***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 PDL-021 V0.0.1 (2023-02)

**Group REPORT**

Permissioned Distributed Ledger (PDL);

Overview of Use Cases in 3GPP Network and Impact Analysis on Architecture Integration

<

Reference

DGR/PDL-0021\_usecase\_3GPP Net

Keywords

Distributed Ledger, 3GPP, Core Network

***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>

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 yyyy.

All rights reserved.

Contents

Intellectual Property Rights 5

Foreword 5

Modal verbs terminology 5

Executive summary 5

Introduction 5

1 Scope 6

2 References 6

2.1 Normative references 6

2.2 Informative references 6

3 Definition of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Review of Use Cases Related to 3GPP Networks 7

4.1 Relevant Organizations 7

4.1.1 ISO: 7

4.1.2 ITU-T: 8

4.1.3 IEEE: 8

4.1.4 IMT-2030: 9

4.1.5 IETF: 9

4.2 Use Cases 9

4.2.1 Infrastructure Management 9

4.2.1.1 Telecom Network Asset Manegement 9

4.2.1.2 Network Co-construction 9

4.2.2 Logging and Multi-party Transparency 9

4.2.2.1 Network KPI Records 9

4.2.2.2 UE Profile Records 9

4.2.2.3 UE Behaviors 10

4.2.2.4 Federated Learning Model Verification 10

4.2.2.5 Operation Log Audit 10

4.2.2.6 Charging 10

4.2.3 Network Security Management 10

4.2.3.1 Device Certificate Management and Cross-Domain Authentication 10

4.2.3.3 Credential & Access Management. 11

4.2.3.4 Decetralized Identity Management 11

4.2.4 Resource Sharing and Exposure 11

4.2.4.1 Operators’ Data Sharing 11

4.2.4.2 Compute & Storage Resources Sharing 11

4.2.4.3 Digital Asset Sharing 11

4.2.4.4 Spectrum Resource Sharing 11

4.2.4.5 Network Slicing 11

4.2.4.6 Sensing Data 12

4.2.5 Vertical Application Support 12

4.2.5.1 V2X 12

4.2.5.2 Other Verticals 12

4.3 Summary 13

5 Gap Analysis 13

Key Issue 1: Nativeness of PDL in 3GPP Network 13

Key Issue 2: Impact of PDL on Protocol Stack in 3GPP Network 13

Key Issue 3: High Throughput 14

Key Issue 4: Data Sovereignty for 3GPP System Users 14

Key Issue 5: Sustanability 14

6 Potential Impacts to 3GPP Network Architecture 14

Conclusion 15

Annex A: Title of annex 16

Annex B: Title of annex 17

B.1 First clause of the annex 17

B.1.1 First subdivided clause of the annex 17

Annex: Bibliography 18

Annex : Change History 19

History 20

# 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](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 <long ISGname> (<short ISGname>).

# 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.

# Executive summary

# Introduction

# 1 Scope

The present document will first provide an overview of use cases/scenarios of PDL specific to mobile networks, based on the deliverables published in major existing standardization bodies. It aims to form a common view to summarize the key benefits of PDL technology to mobile network domain (including its operation controls and services);

Within one or multiple operators, utilizing PDL technology can be widely adopted in different domains (e.g., ranging from end users, RAN/core network to service providers) of a mobile network system and different layers (e.g., data flow layer, management layer and business layer), thus this WI will further identify several key issues / challenges / deficiencies to specialize PDL solutions to a mobile network system and its essential impact to the mobile network system architecture, which could refer 3GPP 5G architecture as a base;

Some WIs already show an initial try by introducing a new network entity in mobile networks to connect to PDL services, this WI will comprehensively investigate if there will be any necessity to make modifications to the mobile network system architecture (starting with 3GPP 5G reference architecture) in order to integrate PDL in a holistic way.

# 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] <Standard Organization acronym> <document number><version number/date of publication>: "<Title>".

