ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Paper

(11/2025)

YSTP-DataInfra-Web3

Trustworthy data infrastructure for emerging web

Technical Paper ITU-T YSTP.DataInfra-Web3

Trustworthy data infrastructure for emerging web

Summary

The existing ICT infrastructures for the future emerging web era need significant changes with emerging technologies (i.e., IMT-2030, AI, blockchain, crypto and quantum computing, etc.). Although there are a lot of related activities in different groups in ITU-T, there are no clear views on the future ICT evolution. Considering the technological evolution in line with the emerging web concepts, it is necessary to provide a clear direction for future standardization based on a holistic view of emerging topics and to stimulate related standardization in the future. Therefore, from a digital asset trading perspective, this Technical Paper provides a comprehensive view of trustworthy data infrastructure for emerging web and help to identify potential work items to support innovative digital asset trading with emerging techniques through gap analysis and preliminary efforts for pre-standardization.

Keywords

Data infrastructure, digital asset, digital asset trading, emerging web, trust.

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.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Technical Paper ITU-T YSTP.DataInfra-Web3

Trustworthy data infrastructure for emerging web

1 Scope

This Technical Paper specifies the following issues.

– Overview of trustworthy data infrastructure for emerging web
– Understanding emerging web
– Key features of digital assets and technical challenges of emerging web
– Data modelling of digital assets
– Overall ICT infrastructure and procedures for digital asset trading
– Technical requirements and considerations for digital asset trading
– Value evaluation and profit sharing of digital assets
– Applications for digital asset trading.

2 References

[ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology.*

[ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology.*

[ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology.*

[ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management.*

[ITU-T X.1404] Recommendation ITU-T X.1404 (2020), *Security assurance for distributed ledger technology.*

[ITU-T X.1405] Recommendation ITU-T X.1405 (2021), *Security threats and requirements for digital payment services based on distributed ledger technology.*

[ITU-T X.1406] Recommendation ITU-T X.1406 (2021), *Security threats to online voting systems using distributed ledger technology.*

[ITU-T X.1407] Recommendation ITU-T X.1407 (2022), *Security requirements for digital integrity proofing service based on distributed ledger technology.*

[ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology.*

[ITU-T X.1409] Recommendation ITU-T X.1409 (2022), *Security services based on distributed ledger technology.*

[ITU-T X.1410] Recommendation ITU-T X.1410 (2023), *Security architecture of data sharing management based on the distributed ledger technology.*

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning in information and communication technology infrastructures and services.*

[ITU-T Y.3053] Recommendation ITU-T Y.3053 (2018), *Framework of trustworthy networking with trust-centric network domains.*

[ITU-T Y.3054] Recommendation ITU-T Y.3054 (2018), *Framework for trust-based media services.*

[ITU-T Y.3055] Recommendation ITU-T Y.3055 (2020), *Framework for trust-based personal data management.*

[ITU-T Y.3057] Recommendation ITU-T Y.3057 (2021), *A trust index model for information and communication technology infrastructures and services.*

[ITU-T Y.3058] Recommendation ITU-T Y.3058 (2023), *Functional architecture for trust enabled service provisioning.*

3 Definitions

3.1 Terms defined elsewhere

None.

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

2FA Two-Factor Authentication

AES Advanced Encryption Standard

AI/ML Artificial Intelligence/Machine Learning

API Application Programming Interface

AR/VR Augmented Reality/Virtual Reality

B2B Business-to-Business

B2C Business-to-Consumer

BI Business Intelligence

CAPEX Capital Expenditures

CCPA California Consumer Privacy Act

CG Computer Graphics

CPS Cyber Physical System

DAO Decentralized Autonomous Organization

D-DAM Decentralized Digital Asset Management

DDoS Distributed Denial of Service Attack

DeFi Decentralized Finance

DevOps Development and Operations

DID Decentralized Identifier

DIY Do It Yourself

DLT Distributed Ledger Technology

DRM Digital Right Management

EAV Entity-Attribute-Value

GDPR General Data Protection Regulation

GNSS	Global Navigation Satellite System
GS1	Global Standard One
HSM	Hardware Security Module
ICT	Information Communication Technology
ID	Identifier
IP	Intellectual Property
IPFS	Interplanetary File System
IoT	Internet of Things
ISBN	International Standard Book Number
ISSN	International Standard Serial Number
ITS	Intelligent Transportation System
JSON-LD	JavaScript Object Notification for Lined Data
KYC	Know Your Customer
NFT	Non-Fungible Token
OGC	Open Geospatial Consortium
OPEX	Operational Expenditures
PIP	Programmable IP Licence
P2P	Peer-to-Peer
RBAC	Role Based Access Control
RDF	Resource Description Framework
RSA	Rivest-Shamir-Adleman
SMS	Short Message Service
SNS	Social Network Service
TCP/IP	Transmission Control Protocol/Internet Protocol
UI/UX	User Interface/User Experience
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
XML	extensible Markup Language

5 Overview of trustworthy data infrastructure for emerging web

Until now, the information communication technology (ICT) infrastructures have evolved from plain old telephone networks to high-speed Internet and 5G mobile networks. Originally, networks were about sharing expensive network resources in order for users to communicate with each other. Nowadays, the concept of networks has been expanded to an infrastructure that supports human life and business. The ICT infrastructures will expand to build physical infrastructures to support the concepts of smart city, smart transportation, and smart energy, etc.

To cope with the digital era, all the files and documents necessary for human life and business are represented by a digital form. Current video, audio, image including 3D are transmitted and shared in digital form. All the software and algorithms, including artificial intelligence/machine learning

(AI/ML) techniques/tools, are written in digital form. All the ideas, opinions, and experience/know-how which are classified as tacit or implicit knowledge will be represented in a digital form. This digital transformation will accelerate the adoption of digital technologies to bring benefits to human life and business with the ICT infrastructures and services.

Nowadays, some digital information is classified as digital assets (see clause 6.1). Originally, all digital data had usage rights. People want to be able to sell or buy a human creative painting as well as to enjoy a funny video at an acceptable price. In the near future, people may be able to sell or buy patented ideas and software including AI/ML algorithms. However, people have not considered digital rights or digital assets when they communicate and share digital information through networks. It is also important to know that security and privacy are the main concerns of people using the Internet and 5G mobile networks.

It should be noted that the existing ICT technologies are designed to support network infrastructures. To date, there are a lot of protocols, technical specifications and standards according to physical transmission media and interface types. Digital devices such as personal computers, mobile phones, and data storage devices are used to carry digital assets and should meet the requirements of network interfaces and protocols.

In addition, the ICT infrastructure may contain a large number of Internet of things (IoT) devices, mainly used by other industries and applications such as home, energy, transportation, health, and military applications, etc. The digital devices and systems used in these environments have their own protocols and technical standards. A future ICT infrastructure can play the role of a platform to accommodate all the digital devices and software running in all industries.

Digital assets are created by many electronic devices (e.g., digital cameras, audio recorders, and musical instruments, etc.). They are stored on local hard disks or in centralized database systems. Most digital assets can be made available to the public through web portals. Otherwise, some service providers provide menu item to access their own digital assets.

