ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(11/2025)

YSTR.Emerging-web

Network enhancement for supporting emerging web technologies for digital assets management

Technical Report ITU-T YSTR.Emerging-web

Network enhancement for supporting emerging web technologies for digital assets management

Summary

The emerging web shifts Internet from an "information Internet" to a "value Internet", focusing on user ownership, digital asset protection and collaborative network construction.

This Technical Report describes the requirements and standardization consideration of network enhancement for supporting emerging web technologies for digital assets management.

Keywords

Digital assets management, emerging web, existing web.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Technical Report ITU-T YSTR.Emerging-web

Network enhancement for supporting emerging web technologies for digital assets management

1 Scope

This Technical Report describes the requirements and standardization consideration of network enhancement for supporting emerging web technologies for digital assets management.

The scope of this Technical Report includes:

– Use cases of emerging web technologies;

– Identification of differences in requirements of existing web and emerging web technologies;

– Potential requirements of network enhancement for supporting emerging web technologies;

– Identification of directions for network enhancement standardization to support emerging web technologies.

2 References

[ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems.*

[ITU-T X.1400] Recommendation ITU-T X.1400 (2026), *Terms and definitions for distributed ledger technology.*

[ITU-T Y.2345] Recommendation ITU-T Y.2345 (2023), *Scenarios and requirements of network resource sharing based on distributed ledger technology.*

[ITU-T Y.2348] Recommendation ITU-T Y.2348 (2025), *Functional architecture of network resource sharing based on distributed ledger technology.*

[ITU-T Y.3082] Recommendation ITU-T Y.3082 (2023), *Mobile network sharing based on distributed ledger technology for networks beyond IMT-2020: Requirements and framework.*

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following term defined elsewhere:

3.1.1 asset [ITU-T F.751.0]: A representation of value. It can be a diamond, a unit of currency, items inside a shipping container, etc. An asset can be physical or virtual.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

CP Control Plane

Dapp Decentralized Application

DLT Distributed Ledger Technology

E2E	End-to-End
IP	Internet Protocol
NF	Network Functions
NRF	Network Repository Function
TCP	Transmission Control Protocol
TLS	Transmission Layer Security
UDM	Unified Data Management
UE	User Equipment
UP	User Plane

5 Introduction

Emerging web has become the trend of global development. It is not a single upgraded iteration of a technology or an integrated innovation of a type of application, but the possible next stage of the evolution of the web, which will evolve from the "information Internet" to the "value Internet", focusing on value generation and the protection of users' ownership and digital assets. It promotes collaboration between users about the co-construction of the network based on the network communication capabilities. From a global perspective, emerging web has emerged as one of the primary areas of research interest. The global research on emerging web is currently underway, exemplified by the signing of Executive Order 14067 in US on Ensuring the Responsible Development of Digital Assets [b-1]. The EU announced Web4.0 as the next phase in the evolution of emerging web, which is characterized by its emphasis on openness, decentralization, and user's control over their data [b-2]. South Korea has passed the 'Virtual Asset User Protection' and positioned Seoul as the future development centre for emerging web [b-3]. China has released a white paper on emerging web to guide research and application development [b-4]. Japan released the "NFT White Paper – Japan's NFT Strategy for the Web3.0 Era" [b-5].

Beyond these activities, many emerging web industrial applications are being developed, such as Helium focuses on network sharing of emerging web [b-6], Filecoin focuses on storage networks of the emerging web, and Ankr focuses on computing networks for emerging web [b-7] and [b-8]. It is considered a very promising technology from a global perspective, with the involvement of governments, research community, and industry.

For the new service requirements of digital asset value generation and ownership protection, the network infrastructure of emerging web needs to provide user collaboration capabilities by building both centralized and distributed infrastructure, as well assession context synchronization capabilities to ensure the consistent transmission of digital assets. Moreover, using the distributed ledger technology (DLT) for the identity authorization and data management through private keys offers strong ownership protection for users, such as asset tokenization provides a transparent and immutable record of ownership [ITU-T X.1400] and [b-8].

6 Requirements differences between existing web and emerging web technologies

For a better understanding, the differences between existing and emerging web technologies are shown in Figure 1.

