ETSI GR PDL 021 V1.1.1 (2023-10)

Permissioned Distributed Ledgers (PDL); Overview of use cases in 3GPP network and impact analysis on architecture integration

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-0021_usecase_3GPP NET

Keywords
3GPP, core network, distributed ledger

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

Contents

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 (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 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) 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] ISO/TR 3242:2022: "Blockchain and distributed ledger technologies -- Use cases".

[i.2] ISO/PRF TR 6039: "Blockchain and distributed ledger technologies -- Identifiers of subjects and objects for the design of blockchain systems".

[i.3] ISO/WD TR 6277.2: "Blockchain and distributed ledger technologies -- Data flow model for blockchain and DLT use cases".

[i.4] ISO/WD 7603: "Decentralized Identity standard for the identification of subjects and objects".

[i.5] ISO/AWI 20435: "Representing Physical Assets using Non-Fungible Tokens".

[i.6] ISO 22739:2020: "Blockchain and distributed ledger technologies -- Vocabulary".

[i.7] ISO/TR 23244:2020: "Blockchain and distributed ledger technologies -- Privacy and personally identifiable information protection considerations".

[i.8] ISO/TR 23249:2022: "Blockchain and distributed ledger technologies -- Overview of existing DLT systems for identity management".

[i.9] ISO 23257:2022: "Blockchain and distributed ledger technologies -- Reference architecture".

[i.10] ISO/TS 23258:2021: "Blockchain and distributed ledger technologies -- Taxonomy and Ontology".

[i.11] ISO/TR 23455:2019: "Blockchain and distributed ledger technologies -- Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems".

[i.12] ISO/AWI TS 23516: "Blockchain and distributed ledger technology -- Interoperability Framework".

[i.13] ISO/TR 23576:2020: "Blockchain and distributed ledger technologies -- Security management of digital asset custodians".

[i.14] ISO/TS 23635:2022: "Blockchain and distributed ledger technologies -- Guidelines for governance".

[i.15] ISO/WD TR 23642: "Blockchain and distributed ledger technologies -- Overview of smart contract security good practice and issues".

[i.16] ISO/DTR 23644: "Blockchain and distributed ledger technologies -- Overview of trust anchors for DLT-based identity management (TADIM)".

[i.17] ITU-T/FG DLT D1.1 TS: "DLT terms and definitions".

[i.18] ITU-T/FG DLT D1.2 TR: "DLT overview, concepts, ecosystem.

[i.19] ITU-T/FG DLT D1.3 TR: "DLT standardization landscape".

[i.20] ITU-T/FG DLT D2.1 TR: "DLT use cases".

[i.21] ITU-T/FG DLT D3.1 TS: "DLT reference architecture".

[i.22] ITU-T/FG DLT D3.3 TS: "Assessment criteria for DLT platforms".

[i.23] ITU-T/FG DLT D4.1 TR: "DLT regulatory framework".

[i.24] ITU-T/FG DLT D5.1 TR: "Outlook on distributed ledger technologies".

[i.25] IEEE Std 3801™-2022: "Standard for Blockchain-based Electronic Contracts", vol., no., pp.1-26, 1 April 2022, doi: 10.1109/IEEESTD.2022.9745868.

[i.26] IEEE Std 2418.10™-2022: "Standard for Blockchain based Digital Asset Management", vol., no., pp.1-19, 30 June 2022, doi: 10.1109/IEEESTD.2022.9810177.

[i.27] IEEE Std 2146.1™-2022: "Standard for Entity-Based Risk Mutual Assistance Model through Blockchain Technology", vol., no., pp.1-18, 11 August 2022, doi: 10.1109/IEEESTD.2022.9853246.

[i.28] IEEE Std 2142.1™-2021: "Recommended Practice for E-Invoice Business Using Blockchain Technology", vol., no., pp.1-18, 18 March 2021, doi: 10.1109/IEEESTD.2021.9381780.

[i.29] IEEE Std 2140.2™-2021: "Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges", vol., no., pp.1-20, 10 January 2022, doi: 10.1109/IEEESTD.2022.9676563.

[i.30] IEEE Std 2140.1™-2020: "Standard for General Requirements for Cryptocurrency Exchanges", vol., no., pp.1-18, 4 November 2020, doi: 10.1109/IEEESTD.2020.9248667.

[i.31] IEEE Std 2140.5™-2020: "Standard for a Custodian Framework of Cryptocurrency", vol., no., pp.1-23, 17 July 2020, doi: 10.1109/IEEESTD.2020.9144688.

[i.32] IEEE Std 2142.1™-2021: "Recommended Practice for E-Invoice Business Using Blockchain Technology", vol., no., pp.1-18, 18 March 2021, doi: 10.1109/IEEESTD.2021.9381780.

[i.33] IEEE Std 2143.1™-2020: "Standard for General Process of Cryptocurrency Payment", vol., no., pp.1-14, 12 June 2020, doi: 10.1109/IEEESTD.2020.9115946.

[i.34] IEEE Std 2144.1™-2020: "Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management", vol., no., pp.1-20, 18 January 2021, doi: 10.1109/IEEESTD.2021.9329260.

[i.35] IEEE Std 2418.7™-2021: "Standard for the Use of Blockchain in Supply Chain Finance", vol., no., pp.1-25, 28 October 2021, doi: 10.1109/IEEESTD.2021.9599622.

[i.36] IEEE Std 2418.2™-2020: "Standard for Data Format for Blockchain Systems", vol., no., pp.1-32, 23 December 2020, doi: 10.1109/IEEESTD.2020.9303503.

[i.37] IEEE™ P2145/D1: "Draft Standard for Framework and Definitions for Blockchain Governance", vol., no., pp.1-35, 10 March 2023.