It should be noted that web technologies are designed to share digital assets. Web 1.0 consists of static web pages that provide useful information about companies and products. Also, some websites, sometimes combined with social networking services, are open for free discussion of interesting or social issues. Web 2.0 is used to upload user-created content. A lot of social media, blogs, and content are shared with the idea of "the web as a platform." Currently, emerging web (referred to as web 3.0) concepts (see clause 6.2) are emerging to share all the digital assets, which can be based on crypto or blockchain technologies to support decentralized and token-based economies.

Here, the existing telecommunications technologies that run the Internet and 5G mobile services will not easily support future requirements. All industries beyond telecommunications have their own technologies and standards. They won't be integrated into the ICT infrastructure. For example, the platforms for smart grid and intelligent transportation system (ITS) will never be merged into the ICT infrastructure, which will be built up independently. Only some digital assets of smart grid and ITS applications can be delivered through ICT infrastructure. Therefore, the web concept can provide a common platform for all industries. All digital assets for all industries can be openly shared through the web platform with uniform interfaces. All the digital assets generated, stored, and shared by all industries can be provided by the web platform in the form of data with emerging crypto and blockchain technologies to ensure trustworthy trading. That's why future ICT should contribute to building a trustworthy data infrastructure to support emerging web.

The existing ICT infrastructures for the future emerging web era need significant changes with emerging technologies (i.e., IMT-2030, AI, blockchain, crypto and quantum computing, etc.). Although there are a lot of related activities in different groups in ITU-T, there are no clear views on the future ICT evolution. Considering the technological evolution in line with the emerging web concepts, it's necessary to provide a clear direction for future standardization based on a holistic view of emerging topics and to stimulate related standardization in the future. Therefore, from a digital

asset trading perspective, this Technical Paper provides a comprehensive view of trustworthy data infrastructure for the emerging web and help to identify potential work items to support innovative digital asset trading with emerging techniques through gap analysis and preliminary efforts for pre-standardization.

6 Understanding emerging web from the perspective of emerging digital assets

6.1 Data and digital assets

Clarifying public data and private data including open data

There are many definitions distinguishing public data from private data. Public data is available to anyone who can afford it. However, private data is not offered to the public and can only be accessed by individual users. A private data system allows individuals to customize it to their needs and operate it directly.

A public data system can make data resources available to others. While this is not much of an issue in situations where the public data does not raise significant concerns, there are some users who are rightly vigilant about where their data resides and its safety. It is noted that public data, which is inherently compliant with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), should be highly reliable and stable. Data governance of public data should be discussed in the design of a future web platform.

If some of the private data is used to provide services to other customers, users should be able to control their personal data. This is a major concern for businesses that handle extremely sensitive data, such as healthcare providers and law firms. Private data systems should provide greater transparency, privacy, and security to individual customers.

It should be noted that all the data, whether public or private, requires a data system or cloud platform. Private data systems are used for business-critical applications, while public data systems are used for basic tasks and non-sensitive applications.

The new term "open data" has a different perspective from the distinction between public data and private data. It should be noted that private data can be made public if the owner is willing to donate it, just like the free use of open software. Open data can include audio/video/text files, educational and research materials, scientific and medical documents, software, algorithms, experience, and know-how, etc.

To reduce the digital divide through data, a large amount of data needs to be open and public data systems need to be widely used. Public data systems can provide most of the functionality and basic security options that organizations or individual users need. Any business based on public data may need to ensure compliance with open data regulations. This will require guidelines or regulations for open data, including the definition and principles of disclosure.

Emergence of digital assets

Wikipedia defines a "digital asset" as anything that exists in a "digital format" and comes with the right to use it. Digital assets include but are not limited to: digital documents, audio content, movies, and other relevant digital data that are currently in circulation or that are or will be stored on digital devices such as personal computers, laptops, portable media players, tablets, data storage devices, communications devices, and any devices which accommodate the design of new modalities capable of carrying digital assets, regardless of the ownership of the physical device on which the digital asset is stored.

Digital assets are therefore defined as any type of content or file that exists in digital form and has an intrinsic or evaluative value that can be possessed. Traditionally, assets refer to goods with economic value, such as cash, real estate, and stocks, which are typical examples of physical assets. In contrast,

digital assets are fundamentally different in that they take the form of data. More specifically, they are data with economic value. Recently, data with economic value that is specified with 'ownership' and can be traded through blockchain-based tokenization has been referred to as a digital asset. However, this should only be considered a subset of digital assets.

Types of digital assets include photographs, logos, illustrations, animations, audio/visual media, presentations, spreadsheets, digital paintings, word documents, electronic mails, websites, and a variety of other digital formats and their associated metadata. The number of digital assets will grow exponentially due to the increasing number of devices for digital media, especially the growth of smartphones.

The difference between data and digital assets

According to Wikipedia, a digital asset is anything that exists only in digital form and has a clear right of use or clear permission to use it. Data that does not have these rights is not considered an asset.

6.2 Emerging web concepts in the future data ecosystem

The term emerging web is emerging in the future data ecosystem. The emerging web is defined as the new Internet for transferring, sharing, and trading digital assets. The emerging web provides secure transaction ledger technology for digital assets and prevents forgery and counterfeiting in a distributed network environment. In particular, smart contracts using digital currencies such as tokens are possible for digital asset transactions. The emerging web has come to force and is now clearly associated with decentralized technology. Specifically, the emerging web is a combination of three things: decentralization, community for collaborating around a vision and culture of emerging web to how people work and collaborate to attitude. The core features of emerging web technology enable the new forms of digital asset trading that can emerge in the future, from digital art to online games, making digital asset trading transparent, and providing the most decentralized transaction governance. To achieve this, the philosophy of a decentralized autonomous organization (DAO), not monopolized by a specific company, must be maintained, and a means of protecting ownership of digital assets is needed.

It notes that a DAO is a digital entity that operates through rules encoded as smart contracts on a blockchain. DAOs operate without centralized control, relying on community voting and automated processes to make decisions and manage resources. This structure aims to increase transparency, reduce inefficiencies and promote collective governance.

It should be recognized that emerging web is the next generation of the Internet, which can be largely based on blockchain and crypto technologies. The most important aspect of emerging web is its philosophy of decentralization. Here, the emerging web platform should be defined and identified in relation to existing and emerging technologies such as IoT, blockchain, crypto, and AI/ML technologies. From the perspective of technology evolution, the future web platform should be developed in a step-by-step manner to include future expected technologies and new concepts. Additionally, the emerging web platform should be clarified with Cyber Physical System (CPS), digital twin and metaverse, etc., which are already used in the world.

So far, user data has been controlled by a few centralized organizations, such as social media platforms, and there have been many concerns such as misuse of user data, violation of privacy expectations, etc. In this regard, there is a strong need to build a data ecosystem and facilitate data sharing and exchange, as well as mitigate the above concerns for the data economy. Data ecosystems involves the collection of data to generate useful insights. It originally refers to part of the information and communication technology environment. Data is collected and used by public organizations and private companies. The best data ecosystems help people integrate multiple data sources. The emerging web platform should be designed to take advantage of the data ecosystem.