[i.2] etc.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the [following] terms [given in ... and the following] apply:

TBD

## 3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

TBD

## 3.3 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

TBD

# 4 Review of Use Cases Related to 3GPP Networks

This clause details key issues related to the integration of 3GPP functions and architectures with blockchain. Each key issue defines the context of the issue, defines the challenges associated with the issue, and raises requirements to address or mitigate the key issue

## 4.1 Relevant Organizations

### 4.1.1 ISO:

|  |  |
| --- | --- |
| ISO/TC 307 | ISO 22739:2020：Blockchain and distributed ledger technologies — Vocabulary |
| ISO/TS 23258:2021：Blockchain and distributed ledger technologies — Taxonomy and Ontology |
| ISO/TR 23244:2020：Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations |
| ISO/TR 23455:2019：Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems |
| ISO/TR 23576:2020：Blockchain and distributed ledger technologies — Security management of digital asset custodians |
| ISO/DTR 3242: Blockchain and distributed ledger technologies – Use cases |
| ISO/WD TR 6039：Blockchain and distributed ledger technologies - Identifiers of subjects and objects for the design of blockchain systems |
| ISO/WD TR 6277：Blockchain and distributed ledger technologies – Data flow model for blockchain and DLT use cases |
| ISO/CD 22739：Blockchain and distributed ledger technologies — Vocabulary |
| ISO/FDIS 23257 :Blockchain and distributed ledger technologies — Reference architecture |
| ISO/AWI TS 23516:Blockchain and Distributed Ledger Technology — Interoperability Framework |
| ISO/WD TS 23259：Blockchain and distributed ledger technologies — Legally binding smart contracts |
| ISO/PRF TS 23635:Blockchain and distributed ledger technologies — Guidelines for governance |
| ISO/WD TR 23642:Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues |
| ISO/WD TR 23644:Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM) |
| ISO/AWI 7603：Decentralized Identity standard for the identification of subjects and objects |
| ISO/PRF TR 23249：Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management |

### 4.1.2 ITU-T:

|  |  |
| --- | --- |
| FG DLT | DLT terms and definitions |
| DLT use cases |
| DLT reference architecture |
| Assessment criteria for DLT platforms |
| DLT regulatory framework |
| H.DLT-FAM | Functional assessment methods for distributed ledger technology (DLT) platforms |
| X.BaaS-sec/SG17 | Guideline on DLT as a service (BaaS) security |
| H.DLT-GTI | DLT governance and technical interoperability framework |
| H.DLT-PAM | Performance assessment methods for distributed ledger technology (DLT) platforms |
| H.DLT-TEE | TEE-based confidential computing on distributed ledger technology system |
| H.DLT-TFI | Technical Framework for distributed ledger technology (DLT) Interoperability |
| H.DLT-TFR | Technical framework for DLT regulation |
| H.DLT-VERI | Formal verification framework for smart contract |
| H.DLT-INV | General framework of DLT-based invoices |
| F.DLT-DPT | Application Guideline for DLT-based Distributed Power Trading |
| TR\_DLT | Usage of Distributed Ledger Technology (DLT) to handle accounting, policy, regulatory and economic issues in the international telecommunications/ICT domain |
| Y.dec-IoT-arch | Decentralized IoT communication architecture based on information centric networking and blockchain |
| Y.BC-SON | Framework of blockchain-based self-organization networking in IoT environments |
| Y.frd | Framework and requirements of network- oriented data integrity verification service based on blockchain in future network |
| X.ss-dlt | Security services based on distributed ledger technology  |
| Q.BaaS-iop-reqts | Interoperability testing requirements of blockchain as a service |

### 4.1.3 IEEE:

|  |  |
| --- | --- |
| CTS/BSC/ CEWG | IEEE Standard for General Requirements for Cryptocurrency Exchanges |
| CTS/BSC/ CEWG | IEEE Standard for a Custodian Framework of Cryptocurrency |
| CTS/BSC/EIBCTWG | IEEE Published Draft Recommended Practice for E-Invoice Business Using Blockchain Technology |
| CTS/BSC/ CEWG | IEEE Standard for General Process of Cryptocurrency Payment |
| CTS/BSC/TIDMWG | IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management |
| C/BDL BSCF\_WG | Standard for the Use of Blockchain in Supply Chain Finance |
| CTS/BSC/ DBC | IEEE Standard for Data Format for Blockchain Systems |
| CTS/BSC/BCGOVWG | Standard for Framework and Definitions for Blockchain Governance |

### 4.1.4 IMT-2030:

|  |  |
| --- | --- |
| Network Group | 6G blockchain senarios and requirements |
| Network Group | 6G blockchain architecture and key technology  |

### 4.1.5 IETF:

*Editorial Note: TBD*

## 4.2 Use Cases

After having a thorough review on the deliverables of the existing SDOs listed in 4.1 Relevant Organizations, relevant use cases in 3GPP network system can be classified into five general use cases.