[i.38] IMT-2030 Network Group: "6G blockchain scenarios and requirements".

[i.39] IMT-2030 Network Group: "6G blockchain architecture and key technology".

[i.40] Birkholz, H., Delignat-Lavaud, A., Fournet, C., & Deshpande, Y. (2023): "An Architecture for Trustworthy and Transparent Digital Supply Chains"(Internet-Draft draft-ietf-scitt-architecture-01). Internet Engineering Task Force.

[i.41] Hardjono, T., Hargreaves, M., Smith, N., & Ramakrishna, V. (2023): "Secure Asset Transfer (SAT) Interoperability Architecture" (Internet-Draft draft-hardjono-sat-architecture-03). Internet Engineering Task Force.

[i.42] Urien, P. (2022): "Blockchain Transaction Protocol for Constraint Nodes" (Internet-Draft draft-urien-core-blockchain-transaction-protocol-09). Internet Engineering Task Force.

[i.43] The Personal Information Protection Law (PIPL) of the People's Republic of China, www.npc.gov.cn, Retrieved 2021-09-30.

[i.44] The Act on the Protection of Personal Information (APPI) of Japan, www.ppc.go.jp, Retrieved 2017-05-30.

[i.45] "AB-375, Chau. Privacy: personal information: businesses". California State Legislature. Retrieved 2018-11-19.

[i.46] The General Data Protection Regulation (GDPR) in the EU and the European Economic Area (EEA), Retrieved 2016-04-27.

[i.47] ETSI GR PDL 020 (V1.1.1): "Wireless Consensus Network".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
AI4NET	AI for NETwork
APPI	Act on the Protection of Personal Information
AR	Augmented Reality
BC	BlockChain
BCaaS	BlockChain as a Service
BS	Base Station

CA	Certificate Authority
CCPA	California Consumer Privacy Act
CLOUD	Clarifying Lawful Overseas Use of Data act
DAPP	Decentralized APPlication
DLT	Distributed Ledger Technology
DRL	Deep Reinforcement Learning
E2E	End-to-End
ETSI	European Telecommunications Standard Institute
FL	Federated Learning
GDPR	General Data Privacy Regulation
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMT	International Mobile Telecommunications
IoT	Internet of Things
IRTF	Internet Research Task Force
ISO	International Standard Organization
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LTE	Long Term Evolution
M2M	Machine-to-Machine
ML	Machine Learning
NET4AI	NETwork for AI
NF	Network Function
NFT	Non-Fungible Token
PKI	Public Key Infrastructure
QoS	Quality-of-Service
RAN	Radio Access Network
RSU	Road Side Unit
SAT	Security Asset Transfer
SIM	Subscriber Identity Module
SME	Small and Medium-sized Enterprises
UE	User Entity
UMTS	Universal Mobile Telecommunications Service
V2X	Vehicle-to-Everything
VC	Verifiable Credential
VR	Virtual Reality
XR	eXtended Reality

4 Information of Existing Standardization Organizations

4.1 ISO

In 2016, ISO/TC 307 "blockchain and distributed ledger technologies" has been set up to meet the growing need for standardization in this area by providing internationally agreed ways of working with it to improve security, privacy and facilitate worldwide use of the technology through better interoperability. This is especially relevant due to the number of SMEs, across various sectors, that are developing blockchain and distributed ledger technologies as a product.

The scope of ISO/TC 307 reads: "standardisation of blockchain technologies and distributed ledger technologies." ISO/TC 307 has 7 Working Groups (WG). Specifically, WG1 places the foundation by defining the necessary terminologies for ISO/TC 207 [i.6], [i.10]; WG2 Architecture [i.9]; WG3's interests are on smart contracts and their applications [i.13],[i.15]; WG4 focuses on security, privacy and identity [i.2], [i.4], [i.7], [i.8], [i.11], [i.13], [i.16]; WG5 studies the mechanism of blockchain systems' governance [i.14]; WG6 aims to identify typical use cases [i.1], [i.3], [i.5]; and WG7 investigates the interoperability issues of blockchain systems [i.11], [i.12].

In addition to the 7 WGs, ISO/TC 307 has 3 Advisory Groups (AGs), 4 Ad-Hoc Group (AHG) and 1 Joint Working Group (JWG). Blockchain and distributed ledger technologies is a rapidly evolving and expanding area. The need for collaboration and cooperation has been identified and ISO/TC 307 is liaising with the relevant ISO and IEC committees, as well as external organizations, to minimize any overlap.

4.2 ITU-T

The ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) was established in May 2017 and concluded on 1st August 2019.

A key element of achieving this mission was to identify and introduce the foundation of the DLT ecosystem (including e.g. terms and definitions [i.17], taxonomies and concepts [i.18], and standardization activities [i.19]). In order to better understand how the technology can be applied in different scenarios and industries, FG DLT conducted an in-depth analysis of applications and services based on DLT, represented in its report [i.20] where 39 use cases were selected from the vertical (e.g. financial, healthcare, information and communication technology, entertainment, industrial, government and public sectors) and horizontal domains (e.g. identity, security and data management, governance and decentralized autonomous organizations, and crypto-infrastructure).

FG DLT has studied many of the DLT platforms available and described their key components and features. The common components and features are defined in the Focus Group's "DLT reference architecture" specification, which also describes their hierarchical relationship [i.21]. In addition, FG DLT identified "Assessment criteria for DLT platforms" described in a separate specification [i.22]. These 25 criteria aim to assist implementers to evaluate and compare different platforms.