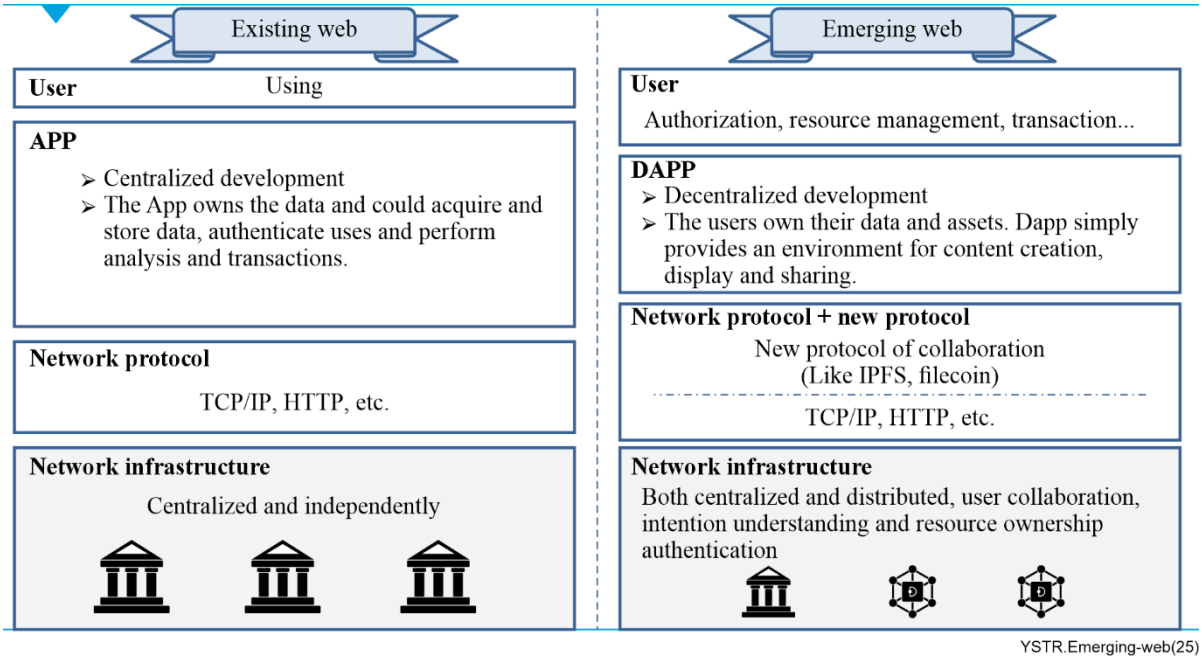

Figure 1 – Differences between existing web and emerging web

– Network infrastructure layer:

As shown in Figure 1, to support emerging web services, network infrastructure needs to evolve from being solely centralized to being both centralized and distributed, where it is not built and managed independently by operators but rather with user participation by their digital identity in collaborative co-construction. Furthermore, in order for machines to understand the purpose and methods of collaboration, network infrastructure for emerging web also needs to have semantic understanding capabilities.

– Network protocol layer:

As we know, the existing web focuses on connection, so its network protocol stack contains only basic communications protocols, such as transmission control protocol (TCP) / Internet protocol (IP). However, the emerging web focuses on collaboration which requires support from new protocols.

– Application layer:

Based on the basic protocols, many applications such as social networking applications are becoming increasingly sophisticated by capturing traffic and analysing user's data or information. In the existing web, data ownership generated by users belongs to the application, which can store, acquire, authenticate identities, analyse and transact data. Users cannot control their own information and identity. In the emerging web, applications are developed in a decentralized manner, and data ownership belongs to users. Decentralized applications (DApps) simply provide the environment for creating, displaying and sharing information.

– User layer:

In the existing web, users can only use applications, with limited ability to manage their own information. In the emerging web, users can perform identity authorization and data management and transactions using their private keys.

Users are the key components in the emerging web. Network resources are defined as digital assets, whose ownership belongs to users. The emerging web brings new features for network construction, where not only operators but also users can participate in the construction of network infrastructure.

7 Use cases with emerging web technologies

7.1 Value generation and protection

At present, there is data leakage and misuse because people do not focus on the value and ownership with their data and information while they communicate and share through networks, where personal information is continuously obtained through users' usage behaviour. Compared with the current networks, networks focus primarily on connectivity. However, networks in the emerging web area will be more focused on the value generation and asset protection.

In the existing web, network resources include computing, storage, connection and data resource [ITU-T Y.2345]. In the emerging web, the first new change is the value of network resource, which could be defined as "digital assets". In the emerging web, network resources will be assigned ownership, which belongs to users and generates value along with the digital assets exchange or sharing. Networks need to provide protection for the value of digital assets during network resource transmission.