### 4.2.1 Infrastructure Management

In this general use case, PDL can be utilized for asset management such as Registration, Update and De-registration. Specifically, the assets of a telecom infrastructure can be physical network entities (e.g., gNB, networking elements and energy supply components) and virtual network entities (e.g., virtual machines, containers and so on). PDL can be used to build a comprehensive asset registry of the network domain.

#### 4.2.1.1 Telecom Network Asset Manegement

For a single domain owned by one network operator, PDL can facilitate the management process when involving a large number of categeries, amounts and lifecycles of various network entities, giving a global view of the whole infrastructure and even building a digital twin of the telecom network infrastructure.

#### 4.2.1.2 Network Co-construction

For a multi-domain scenario, the next generation telecom network infrastructure is expected to consist of infrastructure resources provided from different spectrum of infrastructure operators including (low-orbit) satellite operators, drone operators, IoT providers and terrestrial network operators. In other words, the definition of a telecom network infrastructure is largely generalized, i.e., not limited to an infrastructure of traditional carriers. In some cases, it may even include vertical customers, non-public network segements and end users. In this highly heterogeneous scenario, an efficient and decentralized accouting platform is required in order to guarantee the fairness of every participate contributing to the infrastructure construction. PDL can be a promising technology/standard to build such a platform.

### 4.2.2 Logging and Multi-party Transparency

Under this category, it can be further decomposed into the follow sub use cases.

#### Network KPI Records

Traditional network KPI data, especially the use of air interface KPI data, are based on a layer-by-layer reporting mechanism starting from local collection, aggregation to subnet management, subnet management then reporting to the high-level network management. This reporting mechanism may cause errors during the data transmission and storage or even be attacked. PDL can enable a novel network KPI data recording mechanism, where KPI data can be recorded in the first time, fast, efficient, tamper-proof record on the ledger with a pre-defined consensus protocol.

#### 4.2.2.2 UE Profile Records

As we know, a carrier operator stores massive UE subscription data, secure management of UE profile data is one of th key criteria evaluating the service provided from a carrier operator to its customers. Any loss or tamper of UE profile data may not only hurt customer’s privacy, but also cause law violation. Based on PDL technology, UE profile data can be stored in a decentralized manner, in which any error happening on a single storage node will not invalidate the data on the peer nodes. This largely enhances the resilience of the UE profile records.

#### 4.2.2.3 UE Behaviors

Similar to the UE profile records, UE behaviors data are operational data while a UE is active and uses a network service. UE behaviors are critical to the decision-making process if the operator has to adapt the network control in order to guarantee the user experience. This may not only happen in a single domain of a telecom network, but also across different network operators and/or application service providers. Therefore, sharing UE behaviour data is important when coordinations among different parties are required, which is not trivial without a trustworthy shared data layer. PDL can be a promising tool to build this shared data layer, where UE behaviour data are committed into the ledger and safely shared beyond the boundary of network domain.

#### 4.2.2.4 Federated Learning Model Verification

Federated Learning (FL) over a telcom network is a distributed learning (trainining) framework participated with multiple AI/ML agents, which could be mobile phones, edge computing nodes and network entities distributed in different network domains. In each stage such as data collection, data storage, model training and data sharing, a distributed agent can contribute and collaborate with other agents. However, FL suffers from multi-party trust issues such as data integrity, data history accountability, malicious training model tractability and incentive. PDL can solve or mitigate those issues by providing a shared ledger to create a tamper-proof data record ledger. With this ledger, participating AI/ML agents can rely on this ledger to interact with other agents; in addition, combining with cryptocurrency, an incentive mechanism can be established as well. Therfore, PDL can enhance FL framework in a telecom network environment.

#### 4.2.2.5 Operation Log Audit

Operational log is records of the operating status of the device, network, system, application and other operating conditions and the events generated during operation, and operational logs are critical to re-examine the efficiency, security risks and malicious behaviors of components running a telecom network system. In the security field, logs can reflect many attack behaviors, such as login errors, abnormal access, and vulnerability attacks. Log audit can obtain the security operation status of the system, identify attacks and intrusions against the information system, and log audit can also identify illegal operations and information leakage from the inside, so as to provide necessary information for post-event problem analysis and investigation and evidence collection, and use PDL to securely distribute the storage of logs, which can effectively prevent the single point failure of the log server and the illegal operation of malicious administrators.

#### 4.2.2.6 Charging

Charging audit is a cumbersome operation task especially when involving different parties. For a long time, multi-party charging accouting relies on a third party to audit the operational data so that credit invoices can be issued. With PDL, charging log data can be shared immediately and verified in a decentralized manner without a centralized third party. This significantly improves the efficiency of settlement among different parties.