Apart from considering technical issues, many implementers are concerned with the applicability of DLT in their respective legal and regulatory environments. Meanwhile, lawmakers and regulators are considering the need to adapt their instruments to this emerging technology. FG DLT has considered the key properties of DLT and their relevance to law and regulation in [i.23]. By analysing associated challenges and supplying practical recommendations addressing users, regulators, and technologists, the "DLT regulatory framework" developed by this FG aims to create awareness and mitigate risks. Developed by a multidisciplinary group of experts, the report in [i.23] describes DLT-property specific problems and risks, and guides stakeholders on how to address them. The "DLT Outlook" in [i.24] report explores the advancement of DLT beyond the current state of development, and addresses, inter alia, governance, computation networks, identity and privacy, resilience, risk and audit. The report in [i.24] summarizes existing studies, provides the reader with some future perspectives on these issues, and discusses related standardization aspects.

4.3 IEEE

The IEEE Future Directions Committee, represented by the societies of the IEEE, approved the formation of the IEEE Blockchain Initiative effective 1st January, 2018. This initiative will be the hub for all IEEE Blockchain projects and activities. The BLK encompasses a comprehensive set of projects and activities supported by the following core subcommittees: Pre/Standards, Education, Conferences and Events, Community Development and Outreach, Publications, and Special Projects. So far, it published 11 IEEE standards under this Standardization Association (SA).

The first area of the SA is about the general features and fundamental building blocks of DLT such as electronic contracts [i.25], digital asset management [i.26], E-invoice [i.28], [i.32], data format [i.36], Internet of Things (IoT) data management [i.34], supply chain finance [i.35] and its governance [i.37]. Another interest of the SA is about cryptocurrency, the standards cover its security management [i.29], the requirements for exchanges [i.30], defining a custodian framework [i.31] and the general payment process with cryptocurrency [i.33]; in addition, the SA also covers how to build mutual assistance model in a trustless environment based on blockchain/DLT [i.27].

Moreover, there are more than 50 additional standards under development.

4.4 IMT-2030

IMT-2030 aims to explore the possibility and application scenarios of combining blockchain with 6G networks/businesses in 6G scenarios. By analysing the development trend and security vision of 6G networks, it tries to extract the combination points of 6G and blockchain, using the decentralized, tamper-proof and consensus-based characteristics of blockchain to serve multiple scenarios of 6G networks/businesses [i.38].

Meanwhile, according to the characteristics of 6G networks/businesses, IMT-2030 reversely promotes the development of blockchain technology. Based on scenarios and requirements, it studies the key technologies involved in the integrated architecture of blockchain and communication networks [i.39].

4.5 IETF and IRTF

From IETF, there is no dedicated working group for DLT. However, blockchain technology is mentioned in several use cases in different drafts. For example, blockchain technology was used for building supply chain infrastructure, designing a secure asset transfer protocol as well as enhancing the RESTful protocol to design a blockchain transaction protocol for Constraint Nodes [i.40].

From IRTF, the Decentralized Internet Infrastructure Research Group (DINRG) investigates open research issues in decentralizing infrastructure services such as trust management, identity management, name resolution, resource/asset ownership management, and resource discovery. The focus of DINRG is on infrastructure services that can benefit from decentralization or that are difficult to realize in local, potentially connectivity-constrained networks. The objective of DINRG is to:

1) investigate (understand, document, survey) use cases and their specific requirements with respect to implementing them in a distributed manner;

2) to discuss and assess solutions for specific use cases with a focus on Internet level deployment issues such as scalability, performance, and security;

3) to develop and document technical solutions and best practices;

4) to develop tools and metrics to identify scaling issues and to determine whether components are missing; and

5) to identify future work items for the IETF.

Other topics of interest are the investigation of economic drivers and incentives and the development and operation of experimental platforms. For example, a Security Asset Transfer (SAT) interoperability architecture was proposed in [i.41]; and a transaction protocol for constraint nodes were proposed in [i.42].

4.6 Summary

The analysis in previous parts shows that most of the existing standardization organizations (such as ISO, ITU-T and IEEE) involve the study the blockchain/DLT itself. In other words, studies on its internal mechanisms are widely undertaken as a major research area. For example, ISO focuses on the standardization of the definition of blockchain/DLT, the reference service architecture; ITU-T covers the definition, framework, management, smart contract and even quantum-resistant blockchain, etc.

In addition, most of the existing standardization organizations involve studies on the applications of blockchain/DLT to various vertical industries. For example, ISO studies how blockchain/DLT can be applied to vertical industries; ITU-T has study items on deploying blockchain services within a telecommunication infrastructure such as blockchain-based self-organized IoT network, blockchain-based charging mechanism, personal healthy record databases and so on. IEEE has study items about Fintech, cryptocurrency, digital invoice and so on.

So far, among the existing standardization organizations, studies on applying blockchain/DLT in telecommunication industry, especially in the scope of 3GPP domain, are rare. Specifically, on the one hand, it is lack of further studies on the impact of blockchain/DLT to the architecture of a 3GPP network; on the other hand, how a 3GPP network can facilitate the development of blockchain/DLT applications is also missing. These two aspects are the focus of this study, which will fill the gap in the research community.

