.1.2	Examples of Advanced Machine Learning Models for Pattern Recognition	57
A.1.2.1	Graph Neural Networks (GNNs)	57
A.1.2.2	Transformer-based Models	57
A.1.2.3	Deep Clustering Networks (DCNs)	58
A.1.3	Examples of Adaptive AI Systems for Evolving Threat Detection.....	58
A.1.3.1	Continual Learning Networks.....	58
A.1.3.2	Meta-Learning Systems	59
A.1.3.3	Reinforcement Learning for Adaptive Security.....	59
A.1.4	Examples of AI Systems for Automated Response Mechanisms in PDL Networks.....	60
A.1.4.1	Reinforcement Learning-based Autonomous Defence Systems	60
A.1.4.2	Federated Learning-based Collaborative Defence Systems.....	60
A.1.4.3	Explainable AI (XAI) for Automated Incident Response	61
A.1.5	Examples of AI-Based Machine Learning Models for Fraud Detection	61
A.1.5.1	Graph Neural Networks (GNNs) for Fraud Detection	61
A.1.5.2	Transformer-based Models for Sequential Fraud Detection.....	61
A.1.5.3	Federated Deep Learning for Privacy-Preserving Fraud Detection	62
A.1.6	Examples of unsupervised learning algorithms used to establish baseline behaviours	62
A.1.6.1	Graph Autoencoders (GAEs) for Network Behaviour Modelling	62
A.1.6.2	Variational Autoencoders (VAEs) for Anomaly Detection	63
A.1.6.3	Temporal Convolutional Networks (TCNs) for Time Series Analysis.....	63
A.1.7	Examples of Predictive Machine Learning Models for Fraud Detection	64
A.1.7.1	Graph Neural Networks (GNNs) with Temporal Attention.....	64
A.1.7.2	Transformer-based Models with Self-Supervised Pre-training.....	64
A.1.7.3	Federated Deep Learning with Differential Privacy	65
A.1.8	Examples of Continuous Learning Machine Learning Models for Fraud Detection.....	65
A.1.8.1	Online Adaptive Graph Neural Networks (OAGNNs)	65
A.1.8.2	Incremental Learning with Ensemble Methods	66
A.1.8.3	Federated Continual Learning.....	66
A.1.9	Examples of Machine Learning Models for Reducing False Positives in Fraud Detection	67
A.1.9.1	Attention-based Graph Neural Networks with Explainable AI	67
A.1.9.2	Hybrid Models Combining Anomaly Detection with Supervised Learning	67
A.1.9.3	Federated Learning with Adaptive Boosting	68
A.2	Examples related to clause 5 (Smart contract optimization using AI)	68
A.2.1	Examples of AI-Powered Static Code Analysis Tools	68
A.2.1.1	DeepCode	68
A.2.1.2	Infer®	69
A.2.1.3	CodeQL®.....	69
A.2.2	Examples of AI-Based Machine Learning Algorithms for Smart Contract Optimization.....	69
A.2.2.1	Deep Reinforcement Learning for Dynamic Gas Optimization.....	69
A.2.2.2	Graph Neural Networks with Attention for Code Pattern Recognition	69
A.2.2.3	Transformer-based Model with Transfer Learning for Cross-Language Optimization	70
A.2.2.4	Hyperledger Caliper®.....	70