Digital assets include digital documents, audio/video content, and picture/image. Moreover, digital assets also include digital painting, animation, presentation materials, and text documents.

7.1.1 End-to-end (E2E) emerging web data transmission and content sharing

In the current development of the emerging web, the most emphasis has been given on issues at the application-layer level. However, consideration of the supporting network infrastructure should also be addressed going forward. The IMT-2020 and beyond networks should be designed in such a way that they can enhance the security, reliability, and the scalability of data transmission for emerging web services.

This use case emphasizes the importance of, and possible security considerations for, network architecture and system-procedure-level studies aimed at enhancing the functionality and the reliability of emerging web digital assets transmitted through the underlying network system.

As shown in Figure 2, emerging web applications are connected to networks (e.g., the IMT-2020 network system) to transmit or share data and perform operations related to emerging web applications. Within the network, application data from users are transmitted in data tunnels established through interaction among network functions (NFs) of the control plane (CP) and user plane (UP). From the network point of view, current emerging web discussions are mainly focused on the application layer topics, while the data transmission security within the network relies on the legacy network security architecture/mechanisms, e.g., sidecar for Kubernetes Pod connection level security. Here, only data transmission security is considered, e.g., between NF_A and NF_B, the integrity of the content transmitted by NF_A or NF_B together with cyclic redundancy check and other mechanisms can be guaranteed. However, the emerging-web-applications-related context as digital asset can possibly be modified by the NF involved in the transmission chain of the IMT-2020 network system. Therefore, new network security requirements required by emerging web and corresponding network enhancement should be further studied.

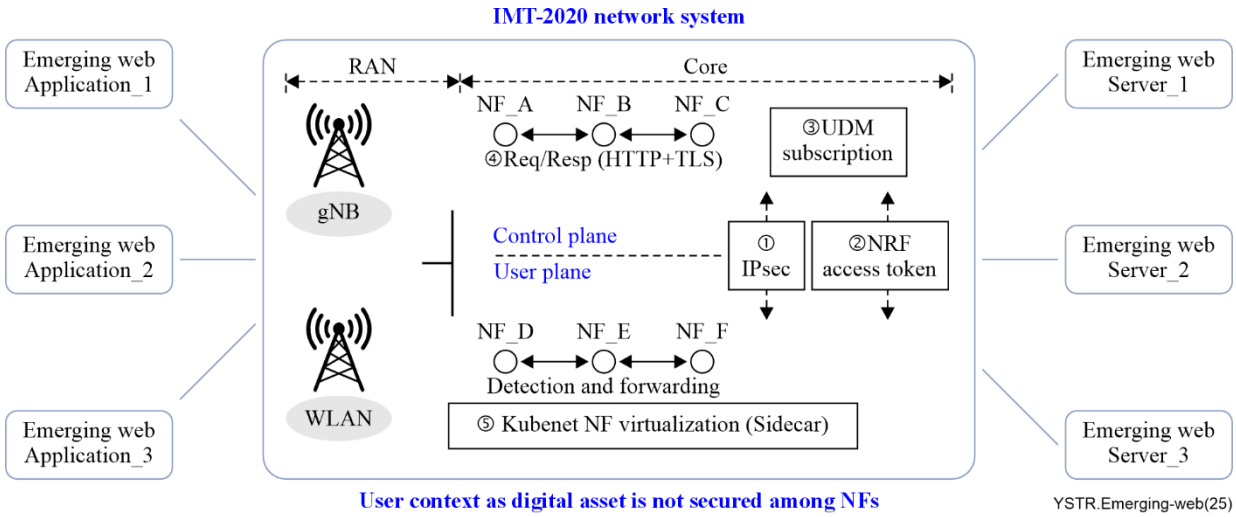

Figure 2 – End-to-end emerging web network architecture

NOTE – The meanings of the number in Figure 2 are as follows:

① : IP security (IPsec) designed for IP-based data transmission applied on both CP and UP.

② : Access tokens of the network repository function (NRF) for NF node level connection security.

③ : Subscription-based unified data management (UDM) for session level security.

④ : Transmission layer security (TLS) for HTTP connection level security.

⑤ : NFs are virtualized in different pods.