5 PDL Use Cases in 3GPP Networks

5.1 Telecom Infrastructure Registry

5.1.1 General Information

The telecom infrastructure of an operator contains many components geographically distributed across nationwide. For example, hardware components can be Base Stations (BS) in Radio Access Networks (RAN), (fibre) cables, network switches and routers in transport networks, and server machines and networking devices in telecom cloud data centres. In addition, with softwarization of the telecom infrastructure, many conventional hardware components are being replaced with cloud-native virtual elements. More importantly, in future generations of telecom infrastructures, virtual network entities do not have to tightly coupled with the underlying hardware resource owned by the operator. Instead, network entities can be flexibly virtualized with 3rd-party resource providers (e.g. a cloud provider and/or other operators' domains). This means that the telecom infrastructure can be federated. Given the factors above, registering and tracking the (physical and virtual) components of the entire infrastructure will not be a static and single domain task anymore. Instead, the number of components in the telecom infrastructure will not only become significantly larger, much more dynamic, but also involve multiple domains. This poses new challenges to all parties involved in building a federated infrastructure. However, PDL can be utilized to facilitate sharing the registry and tracking information of the components from individual domains; meanwhile, PDL also improves the credibility and synchronization of the state of the infrastructure. There are two main sub-cases, which are introduced next.

5.1.2 Single-domain Infrastructure Registry

For a single domain case, from hardware to software entities, the infrastructure is under the control of one operator. In this case, PDL can be used to build a distributed registration repository layer, where network managers controlling different segments can commit the activities of the network entities in the respective segments into the registration repository. In this way, a hierarchical registry organization for tracking the network components within the infrastructure can be avoided. Rather, a global and synchronized view of the whole infrastructure can be maintained. Even a digital twin of the telecom network infrastructure can be built for other purposes.

5.1.3 Multi-domain Infrastructure Registry

For a multi-domain case, the infrastructure is under control of different participants, where each participant contributes its own segment constitute the entire infrastructure. In this case, PDL can be used to build a decentralized registration repository layer, where owners of different parties can directly access and provide information of the involved resource elements. The registration repository based on PDL is owned by all participants and no one can dominate. Hence, with PDL, the information shared via the decentralized registration layer is immutable and automatically synchronized. This helps to avoid setting up a centralized registry where information from all the parties is aggregated. Such a decentralized infrastructure registry becomes necessary in the future generation of constructing a federated telecom network infrastructure.

5.2 Operational Log Sharing

5.2.1 General Information

When a telecom network is in operation, operational logs are generated. These operational logs provide important information for service provisioning, optimization and coordination with application service providers. In the future the telecom network service will deeply couple with other participants (e.g. cloud providers where Internet applications locate and/or non-public networks widely used in industry sectors). However, directly sharing operational log is still difficult among different parties because:

1) there is no standardized interface and procedure where different parties can directly use;

2) setting up a direct sharing channel involves complicated preparations for agreements on data privacy, law issues and so on.

As a result, a trusted third party is usually required. PDL can largely simplify and automate such operational log sharing process. For solving this issue, specifically, a shared data layer can be created based on PDL. It facilitates different players to share operational log data without a commonly trusted 3rd party and avoid complicated agreement negotiation process. There are following use cases for sharing different kinds of operational data.

5.2.2 Charging Bills

Auditing invoice bills is a cumbersome operational task especially for roaming involving different operators. For example, traditional use cases include roaming charging for mobile users traveling to different countries; in addition, when a network service is transported with different networks, each network domain will issue billing invoices not only for the end users, but also for other operators/service providers together forming the end-to-end infrastructure.

For a long time, multi-party charging accounting relies on a 3rd party to audit the billing data that are submitted from different parties; after that, calculations and calibrations are made; at the end, the results are sent back for a final review from different parties; once all these steps are done, the final invoices can be issued. The whole procedure takes time and could be error prone.

With a shared data layer based on PDL, immutable charging bills related to specific service provisioning (e.g. data volume consumptions) can be directly shared across different parties directly even in real time. With the mutually synchronized data, the charging bills can be directly verified and accounted by relevant parties that are involved in a decentralized manner without a centralized 3rd party. This largely improves the efficiency of the accounting process.

5.2.3 Service KPIs

The Quality-of-Service (QoS) is critical to user experience. With the service paradigm shifting to a fully dynamic and flexible manner, monitoring KPIs of the services is not only the job of the operators, but also necessary to service providers because in order to guarantee QoS (user experience), coordination in terms of the real time service KPIs is inevitable.

Traditionally, there is only a few limited ways to expose and share service KPIs to other parties. For example, a service provider can retrieve certain KPIs through interacting with a standardized NF and interface. This can only work with two parties that can communicate with 3GPP specifications. However, in the future application scenarios, involved players may cross different kinds of networks/systems. Hence, such a predefined method is neither common, flexible nor efficient.

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.

5.2.4 UE Runtime Behaviours

UE behaviours data are operational data while a UE is active and uses a network service. UE behaviours are critical to the decision-making process if the operator wants to adapt the network control to guarantee the user experience. This may not only happen in a single domain of one telecom network, but also across different network operators and/or application service providers. Therefore, sharing UE behaviour data is important when coordination 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 runtime behaviours are committed into the ledger and safely shared beyond the boundary of network domain. This improves the timeliness of the UE runtime behaviours shared among different participants.

5.2.5 Energy Consumption Measurement Data

In addition to all kinds of operational log data for system performance and use experience, the next generation of telecom networks also aim to be sustainable and environment friendly. This asks for a stronger monitor on energy consumption and based on that, corresponding energy saving solutions can be figured out. As mentioned, the future telecom infrastructure will evolve to be virtualized, cloud-native and federated with many different infrastructure players (contributing different types of resources and services). Sharing energy consumption measurement data among those involved players become necessary. However, existing architecture and framework does not well support the energy consumption of the whole service chain from data collection, measurement and sharing with similar reasons as the previous use cases. Based on PDL, collected energy consumption measurement data (bound to corresponding services) can be signed, certified by individual domains and directly shared over the distributed ledger. This can help all relevant parties to yield much more precise energy consumption measurement data and coordinate each to figure a joint energy saving solution where the aggregated effects can be maximized.