The key component of the web is the uniform resource locator (URL). In the IETF/World wide web consortium (W3C) standards (i.e., RFC1738 and RFC3986), the URL indicates the location of a web page. Web 2.0 includes user created content and social networking services (e.g., YouTube and Instagram, blog/wiki, etc.). Here, the "resource" for web applications can be extended to identify people, books, credit cards, physical devices/products, barcodes/QR codes, road/street address, company/organization/affiliation, files/documents, audio/video/image, software, service catalogue, know-how, and AI/ML algorithms, etc. In addition, the transmission and access protocol for a "resource" are not limited to the transmission control protocol/Internet protocol (TCP/IP) protocol.

It should be noted that there are many existing identification mechanisms from ITU-T, ISO/IEC, and global standard one (GS1), etc. It should be clarified what kind of identification for "resources" will be handled in the future web platform. It should also be noted that all resources in both the cyber and physical world should be well defined for a future ICT infrastructure. Future web applications should handle all resources to support human life and business. It is expected that a future web platform will be designed to support web applications via ICT infrastructures.

Figure 1 shows the location of the emerging web platform. Currently, the data communication network at the bottom is a wired and wireless network. A cloud computing platform is required to store, process, and distribute data. Here, the emerging web platform provides an environment where digital assets can be shared or traded with others on a cloud computing platform. For digital data to become a digital asset, data ownership and usage rights should be declared in order to receive compensation for transactions. Once the emerging web platform for trading digital assets is established and people are able to express their experiences and new knowledge in the form of digital assets, the future data ecosystem will become a true knowledge ecosystem.

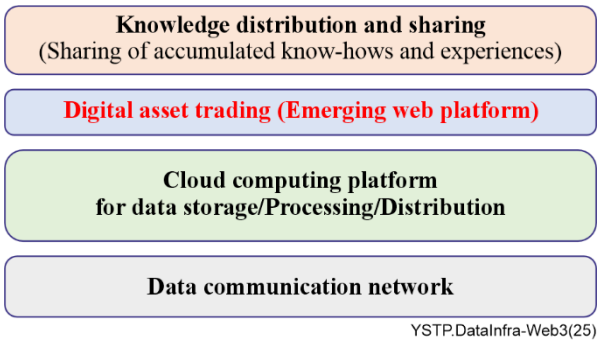

Figure 1 – Emerging web concept in future data ecosystem

6.3 Governance of the data ecosystem for emerging web

Concepts of data governance

To handle digital assets safely and securely, data governance is one of the outstanding issues for the emerging web platform. According to Wikipedia, it is defined that data governance is a data management concept related to the capability that enables an organization to ensure that high data quality exists throughout the data lifecycle and that data controls are implemented that support business objectives. The concepts of data governance are associated with the following terms and meanings:

– Digital rights refer to human rights and legal rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices, and telecommunications networks. The concept of digital rights is particularly related to the protection and realization of existing rights, such as the right to privacy and freedom of expression, in the context of digital technologies.

– Data sovereignty is the idea that data is subject to the laws and governance structures. With the advent of cloud computing, data sovereignty should reflect the law around the control

and storage of data. With self-sovereignty, individuals can fully create and control their credentials. Data sovereignty is seen by people and activists as a key part of self-governing structures. When a network is designed to receive emails, video clips, photos, voice and video calls, social networking details, logins and other data, any information collected by ICT infrastructure must be protected. In 2016, the EU Parliament approved its own data sovereignty measures as part of the GDPR.

– Data ownership is the act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use and distribution policies implemented by the data owner.

– Data stewardship is an essential part of data governance. It is responsible for ensuring the quality and fitness for the purposes of the organization's data assets, including the metadata associated with those data assets. Data stewards have a specialist role that leverages an organization's data governance processes, policies, guidelines and responsibilities to manage all of an organization's data in compliance with policy and/or regulatory obligations.

Data governance paradox

The paradox of data governance in digital asset trading is highlighted here. In general, when attempting to transact with others, various conflict situations arise when transaction details are disclosed. If transaction details are not disclosed, tax authorities suspect inappropriate transactions such as drug trafficking. Conversely, if transaction details are disclosed transparently, an individual's privacy may be violated. In addition, trading in digital assets only takes place when the valuation of digital assets differs between people. For example, in the stock market, trading is possible because the valuations of those who want to buy stocks and those who want to sell stocks are different. If someone thinks the value of a stock will fall in the future, they will not buy it, no matter how cheap it is. In other words, trading digital assets is only possible if there is an information asymmetry between those who want to buy and those who want to sell. No transaction can take place if everyone has the same information. In other words, if the relevant information about digital assets is disclosed transparently, there will be no transactions in digital assets for the same purpose.

If an individual asks a transaction provider or broker to sell a digital asset, the digital asset cannot be sold unless an acceptable price or compensation is agreed upon. In other words, the win-win conditions for profiting from digital asset trading must be met. It is necessary to discuss not only advertising costs and platform usage fees, but also any damages or potential risks that may occur during the transaction of digital assets. If privacy information is compromised or legal costs are incurred, such as ownership/copyright/licensing disputes, appropriate resolution procedures are required.

It is difficult to maintain original contractual terms for digital assets when complex value chains are created. Especially with digital assets, inappropriate duplication and fraudulent transactions can easily occur, making transaction monitoring very important. In this case, there is a conflict between monitoring non-appropriate activity and violating the privacy of individuals. In addition, when trading company confidential information or personal know-how information, stricter transaction conditions are required. There needs to be a way to monitor whether people who buy digital assets are inappropriately sharing or reselling them elsewhere. In addition, a negative cycle of trust can occur if transaction details are inappropriately exposed. The most important way to avoid these risks is to avoid trading digital assets with untrustworthy people or companies. In other words, no matter how perfect the technical solutions are to block inappropriate activity and protect privacy, if there is no trust, it's best not to transact. Otherwise, every digital asset transaction must be conducted under the assumption that there is absolutely no trust (i.e., zero trust).

Decentralized autonomous organization (DAO) philosophy

The concept of DAO is one of the core philosophies of emerging web technology. It means that when digital assets are traded, they should not be arbitrarily regulated by a particular company. It is the

most decentralized indicator of international trade in digital assets. All digital asset transactions need to be transparent. The most important issue in digital asset transactions is privacy. A fair and neutral body is needed to protect privacy in digital asset transactions. Privacy must be protected in all digital asset transactions, provided there is no inappropriate activity. In other words, privacy must be protected even when inappropriate transactions are being monitored. Currently, technologies are being developed to support privacy requirements such as decentralized identifier (DID) technology and zero trust technology. The DID standard states that the way in which verifiable credentials are actually operated is important for privacy protection. No matter what the technical standards are, operational procedures need to be more stringent to protect privacy.

However, in order to maintain the DAO philosophy, trust in the issuer of the credential or verifiable credential is required. Whether it is privacy protection or technical DID or digital wallet technology, the issuer of the credential is the most important part of the digital asset ecosystem. The question is whether an internationally neutral verifiable credential organization should be considered "trusted" in the digital asset ecosystem. There is a trade-off between transparency and privacy protection in digital transactions. Moreover, it is almost impossible to demand privacy protection while engaging in inappropriate digital asset transactions. This is because Bitcoin has so far been used as a means of distributing drug funds or inappropriate transactions, and numerous cybercurrencies are becoming the main activity stage for speculators. In conclusion, a safe and secure market for trading digital assets is needed even without regulation by specific companies or governments.