### 4.2.3 Network Security Management

For security services, specifically, PDL can facilitate the follow sub use cases.

#### 4.2.3.1 Device Certificate Management and Cross-Domain Authentication

当前设备认证使用的为PKI系统，PKI系统的核心执行机构证书授权中心（Certificate Authority，CA）是中心化节点，集中式的CA存在被攻击风险，造成单点失效，某些小型运营商不具备运营CA的能力，或其自身CA自身可信性不高，造成跨域信任建立和证书认证的困难。PDL可以构建CA的信任联盟，运营商、设备商将自己与网络运营所需的数字证书，包括自己CA的数字证书， 通过联盟链的共识机制写入联盟链，提升CA的安全性、透明性和鲁棒性，提升跨域认证的效率。

At present, the equipment authentication uses a public key infrastructure (PKI), the core actuator of the PKI system is a Certificate Authority (CA), which is a centralized node. Therefor, a centralized CA has the risk of being attacked, resulting in a single point of failure, some small operators do not have the ability to operate CA, or their own CA itself is not highly credible, resulting in cross-domain trust establishment and certificate authentication difficulties. PDL can build a trust alliance of CAs, and operators and equipment vendors can write the digital certificates required for themselves and network operations, including the digital certificates of their own CAs, to the consortium chain through the consensus mechanism of the consortium chain, improving the security, transparency and robustness of the CA and improving the efficiency of cross-domain authentication.

#### 4.2.3.3 Credential & Access Management.

In traditional telecom networks, the user's credentials are centralized managed by operators. When a UE has to be authenticated in a roaming scenario, the authentication has to be done back to the place of origin; in addition,currently, users’ credential information are strongly bound to the operator they subscribe while users do not have the ability to flexibly select and switch network operators; Operators and cardholders/equipment vendors establish bindings and need to share card data (root key) through offline channels in advance. Provide credential sharing, authorization, and access authentication through blockchain. PDL plus privacy protection technology can realize the secure sharing of operators' credentials and realize seamless ubiquitous access for users.

#### 4.2.3.4 Decetralized Identity Management

At present, the user identity and its verifiable credentials (VC) in the telecom network are generated by operators (e.g., a SIM card). Users do not have the ability and authority to self-generate, self-maintain their own IDs, PDL provides the possibility for independent generation of user identities, autonomous management, users can selectively generate IDs, and VC verified by authoritative institutions on the decentralized ledger, and selectively disclose the information required by the verifier, so as to achieve decentralized identity management and verification.

### 4.2.4 Resource Sharing and Exposure

#### 4.2.4.1 Operators’ Data Sharing

PDL can facilitate data sharing and transactions between operators, and realize the sharing of data that meets regulatory requirements (such as blacklist information, malicious websites, user tag databases, location information, etc.) between operators, thereby improving cooperation between operators, improving service quality, and creating business value of data.

#### 4.2.4.2 Compute & Storage Resources Sharing

Computing and storage in telecom networks can be used by users as part of resources, and resources can be shared between users. Provide a platform for publishing and trading resources. Resource information, resource status, and resource transaction releases and results can be shared with stakeholders in PDL.

#### 4.2.4.3 Digital Asset Sharing

PDL can facilitate the release, transaction, and transfer of digital assets between operators, equipment vendors, service providers, and content providers. Based on the blockchain infrastructure provided by the telecom network, digital asset information, status, transaction release and results can be shared with stakeholders.

#### 4.2.4.4 Spectrum Resource Sharing

The spectrum resource of telecom networks is valuable thus traditionally spectrum is often allocated statically by national organizations. Spectrum sharing means that the owner of the spectrum can share the spectrum resources and authorize the alliance to licensed users in a specific region. At the same time, there can also be environmental monitoring nodes in the network to monitor the surrounding radio wave environment and spectrum usage. For solving the transaction process of multi-user mutual trust and sharing of spectrum data, PDL-based spectrum auction, spectrum trading, spectrum access and information sharing of free spectrum can effectively improve the efficiency of spectrum use and enhance the security of spectrum sharing.

#### 4.2.4.5 Network Slicing

In the future, the creation of network slicing may require trust between operators/within operator networks, and PDL can provide technical means to maintain trust for cross-operator/operator internal network slice management, and provide a platform for slice resource release and transactions. Dynamic and trusted creation of slices is completed through the release and on-chain of resource allocation information, network status information, RAN resource configuration information, and slice construction/deletion information.