5.3 Security/Privacy Enhancement

5.3.1 Decentralized Data Storage

An operator keeps different types of data for operation. These data could be user-owned data, subscription data, operational logs, system monitoring KPIs and so on. The data could be sensitive and confidential. Hence, any loss or tamper of UE profile data may not only breach customer's privacy, but also violate law (e.g. GDPR).

With PDL, a decentralized storage system can be built where, firstly, the operator has options to choose the strategy of how data should be stored, either on-chain or off-chain, depending on the characteristics (e.g. size and sensitivity) of the data; in addition, the integrity of the data can be guaranteed because all records are immutable; last but not least, the single point of failure is mitigated. This largely enhances the resilience/security of data storage.

5.3.2 Data Auditing

Operational data are records of the running status of the devices, network system, applications and other operating conditions and the events. These operational data are critical for re-examining the efficiency, security risks and malicious behaviours of a telecom network system. For security, operational data can reflect many attack behaviours, such as login errors, abnormal access, and vulnerability attacks. Data audit can help to obtain the security operation status of the system, identify attacks and intrusions against the information system, and data 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 data, which can effectively prevent the single point failure of the log server and the illegal operation of malicious administrators.

5.3.3 Decentralized Certificate Management

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. Therefore, a centralized CA has the risk of being attacked, resulting in a single point of failure; besides, some small operators do not have the ability to operate CA, or the CA of their own is not highly credible, resulting in difficulties for cross-domain trust establishment and certificate authentication. Based on PDL, a trust alliance of CAs can be built, where operators and equipment vendors can write the digital certificates required for themselves and for authentications. Both the certificates of the consortium CAs and issued certificates of the devices will be committed into the distributed ledger 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.

5.3.4 Decentralized Credential Management

In traditional telecom networks, the credentials of a user are managed by operators in a centralized way. When a UE has to be authenticated in a roaming scenario, the authentication has to be done back to homing network, which is 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. With PDL, credentials can be issued based on the decentralized PKI from respective CAs; later on, when a credential has to be verified, an authenticator can retrieve the verification tool (e.g. the corresponding public key information) from the decentralized PKI.

5.3.5 Decentralized Identity Management

At present, the user identity and its Verifiable Credentials (VC) in the telecom network are generated by operators (e.g. a Subscriber Identity Module (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, to achieve decentralized identity management and verification. Decentralized identity management can enable new trustworthy user-centric networking functions and services in future wireless networks, for example:

1) user-centric relaying services among mobile devices via direct communication link;

2) user-centric network access and roaming management that can still properly function even if the home network becomes unreachable.

By providing credential sharing, authorization, and access authentication through blockchain, PDL can realize the secure sharing of operators' credentials and realize seamless ubiquitous access for users.

5.4 Asset Sharing

5.4.1 Infrastructure Assets

As an infrastructure, a telecom network owns powerful networking, compute and storage resources to support service provisioning with guarantees on QoS and user experiences. In order to improve the resource utilization, especially when off the peak hours, monetizing the resource of the infrastructure can benefit for both the operator side and temporary resource consumer side. However, realizing such a dynamical sharing is very difficult at both the business part (e.g. making transaction, contract terms, payment and so on) and the technical part (e.g. configuring the underlying resource and opening interface for other tenants). An existing example is like a cloud resource provider offering its compute, storage and networking resource with a predefined offer as well as relying on a 3rd party payment system. With PDL, all the tasks can be integrated into a smart contract. The transaction will be automatically done and meanwhile the resource will be guaranteed for the buyer.

A popular example is enabling network slicing among multiple operators, 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.

5.4.2 Radio Spectrum

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.

5.4.3 Digital Asset

In the future, a telecom network owns not only infrastructure assets and radio spectrum resources, but also various digital assets. Digital assets include software, operator-owned data and Non-Fungible Tokens (NFT).

First, the software contains traditional licenses, added-value application services for business or normal users and a software execution platform for a 3rd-party application service. PDL service can facilitate its sharing processing between an operator and a potential user, for purchasing purposes and/or access control purposes.

Second, owned data refers to the data that are generated in a telecom network domain and the ownership of the generated data belongs to the operators. Here the operator-owned data and user-owned data are different. The user-owned data have privacy concern because the data is usually associated with user profiles. The examples of operator-owned data can be sensing data from RAN or even utilizing the sensors on UEs that with permissions from the users; and it can be the data that are generated during the telecom network is in operation. PDL service can facilitate the data sharing process between an operator and a data consumer such as an AI/ML agent for model training purposes.

Third, NFT can include all kinds of tokens and credentials. Sharing and distributing such virtual substances was very difficult because digital/virtual copies can be easily faked. Based on PDL, it is possible to transfer them directly between two parties without involving a trusted third party as a moderator.

5.5 Trustworthy and Explainable Network-Native AI

5.5.1 General Introduction

Artificial Intelligence and Machine Learning (AI/ML) have been considered a major application for our daily life and many industry areas. The telecom network provides a ubiquitous execution platform to realize AI/ML applications over its pervasive resources with high availability and reliability, especially connectivity with wireless entities. For example, a Federated Learning (FL) application can be deployed on mobile end devices where model training is done locally at the devices, and after that model parameters from a massive number of distributed agents can be aggregated at a parameter aggregator deployed at the edge data centre of a telecom network. This scenario is called Network for AI (NET4AI).

AI/ML is also considered a promising technology for optimizing the management and control of the future wireless network systems [i.41]. The telecom network will benefit from AI/ML to optimize network operations (with a data-driven approach).

EXAMPLE: It has been demonstrated that Deep Reinforcement Learning (DRL) can derive optimal wireless resource allocation strategies for user devices under multi-access scenarios and potentially enable zero-touch autonomous networks, potentially across different protocol stack and as an integral part of the entire system, referred to as network AI.