6.4 Trustworthy digital asset trading

In the real market, a secure market for trading digital assets will emerge based on trust. Trust means that digital assets will not be traded with untrustworthy people or companies. In other words, no digital asset transaction will take place unless the credit of the person or company is guaranteed according to the trust level. Ultimately, the trust level of an individual or organization determines whether or not they can enter the digital asset trading market. Transaction items and transaction amounts are also limited according to the trust level. Even in direct transactions between individuals, it is necessary to block noon-appropriate transactions or fraudulent activities. In the future, AI/ML algorithms can be applied to these digital asset transactions.

When trading digital assets for the first time or in the early stages, complex verification procedures are required assuming zero-trust environment. Thereafter, as trust is accumulated in the process of trading digital assets, restrictions on transaction items, transaction amounts, and transaction procedures will be reduced. However, if trading rules are violated intentional or not, additional regulations such as trading restrictions or compensation may be added. And trust in the digital asset trading market will also decline.

When secure, lightweight, and low-cost distributed ledger technology (DLT) is developed, the digital asset trading market can expand significantly. In order to create a global digital asset trading market, we need technology that is easy to use, while protecting privacy as much as possible without complex verification procedures.

6.5 Strategies for developing emerging web technology

In developing technology for digital asset trading, consumer preferences are more important than the technology itself. In other words, technology for the digital asset ecosystem must be developed according to changes in consumer tastes or preferences. In other words, technology development does not simply prioritize features and procedures for completing transactions in digital assets.

This is reminiscent of text messaging standards when digital communication technologies were first being developed. At the time, text messaging was designed to convey additional information through signalling channels when communicating with others. What the engineers didn't realize was that text messaging could later be used to replace voice communication between users.

The market for trading digital assets is also driven by trust in human-to-human transactions. In other words, no matter how perfect the technology is, if people do not trust it, it will be difficult for it to appear in the market. For example, NFT (non-fungible token) technology has recently been developed using blockchain technology, but there have been many cases of fraud and inappropriate copying. Even if Bitcoin succeeds in the market, the Ethereum technology, which imitates it, may have difficulties in gaining market trust. Many solutions in the cryptocurrency market may require additional technological development to gain market trust over a period of time. Otherwise, the current inappropriate activities in the cryptocurrency market will be repeated, similar to the stock market. Moreover, due to the vulnerability of digital asset transactions, many people who are unfamiliar with technologies such as blockchain are likely to become victims of fraud. The technical perfection claimed by technology developers is very different from the level of trust required by the market. This is because technology developers lack an understanding of the nature of transactions between people. Therefore, if an imperfect technical solution is applied to the market, the market will fluctuate due to numerous technical problems.

Moreover, even if digital assets are not perfect, there are various trading patterns, such as trying to trade cheaply according to each person's preferences. In other words, the market can calculate the total value of buying digital assets against the total cost, including risks and additional expenses. Of course, if the technology of digital asset trading for transactions, authentication and authorization is made available to everyone for free, there is a possibility that the market will open up quickly.

In addition, social consensus is needed to monitor inappropriate activity and protect individual privacy. While there are cases where it is absolutely necessary to disclose digital asset transactions, there are other digital assets that require appropriate privacy protection. No one will trade digital assets if there is strict monitoring in place to block inappropriate activity. Even if no one knows what a digital asset is, knowing who has traded it can cause fatal problems in trading digital assets. Therefore, there is a conflicting spear and shield situation when trying to track digital asset transactions and protect privacy.

The digital asset trading market can be introduced gradually through a market adaptation process. Digital asset markets are not like factories or machines that can cause major problems if they are not perfect. Initially, the digital asset trading market will start with transactions that do not result in large losses or lawsuits. Digital files that were previously released for free will gradually start to be traded on the digital asset market. Therefore, the digital asset trading market will be introduced depending on the response of consumers and the market. Technologies that are well accepted by the market will be adopted quickly, but just because the technology is perfect does not mean that the digital asset market will open.

In the past when technology was developed, it was field tested in a market environment after the technology development was completed. Therefore, it took a long time from development to release. However, the digital asset trading market requires a development process that allows for rapid feedback. This means that market adaptation processes such as development and operations (DevOps), need to be minimized and any consumer complaints or issues that arise in the market need to be reflected as quickly as possible.

7 Technical challenges for emerging web

7.1 Ownership and usage rights of digital assets

In order to trade digital assets in the emerging web, ownership of any file or document must be verified. Until now, people have not thought about digital ownership when communicating and sharing digital data over networks. Some digital information can be classified as a digital asset if ownership is clearly stated. Digital ownership also includes the right to access, create, modify, package, profit from, and sell data. However, it is difficult to apply existing trading methods to the

trading of digital assets such as software and algorithms, including AI/ML. In the future, people may try to sell ideas, opinions and experiences/methods that are classified as tacit knowledge.

While people may share their data with colleagues to improve the progress of research and development, some users may make changes to "their own data". In this case, it is difficult to manage data if data ownership is not clear. Data sharing has many benefits for society in general and is particularly important for maintaining the integrity of scientific data. At this point, the degree of data ownership needs to be recalculated based on the value that people derive from shared data.

A new paradigm for ownership can enable better decisions about trading digital assets in the emerging web. It is not easy to declare data ownership when people add content to existing digital assets, especially for files or documents that many people have collaborated on. How data ownership is shared among contributors depends on the nature and extent of the contributions. In the case of files or software, it is difficult to clearly define and handle data ownership in the emerging web data transaction process. The licence required to access software or files is tied to the copyright of the digital asset. At a minimum, a licence must be obtained to access the digital assets of others. Technology is needed to monitor the use of the licence.

Paradigm shift in ownership of digital assets

For commonly traded physical assets (books, buildings, cars, home appliances, music, movies, etc.), the procedures for ownership and asset transactions are clear. However, in the case of software and digital files, it is difficult to clearly define ownership or copyright. It is also difficult to protect ownership or copyright because digital assets can be copied indefinitely.

In the case of software, the management of ownership shares during the software development process is more difficult than the management of patent rights, which are currently widely used. This is because many updates are often made after software is developed. In addition, various functions may be added based on other people's software or modified to apply to new application environments. This is easy to manage if there is a legal process for clearly declaring ownership whenever software is developed, distributed, updated, or modified. However, it is not easy to manage ownership when changes or updates are made arbitrarily without proper legal procedures. In particular, problems arise when the initial value of the software is not large and it is treated lightly because of the cost of managing ownership. However, when the value of the software increases significantly, disputes over ownership or copyright arise. The main cause of disputes is disagreement over the valuation of whether the particular features or additional activities has increased the value of the software.

The value of digital assets varies by type and application, but it goes up and down like the stock market. In the case of digital assets, their value can increase through activities such as business activity or subsequent technological development. However, it is not easy to calculate rewards.