To ensure the reliability and scalability required to support emerging web services using IMT-2020 and beyond networks, the following possible security aspects should be further considered (also illustrated in Figure 3):

- **Security of session context synchronization among multiple NF instances**: In order to protect the transmission of digital assets within the network, where the ownership and content of the digital assets cannot be tampered with. The security of session context synchronization among multiple NF instances needs to be taken into consideration seriously. Multiple instances of each NF are used to balance the traffic load and boost the system robustness. It is important to securely share the session context without any eavesdropping, modification or tampering during the context synchronization procedure among NF instances. As the session context mainly relates to NF-specific functionality, the individual chain concept for securing the integrity of the data may need to be further studied.
- **Trust of data transmission among NFs**: How to ensure the trustworthiness and safety in data transmission between NFs (e.g., NF_A and NF_B in Figure 2), especially when NFs are provided by different vendors, may need to be further studied. As different NFs, e.g., the session management function and the user plane (UP) function are functionally distinct systems, the concept of federated chain and possibly cross-chain data transmission could be further considered here.
- **Cross-domain data transmission security**: Supporting emerging web applications may require network connections that belong to different autonomous systems or communication systems (e.g., the evolved packet system, the IMT-2020 system and the bearer network system) to cover geographically large serving areas. Due to the different network modalities, the concept of a customized chain for cross-domain data transmission security should be further considered.

NOTE – The network modality mentioned here involves multiple dimensions, including network service, network architecture, network function, NF deployment topology, protocol stack, processing capability, signalling procedure, and information element composition. The network modality (excluding network service) can be dynamically orchestrated, based on software-defined networking (SDN) and network function

virtualization (NFV). A typical example for understanding network modality is the difference in modality between IMT-Advanced and IMT-2020 networks, in terms of some or all of the dimensions mentioned above.

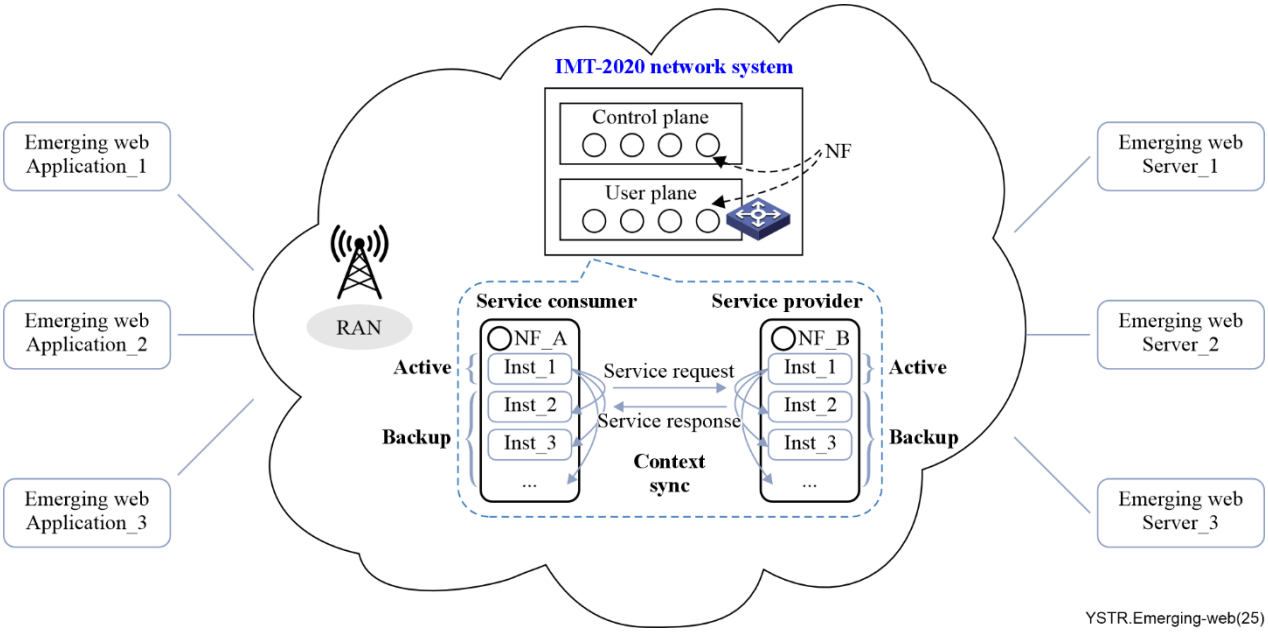

Figure 3 – Emerging web security issues in data transmission and content sharing

7.1.2 Use case of digital assets of traffic resource in emerging web

With the popularity of various intelligent terminals, IMT-2020 and IMT-2030 wireless connection access and network connection capacity are growing explosively [ITU-T Y.3082]. For this reason, the original connection methods are facing challenges and improvements in the cellular frequency reuse solutions have become a new demand. In this regard, 3GPP proposes Prose (proximity service), a new technology that allows LTE terminals to communicate directly from device to device (D2D) by sharing the network resources without infrastructure [b-9]. In short, it is a new approach to establishing connections between two peer-to-peer user nodes under the network resource sharing mode.