Furthermore, connected wireless devices can provide intelligence and AI services, not only for themselves but also for the networks; in other words, AI/ML capability on wireless devices will in turn be leveraged to promote network intelligence and system automation. This is called AI for networks (AI4NET).

In general, it is crucial to guarantee trustworthiness and explainability of network-native AI for both situations above. There are three major use cases where PDL can be utilized to enhance the network-native AI, which are introduced below.

5.5.2 Training Data Collection

For both scenarios, model training data may be collected by all kinds of UEs (e.g. on-device radars/sensors, microphones, cameras, operational logs and/or network elements). The ownerships of the collected data might be heterogenous, which may belong to and be owned by private users, multiple organizations or the operators themselves. Hence, training data collection is concerned with challenging issues such as privacy, confidentiality, credibility and incentivization.

EXAMPLE 1: Mobile devices as data owners may want to keep data ownership and prefer decentralized data access directly between data providers (e.g. a mobile device) and data consumers (e.g. other mobile devices, applications, and/or network functions).

EXAMPLE 2: Is that a data consumer may want to assure that the received data is not modified during transmission. Moreover, a data provider may want to be incentivized (e.g. rewarded) by providing training data.

With PDL, a unified distributed trust platform can be established to enable various terminal devices and sensing devices to achieve decentralized data access and a more credible relationship, and ultimately ensure the credibility, accountability and transparency of the perception. Collected data via distributed ledger could be used for batch learning and/or online learning. Since online learning and batch learning have different requirements on data access performance such as latency, training data collection will need customizable distributed ledger (e.g. customized consensus protocols, customized number of distributed ledger nodes); for instance, data collection for online learning needs more low-latency and scalable distributed ledger than data collection for batch learning. 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.

5.5.3 Distributed Learning

For both scenarios, with training data (either stored in a distributed or centralized manner), model training needs to deploy training algorithms as well as distributed learning protocols when multiple AI agents are involved. Currently, the whole process is done in a trusted environment or with a strong trust relationship/belief. Such assumptions cannot be always met in the future where an open, dynamic and zero-trust environment will be normal conditions. For example, the execution of a training algorithm is simply done internally at a distributed agent, while whether the agent honestly follows the training algorithm cannot be checked. This results in the correctness of the training results (i.e. the model parameters) difficult to check as well. In a malicious environment, this may fail the whole training process and the consequence is unpredictable.

With PDL, DLT can be exploited to enhance the traceability and accountability in order to govern the lifecycle of model training phase. For instance, the AI pipeline (e.g. AI task deployment, AI model deployment) can be partially or fully traced and recorded on immutable ledgers for data and model provenance, afterwards diagnosis, AI traceability and explainability. An efficient way is to configure and trigger trace instructions as a part of AI model management and AI pipeline to meet application requirements. Also, PDL and smart contacts can promote trustworthy training data sharing, AI/ML model sharing, and inferred knowledge sharing.

5.5.4 Model Verification

For training the model, the (distributed) model training process could be executed with the diverse resources across the whole network (e.g. mobile phones, edge computing nodes and network entities). To the trained model (parameters), once the training is done on respective agents, the correctness and authenticity are hard to verified because the whole process involves many previous stages and the process is non-trivial. Verifying the training results needs to repeat the process alone, which may also not be feasible unless the entire process can be recorded.

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. Therefore, PDL can enhance FL framework in a telecom network environment.

5.6 Smart Contract-based Direct Interoperation

Multi-party interoperations will be inevitable in future wireless networks such as collaboration among mobile devices (e.g. a mobile device shares resources with and provides services for another mobile device), interoperability among NFs (e.g. collaborations among different types of NFs and/or collaboration among different instances of the same type of NFs), and collaboration among different network and service providers. Such collaborative parties (e.g. mobile devices) may not have any preestablished trust relationships and may need transparent collaboration among them. PDL can be used to meet those requirements where smart contracts can be utilized to guarantee the self-execution of the requested operations.

5.7 Vertical Support (Blockchain-as-a-Service)

The previous clauses mainly focus on use cases that directly matter to the telecom network's services. As a unified communication platform, the next generation telecom network will accommodate countless vertical applications of its tenants. Hence, a generalized use case here is a BlockChain-as-a-Service (BCaaS) that will provision a blockchain service on top of the telecom network with the resources from the infrastructure layer. Such a generalized use cases cover all blockchain applications that are already been adopted in many industry/business areas.

Note that some of them are more relevant to the wireless mobility environment. For example, for V2X scenarios, a large amount of data is exchanged between vehicles, people, Road Side Units (RSUs), edge computing nodes, and cloud servers in a connected vehicle system. Another example could be immersive eXtended Reality (XR) services. Specifically, today, many content creators rely on on-site live streaming. With the popularity of VR/AR services, 360-degree video data will be transmitted over mobile networks. Based on telecom networks, PDL can facilitate the transactions (such as subscriptions and payments) between the content creators and consumers.

Some other are less relevant to the wireless mobility environment, which are more related to the typical blockchain applications that already exist in cloud environment and Internet. 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.