New ways of managing ownership and copyright of software are therefore needed. If applied in the same way as traditional physical assets, it would be difficult for anyone to afford the costs of managing ownership and maintaining ownership disputes. In addition, following the DAO philosophy (i.e., the rules for managing digital assets are managed by a neutral organization rather than a specific company), it is not easy to manage ownership or copyright in the international market. For example, the cost of managing ownership is very high while registering a national patent or an international patent. In conclusion, global trade in digital assets should require minimal costs to register and manage ownership or copyright. There should at least be an international agreement on ownership and copyright of digital assets, although it is impossible to solve all problems. Registration and management of ownership or copyright of digital assets should be very simple and clear. New technological alternatives are expected to be developed to register and manage digital assets in the future. The process of creating, registering, and managing digital assets should be easy for everyone. In addition, it should be easy for anyone to verify ownership of digital assets.

Updating ownership and licence of digital assets

It is necessary to consider how often the ownership or licence of digital assets changes. Houses and cars do not change ownership often. If someone else's house or car is rented, changes occur at least on a daily or hourly basis. However, software or digital files can change ownership much more frequently. Similar to stock market trading, there can be millions of changes per day. Software or AI algorithms may be updated several times a day. In addition, some may be linked to software created by others. New software may be installed in conjunction with existing software.

In a geographically distributed environment, it is not easy to track and manage changes in ownership and licensing of digital assets. This is similar to registering thousands of new mobile phone subscribers and changing or cancelling thousands of mobile phone subscriptions every day. This means that digital asset transactions take a significant amount of time to be contracted, approved, and ultimately paid for. In addition, transactions can be cancelled midway. Additionally, some transactions may be temporarily suspended if there is a legal dispute or concern about money laundering or inappropriate transactions. In the case of a licence agreement, real-time monitoring is required. Companies that own digital assets manage them directly, or digital asset exchanges manage them in real time, like renting a car or other goods.

7.2 ID provisioning for digital assets

Two types of identification are required for trading digital assets.

- Person/organization identity
  - e.g., personal identification numbers, social security numbers, and company/ organization/community IDs, etc.
- Digital object identifiers
  - e.g., bank accounts, email address, social network service (SNS) / short message service (SMS) IDs, token/coupon IDs, physical products codes such as E.164, international standard book number (ISBN) / international standard serial number (ISSN), and GS1, etc.
  - e.g., building, cars, electrical appliances, book, digital files, and audio/video material, etc.

To enter the digital asset market, individuals and organization must use an appropriate identity. When an individual or organization uses multiple identities, identity verification such as know your customer (KYC) can be used to prevent Sybil attacks. When a new digital asset is created, a digital object identifier must be assigned. To declare ownership of digital assets, digital object identifiers must be linked to individual/organization identities.

When a digital asset transaction takes place, the digital asset is associated with the identity of another individual or organization. Ownership is only transferred when the identifier of the digital object is linked to the identity of the individual/organization purchasing it. Secure transactions are possible through the use of DLT, including blockchain. To protect the privacy of digital asset transactions, the identities of individuals/organizations can be hashed or encrypted.

Figure 2 explains the relationship between individual/organization identity, digital asset (mapping to digital object identifier), and their keys to control access. An appropriate public/private key is required to access or verify digital assets owned by individuals and organization. Individuals and organizations need to know which identities they can access to trade digital assets. To protect the privacy of an individual or organization, even if the individual/organization ID is disclosed, it must not reveal who the individual or organization actually is. Privacy is protected because if identity verification like KYC is not required, no one can know who the ID belongs to.

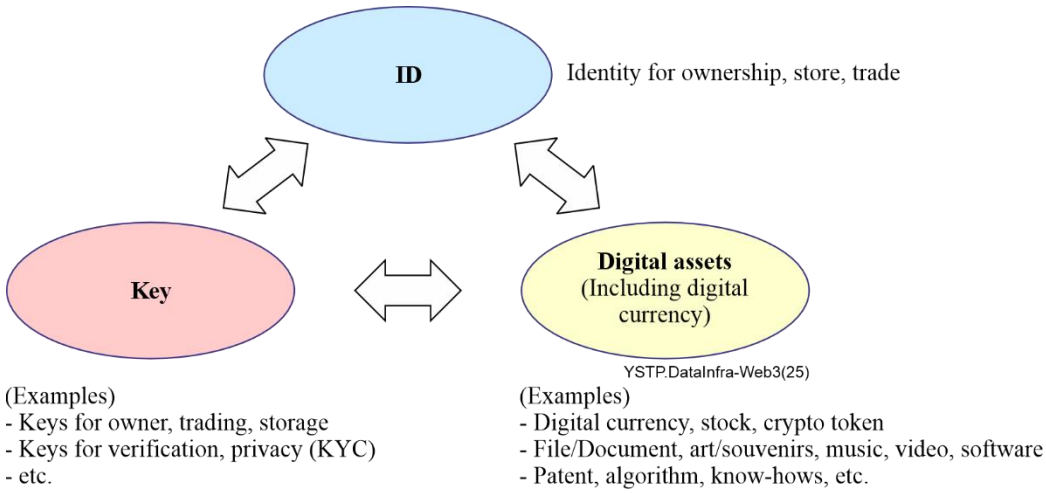

Figure 2 – Relationship among ID, key, and digital assets

Transaction records can use DLT (e.g., blockchain) to prevent inappropriate transactions. Even when all transactions are disclosed using DLT, privacy can be protected for digital asset transactions. In digital asset transactions, public or private key systems can be used to protect privacy and prevent unnecessary actions between sellers and buyers. Private keys are used to access and manage one's own digital assets. Public keys are used to transfer digital assets to others.

Convention and custom of ID allocation

The principle of creating an ID is to make it easy for people to remember. Alternatively, it should be easy for a computer to sort and find. This means that it is recommended to include product type, company name, and easily categorized characteristics to make the ID easily identifiable. It should either help the human memory system or be easy for computers to store and retrieve. In addition, digital assets need to be easy for people to find in order to sell or attract attention. Digital assets are more likely to be traded if search algorithms can easily find them. On the other hand, the ID should be encrypted to protect privacy, and the transaction contract should not be known to others. Even if the ID is randomly generated, it should be possible to block inappropriate transactions immediately. Otherwise, proof of identity (i.e., KYC) is required to verify the identity of the person or organizations holding the ID. This means that there is a trade-off between protecting privacy and blocking illicit transactions.

Next, let's consider whether to assign an ID. When you're launching a new product, it's important to have a unique name that grabs people's attention. This is because the product name has a huge impact on sales. The same is true when people create email addresses or social media IDs. The product ID or name should be easy for others to remember. Sometimes products are given simple nicknames. If the product name is too long or the email address is complicated, the other person may get annoyed or mistype it. Application software can automatically save IDs, even if they are complex. However, if there are many similar IDs on the phone or PC, it can be difficult to find them. This means that when creating an ID, it must be easy to distinguish from other similar IDs and be easy to remember and search for.

Let us look at the habits of how people have used IDs in the past. First, a product can have multiple IDs. Although the product itself is one, producers (manufacturers) and consumers may use different product codes or product names. In some cases, each company that distributes or sells a product has its own unique product code. Product codes must be approved in a sales region. Where there is an internationally standardized code system, international standards must be followed. However, each company may have its own product code. This is similar to how different countries have different naming and telephone number systems.