Mobile users can register as service nodes to share mobile network resources with other mobile terminals, so as to obtain tokens. At the same time, they can also be used as a user node to obtain network services and pay using tokens [ITU-T Y.2348].

In this scenario, a user's traffic resource is one of the digital assets and could generate revenue by sharing that digital asset.

7.2 Distributed management of digital assets of network resource

Distributed management is the key feature of emerging web technologies. Therefore, the emerging web is more focused on multi-agent collaboration rather than centralized (one person or company) control of the network system.

In the emerging web, network infrastructure will not only be built independently by operators but can also be constructed with users' involvement. Users can contribute their resources (bandwidth, storage, and computing) to form network elements, build network transmission tunnels, and support network management.

7.2.1 Distributed construction and sharing of network infrastructure in the emerging web

The emerging web will be a new type of network that all users can jointly build, govern, and share the value of. Its core function is to build a distributed network ecosystem with users as the main participants, helping users complete network interactions. For the network infrastructure of the

emerging web era, all network participants can become builders and managers. In addition to traditional communication operators, network infrastructure will present a state of decentralized ownership. Not only will operators form a joint and shared network, but ordinary users will also share their own resources to support a wide range of network communication, computing and other capabilities, helping the emerging web form a new network world that can be accessed at any time and from anywhere. Figure 4 shows a typical example of wireless access network co-construction and sharing under the vision of the emerging web.

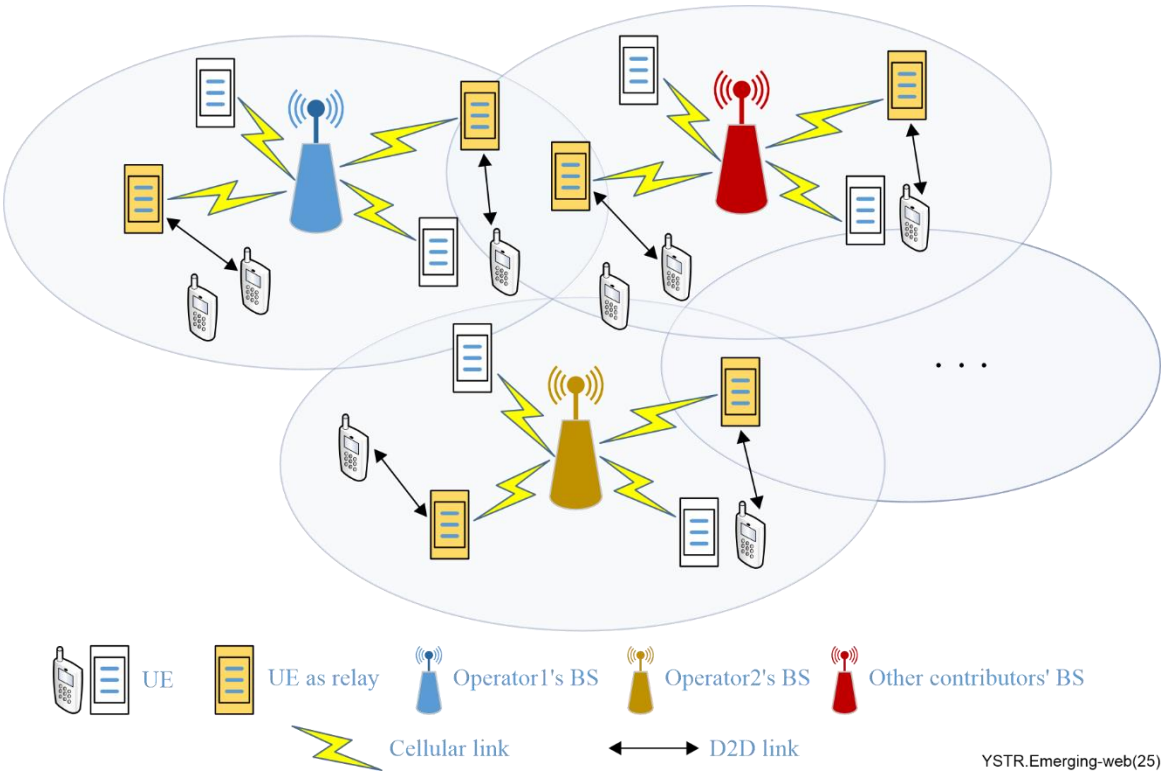

Figure 4 – Typical scenario of collaborative construction and sharing of wireless access network