A.2.2.5	OptSmart.....	70
A.2.3	Examples of AI Algorithms for Identifying Smart Contract Vulnerabilities.....	71
A.2.3.1	Graph Neural Networks (GNNs) with Semantic-Aware Embedding	71
A.2.3.2	Transformer-based Models with Transfer Learning	71
A.2.3.3	Reinforcement Learning with Symbolic Execution.....	71
A.2.4	Examples of AI Algorithms for Code Generation and Optimization in PDL Platforms	72
A.2.4.1	Large Language Models with Few-Shot Learning.....	72
A.2.4.2	Graph-to-Code Neural Networks with Attention.....	72
A.2.4.3	Hierarchical Transformers with Code Semantic Embedding.....	72
A.2.5	Examples of AI-Powered NLP Tools for Smart Contract Documentation.....	73
A.2.5.1	CodeBERT-based Documentation Generation	73
A.2.5.2	Graph-to-Sequence Neural Networks for Contract Summarization.....	73
A.2.5.3	Hierarchical Transformer with Code-Text Alignment.....	73
A.2.6	Examples of AI-Based Machine Learning Algorithms for Smart Contract Test Case Generation	74
A.2.6.1	Deep Reinforcement Learning for Adaptive Fuzzing.....	74
A.2.6.2	Graph Neural Networks with Symbolic Execution.....	74
A.2.6.3	Transformer-based Models with Program Synthesis	74
A.2.7	Examples of AI-Driven Fuzzing Techniques for Smart Contract Testing.....	75
A.2.7.1	Reinforcement Learning-based Adaptive Fuzzing.....	75
A.2.7.2	Neuro-Symbolic Execution with Mutation	75
A.2.7.3	Evolutionary Fuzzing with Natural Language Processing (NLP).....	76
A.2.8	Examples of AI-Based Tools for Formal Verification of Smart Contracts	76
A.2.8.1	Neural-Guided Theorem Prover (NGTP)	76
A.2.8.2	Transformer-based Model Checker (TMC)	76
A.2.8.3	Graph Neural Network-based Invariant Synthesizer (GNNIS).....	77
A.2.9	Examples of AI-Enhanced Symbolic Execution Techniques for Smart Contract Analysis	77
A.2.9.1	Neural-Guided Symbolic Execution (NGSE)	77
A.2.9.2	Reinforcement Learning-based Concolic Testing (RLCT).....	78
A.2.9.3	Graph Neural Network-Enhanced Symbolic Execution (GNN-SE)	78
A.2.10	Examples of AI-Based Tools for Smart Contract DevSecOps Pipelines.....	78
A.2.10.1	SmartBugs: AI-Enhanced Vulnerability Detection Pipeline.....	78
A.2.10.2	ContractGuard: Automated Verification and Deployment Framework	79
A.2.10.3	AISeOps: AI-Driven Security Operations for Smart Contracts	79
A.2.11	Examples of AI Systems for Continuous Improvement in Smart Contract Security.....	80
A.2.11.1	VELMA: Vulnerability-driven Evolutionary Learning for Smart Contract Auditing	80
A.2.11.2	SCSCAN: Self-Correcting Smart Contract Vulnerability Scanner	80
A.2.11.3	ASTRAEA: Adaptive Smart conTRact Auto-Evaluation and Auditing	80
A.3	Examples related to clause 8: Privacy-preserving techniques.....	81
A.3.1	Examples of Federated Learning	81
A.3.1.1	PySyft	81
A.3.1.2	Flower	81
A.3.1.3	OpenFL.....	81
A.3.1.4	FedML	81
A.3.2	Examples of Differential Privacy in Machine Learning.....	81
A.3.2.1	Differentially Private Stochastic Gradient Descent (DP-SGD)	81
A.3.2.2	Differentially Private Follow The Regularized Leader (DP-FTRL).....	82
A.3.2.3	Gaussian Differential Privacy (GDP)	82
A.3.3	Examples of Generative Adversarial Networks (GANs) for synthetic data generation	82
A.3.3.1	Privacy-Preserving Synthetic Data Generation Using Conditional GANs	82
A.3.3.2	TabFairGAN: Fair Tabular Data Generation with Generative Adversarial Networks.....	83
A.3.3.3	SynSig: Generating Synthetic Signatures for Large-Scale Time Series Anomaly Detection	84
A.4	Examples related to clause 11 (Identity management using AI)	85
A.4.1	AI-Powered Facial Recognition	85
A.4.1.1	Description.....	85
A.4.1.2	Use Case	85
A.4.2	AI-Powered Document Verification System	85
A.4.2.1	Description.....	85
A.4.2.2	Key components	85
A.4.2.3	Process	86
A.4.2.4	Performance.....	86

A.4.3	Anomaly Detection: AI-Powered Behavioural Biometrics for Continuous Authentication.....	86
A.4.3.1	Description.....	86
A.4.3.2	Examples	86
A.4.3.3	Application	87
A.4.3.4	Key Advantages.....	87
A.5	Examples and recent research related to clause 12 (AI-Assisted PDL Interoperability).....	87
A.5.1	AI-Facilitated Cross-Chain Communication and Data Exchange	87
A.5.1.1	Examples of AI applications in cross-chain communication	87
A.5.1.2	Recent research in this area.....	87
A.5.2	Examples of AI applications in Smart Routing of Transactions Between Different Ledgers	88
A.5.2.1	Reinforcement Learning for Optimal Path Finding	88
A.5.2.2	Predictive Analytics for Network Congestion	88
A.5.2.3	Federated Learning for Collaborative Routing Optimization	88
A.5.2.4	Graph Neural Networks for Dynamic Topology Analysis.....	88
A.5.2.5	Multi-Agent Systems for Decentralized Routing.....	88
A.5.3	Additional Scenarios and Examples	88
A.6	Examples and recent research related to clause 13 (AI based PDL Scalability solutions).....	89
A.6.1	Developing More Efficient Scaling Solutions using AI	89
A.6.1.1	Adaptive Consensus Optimization.....	89
A.6.1.2	Intelligent Sharding.....	89
A.6.1.3	Smart Contract Parallelization	89
A.6.1.4	Predictive Caching	89
A.6.1.5	Network Topology Optimization	89
A.6.2	Dynamic Sharding Based on Network Traffic and Usage Patterns	90
A.6.2.1	Predictive Sharding.....	90
A.6.2.2	Adaptive Shard Allocation.....	90
A.6.2.3	Intelligent Cross-Shard Transaction Management.....	90
A.6.2.4	Anomaly-Aware Sharding	90
A.6.2.5	Federated Learning for Collaborative Sharding.....	90
A.6.3	Additional Scenarios and Examples	90
History	92

ETSI GR PDL 032 V1.1.1 (2025-04)

<https://standards.iteh.ai/catalog/standards/etsi/gr-pdl-032-v1.1.1-2025-04>