ID systems vary according to the type of product, such as cars, home appliances, books, music, software, art, paintings, and animation, etc. IDs are also needed to classify and identify professional know-how (expertise), such as cooking skills, medical treatment, and legal interpretation. ID relationships are required between separate pieces of information. In other words, an ID needs to be assigned to each piece of information, and semantic links between ID elements need to be organized. Furthermore, a knowledge map can be built between all information elements, which can be expressed in terms of semantic links between IDs.

ID and key management for privacy and KYC

To register ownership of a digital asset, a digital object identifier must be linked to a person/organization ID. This means that the person/organization ID is used as a means of verifying ownership. This is similar to opening a bank account or obtaining a credit card. Multiple digital assets (e.g., digital object identifiers) can be associated with one identity (e.g., person/organization ID). When ownership of a digital asset changes, the digital asset (digital object identifier) must be changed to the person/organization ID of the other party. If a licence is granted without a change of ownership, there is no need to change the link between the digital object identifier and the person/organization identity. However, temporary IDs may be used for licence management. To pay taxes or detect inappropriate transactions, it is necessary to verify ownership or licensing of digital object identifiers. Sometimes, KYC verification may be required to confirm the true owner of a person/organization identity, which conflicts with privacy protection. However, if a person/organization ID is lost, an identity recovery procedure such as KYC verification is required. If digital object identifiers are lost or stolen, digital assets can be recovered by verifying transaction history (e.g., through digital ledgers or blockchain technology).

Not all digital materials become digital assets, only those that are necessary for transactions are registered as digital assets. A key is needed to manage digital assets. Digital assets can be managed using keys or passwords. To manage licences for digital assets, it is necessary to track where and how the digital assets are being used. If digital assets are being used in violation of permitted regions or regulations, there needs to be a way to stop them.

If the key or password is lost, it can be recovered or reissued through KYC authentication. If the ID cannot be verified to protect privacy, the corresponding digital assets cannot be recovered. In other words, with zero knowledge proof technology, if the ID or key is lost, the digital asset cannot be recovered. KYC verification may be required to recover the ID or key. In this case, privacy protection cannot be guaranteed at that time. There is a trade-off between privacy protection and secure recovery of digital assets.

In extreme cases, individuals or organizations may prefer to give up digital assets rather than expose their identity through KYC. That is, they may decide that giving up digital assets is more beneficial than exposing their identity. In other words, privacy may be more valuable than recovering digital assets. Privacy may be more important than digital asset transactions if exposing the true owners could lead to a large-scale attack or reveal all past activities. There is no need to provide privacy protection for inappropriate transactions because such transactions do not follow normal digital asset transactions anyway. In conclusion, privacy protection should be strictly applied only to normal digital asset transactions.

However, it should be noted that when trading digital assets using a person/organization ID, all digital asset transactions are transparently disclosed and recorded. When using DLT technologies such as blockchain, all transaction records are transparently disclosed within the same domain. This is similar to when a person/organization's bank account is managed in a specific domain, all banks in the same domain can directly or indirectly know the details of the actual individual/organization and the digital asset transactions. Therefore, it is necessary to develop various technologies to protect privacy in a transparent trading environment. The current DID standard developed by W3C can also be used to protect the true owner.

Technical issues for the provisioning of digital asset identification

This clause is a reminder of the traditional ways in which people use identity or identifier. In fact, IDs can be used for any person with whom one wishes to associate, or linked to any object of tangible or intangible value. There are currently a large number of standardized ID mechanisms. When people want to talk to someone or make a transaction, they have to ask for their mobile phone number, know their address, or know their bank account number. Personal information such as a person's phone number, address, and bank account has to be shared with. At this point, it becomes a sensitive privacy issue for the other party to disclose their personal information to others. Decentralized Identity (DID) can be used to protect privacy when trading digital assets, However, if the ID owner is not verified before the initial transaction, the digital assets can be misdirected. (For example, the target bank account to which the digital asset is transferred could be mistaken for a different bank account or the hacker's bank account).

According to the DAO philosophy, ownership must be registered in public/private repository. Ownership registration basically uses the IDs of individuals and organizations. In addition, all digital assets owned by individuals and organizations must be linked (i.e., registered). For global transactions of digital assets, the ownership of the digital asset must be accurately confirmed. However, for purposes such as tax tracking or monitoring inappropriate activity, it is necessary to find out who the individual or organization using the ID actually is. The mere suspicion of inappropriate transactions can be an invasion of privacy. The owner of an ID should not be revealed unless strict procedures are followed. For example, it is similar to trying to find out a smartphone password to investigate an individual's inappropriate activities.

Trust level of person/organizational identity or digital object identifier

Anyone can create their own ID to trade digital assets, just like creating their own email account. Identity authentication (i.e., know your customer) can be performed when creating a one-time ID or to prevent the creation of many IDs.

When digital assets are stored in a corresponding identity that an individual or organization creates, it is very difficult to identify the owner of the digital asset and recover the digital asset if the actual person or organization ID is lost. For example, when you create a bank account and deposit a lot of money into it, it is similar to not being able to retrieve the money in the bank account if you cannot confirm who owns the bank account. Therefore, if an identity belonging to an individual or organization is stolen by a hacker, etc., all digital assets stored in that identity are lost. Another example is that when using an identity to vote online, it is necessary to prevent double voting or voting under someone else's identity.

In summary, identity management is very important. Improper identity management can cause many problems in digital asset transactions. Because the subjects who create identities are humans, human mistakes cannot be prevented. Therefore, when an individual or organization uses their identity to trade digital assets, appropriate procedures are needed to prevent human error.

The best way to address human error in digital asset trading is to establish trust ratings for people and organizations. Traditionally, when buying a car or any other item, the creditworthiness of the seller is very important. Similarly, when trading digital assets, the purchasing process becomes more rigorous if the trust rating is low. And the higher the trust rating, the easier the purchasing process becomes. At the beginning of a digital asset transaction, strict procedures that assume zero-trust model must be followed, starting with verifying the identity of the individual or organization. Later, as the trust rating increases, the transaction process can be relaxed slightly.

7.3 Privacy protection and repositories

Public and private repositories of digital assets

Ownership of digital assets must be registered with the appropriate repository of a neutral organizations according to the DAO philosophy. When registering, ownership must be verified along with the digital asset. To protect privacy, the owner's ID may be encrypted or hashed when verifying ownership. The location of the neutral repository where digital assets are registered and managed must be determined depending on the type of digital asset and the transaction domain. In other words, a public or private repository is required depending on the type or transaction domain of the digital asset.

Private and public repositories should be internationally standardized to prevent indiscriminate installation. This should also include standards for the registration and management of digital assets. Repositories should verify ownership of registered digital assets. Dealing with counterfeit or inappropriate copies of digital assets is an investigative matter, not the operation and management role of the repository. According to the DAO's philosophy, the operation of the repository should not be arbitrarily managed by any specific company. In principle, the registration fee should be free, and the operation and management costs of repositories must be handled by the operator of the digital asset trading system.

When registering digital assets, it is important to classify them according to the type of digital asset. It is also important to easily identify relationships between digital assets. When classifying digital assets, it is important to be able to easily identify their characteristics or differences. This means that classification is important for both buyers and sellers when trading digital assets. In order to trade ideas, know-how, and experience contained in digital assets, it is useful to have semantic relationships between digital assets. If the semantic relationships between digital assets are well organized, the trading environment for digital assets could be greatly improved. It can also reduce the effort required to search and compare existing digital assets. It will also make it easier to create new digital assets using AI.