#### 4.2.4.6 Sensing Data

Sensing data may come from the data collected by radar, consumer devices, and personal devices. The devices generate different types of data, and may belong to and be owned by multiple organizations, contain multiple data types and depend on the joint organization of multiple organizations. Data collection and protocols require a secure foundation of trust. By introducing PDL technology, a unified distributed trust platform can be established to enable various terminal devices and sensing devices to achieve a more credible relationship, and ultimately ensure the credibility, accountability and transparency of the perception. The perception data storage audit based on PDL (e.g., through regular storage of data snapshots, key information, etc.), it forms a traceable and accountable data storage management method, thereby improving the security of communication perception integration.

### 4.2.5 Vertical Application Support

As a unified communication platform, the next generation telecom network will support various vertical applications and business or customer users will become the tenants of the telecom network. Therefore, a large category of use cases are for vertical application supports. We basically split them into two sub-categories.

#### 4.2.5.1 V2X

A large amount of data is exchanged between vehicles, people, road side units (RSU), edge computing nodes, and cloud servers in a connecte vehicle system. Some key data directly affects the safety and stability of the connected vehicles in the system. In order to ensure the traffic safety of participants and improve the service level and operation efficiency of the traffic system, important data information (such as vehicle driving data before and after traffic accidents, legal identity letters of vehicles and people in vehicles, etc.) have to be correctly and immutably recorded. Based on PDL technology, transportation system/government regulators can participate the distributed ledger system (e.g., by contributing a data validating node) and retrieve data from the ledger. The data can be traced throughout the process and used for audit analysis to achieve the effect of "penetrating supervision". Regulators can deeply involve the full business process to comprehensively monitor all data and behaviors in the V2X services, facilitating to regulation enforcement.

#### 4.2.5.2 Other Verticals

In the fields of healthcare, finance, digital currency, supply chain, energy, law, entertainment, public welfare, etc., there may be low-layer bearers who use blockchain as their services, and telecom networks as ubiquitous cases of inclusiveness can use telecom networks as infrastructure to provide PDL services for industries in these vertical fields. Record key information, provide multi-party trust establishment, immutable storage, security and traceability of information, writing based on multi-party consensus, and dynamic execution based on smart contracts.

## 4.3 Summary



*Editorial Note: further analysing texts TBD*

# 5 Gap Analysis

## Key Issue 1: Nativeness of PDL in 3GPP Network

According to the degree of integration of blockchain service and telecom network service, three types of blockchain are classified, independent blockchain, coupled blockchain, and native blockchain.

• Independent blockchain: An independent blockchain is a blockchain independent of communication services and network protocol processes. For example, an independent blockchain provides data storage and source tracing support for network O&M and management. Typical applications include roaming charging and settlement. Although these interaction procedures are not included in the signaling procedures defined by 3GPP, they are important for establishing trust relationships between operators and improving efficiency through smart contract.

• Coupled blockchain: A coupled blockchain refers to a blockchain that interacts with a communication network in a protocol process, including offline connection and online check. Take blockchain-based authentication services as an example: Information owners or authorized operators store information (such as credentials) or hash values in blocks in advance. When a communication request is received, the recipient searches the blockchain for the requester's credentials to authenticate it. During this time, the requester waits for a response. If the authentication is successful, the recipient accepts the connection request and continues the process.

• Native blockchain: A native blockchain refers to a blockchain in which an algorithm, a communication protocol, and an enabling function of a blockchain are embedded in a function and protocol of a communication network. Writing to the blockchain and searching in the blockchain occur online in real time and are part of the communication process. However, the real-time application of blockchain technology in communication networks still faces many new challenges. One of the goals in the next generation mobile network is to create a real-time, large-scale blockchain system that serves as the basis for trusted network operations so that every real-time data session and every real-time signaling interaction can be recorded untampered, such as a permission-based super account.Therefore, a native blockchain architecture needs to be designed to meet the potential requirements of wireless and network deterministic low latency and high throughput and meet privacy protection objectives.

## Key Issue 2: Impact of PDL on Protocol Stack in 3GPP Network

When blockchain is integrated with telecommunications network, that is, an endogenous telecommunications blockchain, control and data of the blockchain are also integrated into a signaling message and a data message of the telecommunications network. Therefore, how to complete management of this part is a key issue.

## Key Issue 3: High Throughput

In order to enable the blockchain to be adaptable to the extreme capabilities of Beyond 5G wireless networks, the blockchain shall overcome several issues such as high-speed consensus algorithm and the integration of the distributed blockchain with the centralized network architecture, which are the areas for studies.