5.8 Summary

Table 1: A Classification of Use Cases with Telecom Networks

	For Operator Use						For 3rd-party Use	
General Use Cases	1. Telecom Infrastructure Registry	2. Operational Log Sharing	3. Security/Privacy Enhancement	4. Resource Sharing	5. Trustworthy and Explainable Network-Native AI	6. Smart Contract-based Direct Interoperation	7. Vertical Support	
Sub-use Cases	1.1 Single-domain Infrastructure Registry 1.2 Multi-domain Infrastructure Registry	2.1 Charging Bills 2.2 Service KPIs 2.3 UE Runtime Behaviours 2.4 Energy Consumption Measurement Data	3.1 Decentralized Data Storage 3.2 Data Auditing 3.3 Decentralized Certificate 3.4 Decentralized Credential 3.5 Decentralized Identity	4.1 Infrastructure Resource Sharing 4.2 Spectrum Resource Sharing 4.3 Digital Asset	5.1 Training Data Collection 5.2 Distributed Learning 5.3 Model Verification	N/A	N/A	
Total Number	2	4	5	3	3	1	1	19

A classification of the introduced use cases is summarized in Table 1. In general, the identified use cases can be split into two main categories.

The first category (listed in the first six columns of Table 1) is for the purposes of operators of 3GPP networks. They range from the basic level usages to more complicated usages, on which the complexity/functional components can be different. Specifically, the PDL service is utilized as a registry for registering all network components for both single-domain and multi-domain scenarios. In these two use cases, only the decentralized information storage is used; after that, there are four use cases for sharing operational logs, where not only the immutability feature is used, but critical information is shared over a PDL service; in addition, based on PDL, a new service paradigm can be achieved for the security and privacy-preserving for the next generation of telecom network systems; besides, the infrastructure resources are monetized under a blockchain/DLT governance layer and can be shared in a dynamic way to improve its resource utilization; furthermore, a more advanced use case is identified for enabling direct interoperation among different participants for service provisioning. This requires more building blocks to realize the E2E interactions. Last but not least, using AI/ML (for both the telecom network itself and the third-party) in a telecom network infrastructure is identified and with combining some of the key features of blockchain/PDL, it can enhance the trustworthiness and privacy of the whole workflow of AI/ML. This partly mixes the purposes of using AI/ML for the 3GPP network (AI4NET) and the 3GPP Network for AI/ML applications (NET4AI), which is relevant to the second category.

The second category (listed in the seventh column of Table 1) summarizes to a generalized use case for the applications from vertical industries, so-called BCaaS. As an intrinsic capability, integrating PDL into a telecom network infrastructure can provide better PDL services to verticals. Specifically, an emerging use case is supporting vehicle-to-everything (V2X). Under this category, many relevant services can be built based on BCaaS capability in a telecom network. For example, for accident insurance claiming where combing with the information from a carrier network can better identify/preserve the authenticity of accident events. In addition, for road state data sharing, PDL service provided form a telecom network infrastructure can preserve more fine-grained information thanks to the pervasiveness of telecom infrastructure coverage. Additionally, other vertical use cases (such as medical, finance, cryptocurrency, supply chain, entertainment and societal functionalities) can also be built based on BCaaS from a telecom network infrastructure. Those use cases only utilize the resources provided from the telecom network infrastructure. Note that the number use cases listed in this category is less, because those use cases do not concern the internal control mechanism (such as security, operation and so on) of the telecom networks; in addition, those use cases are largely covered from existing studies. Hence, it is less focused here.

6 Gap Analysis

Key Issue 1: PDL Capability Integration in 3GPP Network

As shown in the use cases identified in the last clause, no matter if a use case is for a telecom network operator or a vertical user, it is built on top of the PDL capability that should be available from the 3GPP network. There are many ways of implementations to achieve the same goal. For example, one way is to utilize cloud resources to realize the use cases, which is completely independent to the 3GPP network architecture but a standalone or plugin implementation, while the telecom network only accesses to that service point (either for its own purpose or for a vertical user). Such an add-on method does not integrate PDL/blockchain as part of the telecom network architecture and will have difficulties to optimize for service provisioning, (re-)scheduling, coordination, risk control and so on. Hence, in the next generation of 3GPP network, it is expected that PDL capability should be part of the 3GPP network architecture so that this capability can be seamlessly integrated. Hence, a critical challenge is how to enhance the 3GPP network with blockchain/DLT capability.

A native blockchain/DLT capability refers to a blockchain in which an algorithm, a network protocol, and an enabling function of a blockchain are embedded in a function and the protocol stack of a telecom 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 signalling 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.

However, such a native capability from the 3GPP network architecture is still unavailable, where its functional design, interfaces/reference points and so on a still missing.

Key Issue 2: Flexibility of PDL Service Provisioning

Provisioning a PDL service in a 3GPP network is not like provisioning a PDL service on Internet and cloud data centres. For the former case, due to its openness and permission-less natures, deploying a blockchain service is completely voluntary, which cannot be planned and/or firmly regulated. For the latter case, the underlying resource is usually considered homogenous and unlimited, how to deploy a blockchain service usually considers the total amount of resources and pricing issues, while less considers the availability and reliability issues. Different from the two typical scenarios, deploying a PDL service over a telecom network infrastructure faces completely different settings.

For the resource layer, the key challenges are as follows:

1) the infrastructure is fully distributed rather centralized, where from base stations, transport networks, core networks and telecom clouds, they may be across different geographical locations; and

2) the resource types are highly heterogenous, where from the computing capability, storage capacity to resource behaviour patterns, different resource nodes have distinctive differences. For example, a network function in the core network may have much more computing power and processing capability than a UE node as a mobile entity; in addition, a UE node (such as a drone/vehicle) may be on mobility while its connectivity may not be always in the best condition. All these factors should be considered when provisioning a PDL service.

For the requirement of a PDL service, the key challenges are as follows:

1) The requirements of different PDL services are also various. Some PDL services need higher security feature but moderate processing speed, such as authentication services for normal users and decentralized storage services; however, some PDL services need higher processing speed but moderate security feature, such as in a small consortium with trusted participants, for example, a session establishment prefers a smaller getting-through delay.