Demarcation point for privacy

Figure 3 illustrates the privacy demarcation line for trading digital assets in the DLT functional model. In the figure, users are individuals or organizations that own and trade digital assets. DLT nodes are entities that trade digital assets. Digital assets are traded between DLT nodes according to appropriate trading procedures. A digital asset transaction service provider may be required. In the demarcation line, the right direction from the user to the DLT node indicates which digital asset belongs to whom. To protect privacy, a hash algorithm can be used between users and nodes. The left direction from the DLT node to the user does not reveal who owns the DLT node (i.e., the entity that owns the digital asset) without any legal procedures to protect privacy.

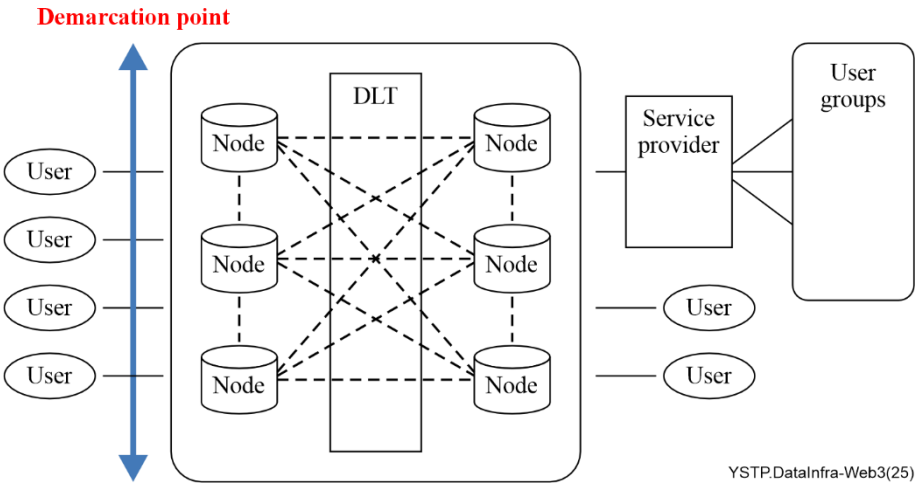

Figure 3 – Demarcation points for privacy

Protecting the privacy of digital asset transactions

To protect privacy, there are many ways to prevent verification of the true owner in digital asset transactions. There are also a number of mathematical algorithms that prevent a user ID from being traced back to its true owner (i.e., prevent backtracking). Techniques such as zero-knowledge proof (ZKP) can be used. In order to protect privacy when trading digital assets, it is necessary to ensure that the true owner of the person/organization ID is unknown. Key issues are the prevention of money laundering and other inappropriate activities and the fair collection of taxes. This can be primarily done by tracking the person/organization identity or digital object identifier rather than tracking the actual owner. The most important thing for safe and secure digital asset transactions is the instance of creating an individual/organizational ID and digital object identifier. The trust class of individuals/organizations can be important when creating IDs. Digital asset transactions may be blocked if a certain level of trust on IDs is not met. Transactions may be assessed immediately if fraudulent personal/organizational IDs or digital object identifiers are used. If real-time detection is difficult, stricter transaction procedures must be followed after non-appropriate transactions. In other words, when a new ID is created, it is necessary to investigate whether the individual or organization has committed any inappropriate acts in the past. This means that the creation instance of a new ID is important because it is impossible to determine whether transactions in digital assets that exceed billions per hour are inappropriate. In fact, it is impossible to prevent non-appropriate transactions during a digital asset transaction. Further use of the person/organization identity or digital object identifier can be blocked only after the inappropriate transaction has been completed. It notes that a new ID can be created immediately and inappropriate transactions can continue while that ID is blocked.

Sometimes, intermediaries can be used to hide the true owner of digital assets. Broker/agent ID can be used to hide the true owner of digital assets. If an inappropriate activity occurs, the broker/agent can reveal the real owner, but first the broker/agent can monitor the non-appropriate activity itself. This is similar to the way people buy real estate or invest in stocks. The question is whether the broker/agent will reveal the true owner of the digital asset. Since most drug transactions and inappropriate activities often use various types of multi-level intermediary companies, it is necessary to closely investigate brokers or agencies when trading digital assets. In conclusion, it is important to verify trustworthiness when creating a new ID of the broker. This is because when a new ID is created, it is not possible to accurately determine whether they are only trading their own digital assets or whether they are relaying the digital asset transactions of others. Therefore, the management of digital asset trading brokers or agencies should be stricter than the direct trading of digital assets between individuals.

In the digital world, verifying the true owner is not easy. Even if KYC is verified using the real owner's fingerprint, iris, DNA, etc., there are cases where it cannot be trusted. This is because even

in the case of fingerprint or iris recognition, if these are converted to digital, they can be copied at any time. Even your mobile ID or mobile driver's licence is always at risk of being copied. In other words, if someone else's mobile ID or driver's licence is surreptitiously copied, it is not easy to verify their identity. It's cumbersome and expensive, but it can be deceptive even when checked for inappropriate copying in real time. KYC verification is not easy without a non-copiable solution. Currently, the traditional method of going directly to the site where the ID card was issued or checking it in real time through live video is the most reliable. In the future, it may be possible to indirectly verify the identity of an individual if unclonable technology is developed.

Storage and wallet of digital assets

Digital assets must be stored in a location identified by the individual or organization's ID. An appropriate key is used to prevent unauthorized access to the digital asset. Because it is a digital file, a major problem occurs if the digital asset storage is hacked. In order to trade digital assets safely, it is necessary to verify the ownership of digital assets and whether they are counterfeit or inappropriate duplicates.

The problem arises when the storage location of digital assets changes as a result of digital asset transactions (transfer of ownership, licensing, etc.). In addition, due to the possibility of digital assets being lost, sellers or buyers may make copies using IPFS interplanetary file system (IPFS) technology, etc. However, even when the ownership of digital assets is transferred to another person, there is a possibility that the seller will keep the original digital assets rather than destroy them. This is similar to secretly duplicating the car keys and keeping them even after you sell the car. In addition, if only a licence is granted, tracking must be possible to determine whether the buyer arbitrarily copies and distributes the digital asset in violation of the licence agreement. If online/offline digital wallets are used simultaneously, multiple transactions of a digital asset may occur using the offline wallet.

7.4 Smart contract and legal inspection

Smart contract of digital asset trading

Digital asset trading can use smart contract technology, which is specified in the DLT standards. However, the smart contract technology currently used in Ethereum does not allow transaction details to be changed once the transaction contract is complete. All transaction details are publicly available and it is difficult to arbitrarily change them without changing the entire ledger using a hash algorithm.