## Key Issue 4: Data Sovereignty for 3GPP System Users

Generally, the telecom network stores data for a certain period. If it expires, the data will be deleted to save storage. This is contrary to the data undelete feature of the blockchain. The effective use of storage of network, and the permanent history record of data in blockchain can be achieved by designing the blockchain architecture or algorithm.

Recently, multiple personal data protection laws have been implemented worldwide. For example, the GDPR Act of the People's Republic of China, the APPI Act of Japan, the CLOUD Act of the US, and the California Consumer Privacy Act (CCPA) are increasingly important to protect users' personal data and information. The EU proposed the "right to be forgotten" data protection principle, which was incorporated into the General Data Protection Regulation (GDPR) in 2016. GDPR requires that data can be modified or deleted as necessary to comply with legal requirements. Therefore, subscriber data on the carrier's network must be deleted when triggered by subscribers.

## Key Issue 5: Sustanability

The benefits of using blockchain or DLT do not come for free. The core mechanism of a blockchain system relies on a distributed consensus protocol, where in certain cases, the energy consumption of running such a protocol is energy inefficient. In order to align with the general goal on environmental impacts, i.e., green network, the sustananbility of telecom. blockchain has to be considered. How to integrate this goal when designing the telecom. blockchain services is very challenging because it is a multi-lateral optimization task depending on the whole system performance, network entity depoloyment/provisionin and lifecycle management and so on.

# 6 Potential Impacts to 3GPP Network Architecture

Considering the use cases and key issues analysed in the previous cluases, realizing them is not trivial, which may influence the design of the next generation 3GPP network system. In this clause, we generally discuss the potential impacts to the architecture of a 3GPP network system. Building 3GPP network services on top of PDL capability requires a deep integration within the 3GPP network infrastructure at all layers.

First of all, 3GPP management plane will be influenced where the lifecycle management is needed for deployment, instantiation, provisioning, termination and fault treatment of any PDL-related network entities. Such functionalities are missing, which are expected to be added.

Secondly, for a certain use case of transforming a control plane service by using PDL within the 3GPP network domain itself, such a transformation is not equivalent to running distributed control plane network entities at different places. Instead, it means that such a control plane network service fully operates without a centralized control authority. In other words, although there could be multiple control network function instances, they are purely equal and there is no master-slave relationship. Therefore, some existing control plane network functions may have to be enhanced/extended/re-designed so that a certain control plane network service can work in a decentralized manner.

Thirdly, for some other use cases (e.g., intracting with other blockchains with different types and/or run by different platforms), existing network functions defined in 3GPP could be insufficient. Therefore, it is not surprising that there could be a set of new network entities (nodes) that would be proposed for standardizations. Therefore, the 3GPP network architecture may be extended with new network entities that are dedicated for supporting PDL services for both internal and external 3GPP domains.

Last but not least, Blockchai-as-a-Service (BaaS) will be a necessary capability/service provided by the next generation mobile network system. It integrates the computing, storage, and network resources of the network infrastructure, shields underlying details for upper-layer services and applications, and provides a service platform for creating, managing, and maintaining blockchain networks. Compared with traditional cloud-based BaaS, BaaS based on mobile networks relies on ubiquitous network facilities to implement nearby deployment of chain nodes, ubiquitous collection of chain data, and unified interface for chain scheduling and management. Therefore, it will not be surprising as well that the creation, management, maintenance, use, and access of blockchains are converted into standardized interfaces to provide standardized capabilities for verticals.

# Conclusion

*Editorial Note: TBD*

Annex A:
Title of annex

Annex B:
Title of annex

# B.1 First clause of the annex

## B.1.1 First subdivided clause of the annex

Annex:
Bibliography

Annex :
Change History

| Date | Version | Information about changes |
| --- | --- | --- |
| 2022-12 | V0.0.1 | An initial outline of the draft was created |
| 2023-01-30 | V0.0.1 | Main clause sections were finished |
| 2023-02-09 | V0.0.1 | Revise use cases and key issues clauses |
|  |  |  |

# History

|  |
| --- |
| **Document history** |
| V0.0.1 | 2023-01-31 | The first version with major clauses done |
| V0.0.1 | 2023-02-09 | A revised version with further revised use case and key issue clauses |
|  |  |  |
|  |  |  |
|  |  |  |

*Latest changes made on 2022-03-14*