From the nature of a PDL service, when using PDL to support use cases as described in clause 5, a typical operation is to submit new transactions to distributed ledgers, from both a user (e.g. UE) or being generated by NFs when operation. A side-effect is that a large amount of transactions will be composed, generated and submitted. Then an urgent issue to be solved is how to efficiently manage such transaction creation; for example, which pieces of data (from mobile devices and/or from the network) should be on-chain or off-chain for a particular PDL service. Whether or not the system has storage capability.

Given these three aspects, the flexibility of PDL service provisioning will be a major challenge for the 3GPP network because the location distribution, types and behaviours of the resource nodes, as well as specialized service configurations in terms of individual service requirements become very important. To sum up, blockchain application services provisioned in 3GPP networks have to be customized/specialized, instead of trivially migrating from Internet. Depending on specific use cases, different blockchains might be needed wherein the structure of the ledger blocks, the consensus protocol used, multiple blockchains (with inter-chain operations) as well as the cryptographic methods selected have to be specialized.

Key Issue 3: Data Sovereignty in 3GPP Network

Recently, multiple personal data protection laws have been implemented worldwide. For example, the Personal Information Protection Law (PIPL) of the People's Republic of China [i.43], the Act on the Protection of Personal Information (APPI) of Japan [i.44], the CLOUD Act of the US, and the California Consumer Privacy Act (CCPA) [i.45] 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 [i.46]. GDPR requires that data can be modified or deleted as necessary to comply with legal requirements. Therefore, subscriber data on the carrier's network should be deleted when triggered by subscribers.

Such a requirement by law contracts to the nature of blockchain/DLT, so as a PDL service, especially one deployed in a telecom network. First, a telecom network as an owner of an infrastructure providing a particular network service, it legally collects data from users; in addition, it also generates many operational log data and so on. If many use cases will be built with blockchain/DLT as a PDL service, by default, the committed data in the ledger will become permanent and immutable. Secondly, currently, a telecom network decides how the data will be utilized and to whom the data will be shared (with an agreement between the actual data generators), however, even if in the future, many use cases will be built with PDL services, the access right control mechanism is still missing and the responsibility is still unclear. Therefore, in order to comply with the law requirement, it is inevitable to address the data sovereignty issue challenge in 3GPP network, for example, redactable blockchain capability has to be enabled and decentralized data management system should be also designed.

Key Issue 4: Smart Contract Specialization in 3GPP Network

Smart contract is a key enabler for realizing various Decentralized APPlications (DAPPs) as part of PDL services.

First, smart contracts running as PDL services in a telecom network need to consider the underlying features, constraints and heterogeneities of the infrastructure layers. In other words, a smart contract for a PDL service running in a 3GPP network should be specialized for the execution environment. This is totally different from the smart contract/DAPPs developed for Internet blockchain services (i.e. Web 3.0).

More importantly, 3GPP network services need special telecom industry knowledge such as the standards including architecture, functional split, interfaces and interaction procedures. In fact, a Web 3.0 developer is far from the telecom industry. For example, how to develop smart contracts/DAPPs for the use cases for the telecom network operators introduced in clause 5 is still very initial. Hence, though there are lots of developers for smart contract developments (i.e. Web 3.0 developers), there are few for smart contract development towards 3GPP networks.

Key Issue 5: Offline and Mobile PDL Mode

When using PDL to support use cases as described in clause 5, a wireless node may become a PDL application node, a PDL platform service layer node, a distributed ledger node, etc. The wireless node could become offline (e.g. lose the connectivity to the core network, the depletion of energy) or on mobile leading to the issue of offline or poor connectivity PDL operations. Scenarios and a starting point as defined in ETSI ISG PDL 020 could be leveraged [i.47].

Key Issue 6: Sustainability

The core mechanism of a blockchain service relies on a distributed consensus protocol, where in certain cases, the energy consumption of running such a protocol is energy inefficient. To align with the general goal on environmental impacts, i.e. green network, the sustainability of telecom blockchain can 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 deployment/provisioning and lifecycle management and so on.

7 Potential Impacts to 3GPP Network Architecture

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

First, 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. interacting 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.

Fourthly, BlockChain-as-a-Service (BCaaS) 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 BCaaS, BCaaS 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.

Finally, 3GPP network may need to be optimization to better support blockchain-related service and the resulted blockchain traffic. One issue is related to how to set up appropriate policies to control and manage which UEs can use which blockchain services; existing policy control management in 3GPP network could be expanded and leveraged. Another issue is about how to efficiently transmit multicast-nature blockchain traffic through 3GPP networks. Other types of potential optimization of 3GPP network are possible.

8 Conclusion

8.1 Introduction

The present document discusses the potential use cases of blockchain/DLT that are closely related to 3GPP network systems. It first reviews the related work about blockchain/DLT in existing standardization bodies. After that, major use cases that can be utilized by 3GPP network systems are described and categorized. Based on the described use cases, a gap analysis is introduced where six key issues are identified to realize the PDL use cases within 3GPP networks. At the end, a brief discussion of the impact of those PDL use cases to the 3GPP network architecture is provided.

8.2 Recommendations for Next Steps

As described in clause 6, there are six identified key issues. These key issues cover different aspects where new technical solutions are needed to fill the gap between the expected PDL services in 3GPP networks and the current network architecture. To address those challenges, the following steps could be considered for standardizations by ETSI ISG PDL:

1) Specification of architecture enhancement for PDL service provisioning in telecom networks.

2) Specification of PDL service operation in telecom networks.

3) Specification of protocol design for PDL service in telecom networks.

History

Document history		
V1.1.1	October 2023	Publication