In Figure 4, there are two types of collaborative construction and sharing. The first typical type occurs between base station (BS) builders, e.g. between operators. Users can flexibly access the shared BS resources of different operators, and the operators can deploy their own applications/services using the shared BS resources. This is a type of traditional sharing where, through the use of DLT, operators become free from their traditional constraints and start sharing resources. The second type of collaborative construction and sharing in wireless access network occurs between users and operators, physically between user equipment (UE) and BS. Any user with idle equipment can deploy the equipment as a network relay providing service to other UEs. The relay formed by the UE can establish relay communication links for other UEs via D2D link and connect to a BS and can also share resources like computing resources, data resources, etc. Then all network constructors can benefit from it. This mode is a typical emerging web mode where all users have the right to join in network construction to provide traffic or wireless access resources and receive benefits. The contribution and reward rules will be written into smart contracts, making multi-agent participation in network construction transparent.

8 Considerations for network enhancement for supporting emerging web

As mentioned in clause 6, the emerging web has brought about **two important changes**, **which are value generation and protection, and distributed management** of digital assets. These new features of the emerging web have brought new demands and changes to the direction of existing

network construction and research approaches. These changes can be considered from different perspectives as listed below.

1) From the high-level perspective

– Networking for the emerging web is different from current networking as resource allocation, traffic steering, distributed computing and other requirements are basically determined or optimized by users' requests or negotiation among users rather than just by operators' intention.

2) From the application-level perspective

– For supporting value transfer, networking needs the ability to protect users' ownership, authenticating resources and working effort, and achieving value generation, such as through the exchange of digital assets;

– For supporting co-construction of the network in the emerging web, networking needs distributed and authenticated network elements/nodes, and consideration needs to be given to how to integrate existing network architectures (e.g., orchestration) with third-party trusted delivery;

– It also needs enhanced capabilities to understand users' intentions, thereby enhancing intention negotiation and efficient coordination and transmission among users.

3) From the technical perspective

– For supporting value transfer, emerging web networking needs to protect the value of user data or information in the network transmission tunnel, as well as the verifiability of the contextual information;

– For supporting network construction in the emerging web, emerging web networking needs to be realized in the form of a distributed network that any user can join or contribute to for the purpose of constructing network infrastructure according to their intentions.

9 Consideration on the network enhancement standardization

Compared with the current network capabilities, emerging web networking has new characteristics, requirements, and capabilities, which need to be considered from the perspectives of the standardization of the following items (including but not limited to):

1) Digital assets of network resources

– Definition of digital assets of network resources, including bandwidth resource, data resource, computing resource, and storage resource.

– Study of the management, transaction, and authentication of digital assets.

2) Transmission of digital assets

– Study of the new requirements of network transmission to protect the value of digital assets and their authentication and authorization.

3) Distributed management of digital assets of network resource

– Study of the new requirements and architecture of the networks constructed in collaboratively by users and operators with distributed features.

– Study of the requirements and architecture of distributed management of digital assets of network resources by both users and operators.

Bibliography

[b-1] Ensuring Responsible Development of Digital Assets.
https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets

[b-2] Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds.
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718

[b-3] Virtual Asset User Protection.
https://elaw.klri.re.kr/kor_service/noticeList.do

[b-4] Virtual asset policy stated.
https://www.news.gov.hk/eng/2022/10/20221031/20221031_102428_003.html

[b-5] NFT White Paper – Japan's NFT Strategy for the Web3.0 Era.
https://www.taira-m.jp/Japan%27s%20NFT%20Whitepaper_E_050122.pdf

[b-6] Helium Network: A Decentralized but Connected Future.
https://hackernoon.com/helium-network-a-decentralized-but-connected-future

[b-7] Ankr Network (ANKR): Infrastructure Tools for Web3.
https://www.gemini.com/cryptopedia/ankr-coin-web3-blockchain-api

[b-8] Asset Tokenization: The Digital Transformation of Ownership and Value.
https://www.vestr.com/blog-posts/tokenization

[b-9] 3GPP WI # 580059[Rel 12], *Proximity-based Service*.