What is important in digital asset trading is the ownership of the digital asset and whether the digital asset is original. First, it is easy to authenticate ownership of digital assets using digital IDs. This is because it is similar to the method people use to prove ownership of physical assets. However, if the method of proving ownership is digital, there is a risk of piracy, so various ways of verifying digital assets may emerge in the future. Second, the most important issue in trading digital assets is whether the digital asset is original. In the case of counterfeits, some way of verifying this is needed. So far, many technologies (e.g., watermark, authentication code, or digital signature, etc.) have appeared to prove originality. However, this work of proving the original is similar to finding out whether a paper has been plagiarized or whether a work of art is authentic. In the future, technologies that use various AI techniques to verify originality may emerge.

The question here is whether DLT such as blockchain can be used to trade digital assets. At present, blockchain technology can only be used for cryptocurrency transactions, but there are many issues as to whether it can be extended to digital asset transactions. In other words, the current blockchain technologies including Ethereum cannot confirm the origin of digital assets or the ownership of digital assets. The current DLT standards are applicable to digital asset transactions, including future digital currencies, but it is necessary to analyse whether they can also be applied to digital asset transactions. It should be noted that the current blockchain technologies does not prove that the digital asset is the original. Blockchain is only a technology that cannot arbitrarily modify transaction details. It cannot

verify whether it is someone else's digital asset. In other words, it cannot prevent counterfeiting or inappropriate activities of digital assets.

Another problem with current blockchain technology is that once a transaction is completed, it cannot be cancelled. This means that even if there is a problem with the digital asset, the transaction cannot be cancelled and all damages must be borne by the person requesting the purchase. Anyone wishing to purchase digital assets does so at their own risk. In other words, additional transaction terms such as contract termination, compensation for damages, etc. cannot be added. Counterfeiting or quality problems of digital assets may occur.

The problem of not being able to withdraw from a transaction contract is not a significant issue in the case of cryptocurrency transactions, but it cannot be applied to digital asset transactions. Unlike cryptocurrency trading, it is more difficult to complete digital asset transactions. In the case of digital assets, even if sufficient pre-trade verification is completed, there is another problem. Even if a transaction contract is concluded, various problems may arise during the payment of the transaction, transfer of ownership of the digital assets, tracking of licence terms, and final approval. This can result in unintended delays or situations that violate laws or trading regulations.

Once ownership of digital assets has been transferred or files of digital assets have been transferred, it is not easy to cancel the transaction. Therefore, it needs to be clear who is responsible if there is a problem with a transaction. In the case of blockchain, the buyer is responsible for all losses, whereas in the case of digital asset transactions, it is difficult for the seller, the buyer, or the business operator facilitating the transaction to avoid some level of responsibility. For digital asset transactions, clearly defining who is responsible makes it easier to establish transaction procedures and ensure accountability in the event of a dispute.

Legal inspection of digital asset trading

When trading digital assets, it should be checked whether the digital asset is legal. This includes not only drugs or weapons, but also counterfeit goods or digital assets that contain intentionally false information. The first step is to check whether it is a digital asset that is prohibited by law from being traded. It is out of scope of this document whether trading in digital assets is permitted without legal regulations. It is necessary to check which digital asset trading is permitted according to regulations (e.g., GDPR, Personal Data Protection Act, etc.). Depending on the region, trading in digital assets may be restricted for some items. Alternatively, trading may be conditionally permitted for certain digital assets, subject to compliance with required procedures. In addition, there may be restrictions on the amount of the transaction or the trading area. Secondly, in a direct transaction, the owner of the digital asset should be confirmed. Brokers or agencies (intermediaries) for relay transactions must take stricter measures against inappropriate activities or breaches of transaction agreements. Third, it must be verified whether the product is an inappropriate copy, imitation, or counterfeit. If a work is plagiarized or someone else's image or artwork is imitated, it should be inspected to what extent it is plagiarism or imitation. Detecting inappropriate copies is technically very difficult. As relevant technologies develop in the future, there can be many ways to detect inappropriate copies or counterfeit products. In conclusion, trading digital assets requires the development of various legal systems and technologies not only to protect privacy but also to create a secure trading platform.

7.5 Data modelling of digital assets

Principle of data modelling

All elements of the data ecosystem can only be processed if the input/output data formats match. Data collection or production devices generate and collect data according to the capability and purpose of the input/output tools. Data classification and storage methods vary according to the purpose for which the data will be used. Data must also consider when and how often it will be used, as well as its cost. Since data cannot be processed directly by humans, a data device or system is required. The basic principle of data modelling is that data should match the format required by the data system

when data is collected, stored, processed, transmitted, and expressed. The data format should also match when data is processed with AI/ML algorithms. Data should always be easily converted during generation, processing, storage, and transmission according to the format required by data devices and systems.

In particular, there has been a lot of interest recently in the reusability of data. Data can be combined with completely different data to create new value and help make good decisions. In other words, no matter how much data are generated, it is more important to use the data to create new value or help make important decisions. In particular, there is a high possibility of creating new value by combining multimodal data or heterogeneous data from other ecosystems that are not yet connected. It is also expected that data to be used not only for simple delivery or web applications, but also to be combined with 3D augmented reality/virtual reality (AR/VR) and IoT technologies by adding AI/ML algorithms. Data can also create new future ecosystems such as the cyber-physical world as well as evolving existing industrial systems. Therefore, data modelling should be able to welcome, flexibly transform, and exploit new ecosystems.

A data model is an abstract model that organizes data elements. The generic data model is similar to that of a natural language. It defines types of relationships such as classification relationships and part-whole relationships. A data model allows the expression of a relationship between a single thing and a group of things that are predefined in a fixed and limited domain. A semantic data model in software engineering is a technique for defining the meaning of data in the context of its interrelationship with other data. Data modelling standards are agreements on representations, formats, and definitions of data. Without data standards, data interoperability problems arise. Therefore, data formats need to be standardized. Data models should be standardized to make it easy to manage and share data. A consensus on a standardized data model needs to bring together interested parties from vendors and consumers, domains, agencies, and professional organizations.

Objectives and key requirements for digital asset data modelling

When people create some documents, they may send them to others via email or file transfer protocol. If people want to make their documents available to the public, they can do so through the web portal sites or private social networking services. If some users find valuable information among millions of documents, including software and application packages, they may want to buy or sell these documents. This is because it takes a lot of time and effort to find or organize documents that are essential for a specific purpose. While creating, sending, and storing digital assets, linked information among digital assets becomes more useful to add the value of digital assets. AI/ML technologies can be used to analyse market trends and user preferences by examining large volumes of digital assets for specific purposes.

There are a few principles to keep in mind when selling or licensing digital assets. The most important thing is to pay for the value of the digital asset. It is necessary to consider not only the value agreed at the time of the transaction, but also the potential value that can be added in the future. It is also necessary to consider when the value of the digital asset will increase or decrease due to various factors. This is because the value of digital assets is constantly changing depending on the situation or conditions. Therefore, when trading data, the change in value of the digital asset should be calculated according to the 5W1H format.

The key issue is how to properly and confidentially sell the digital assets owned by the user. If the user sells the digital assets to the target business customer, there may be concerns about the inappropriate distribution of the digital assets. The user may publish some paid content on a specific domain that should only be available to the subscription customer. However, even if the original content is encrypted with the appropriate security code, the buyer may distribute the received digital assets to others after decrypting the document. They can inappropriately distribute the original digital assets and the key together. In other words, if the buyer intentionally inappropriately distributes the original content to others, the security protection for the digital assets may not be effective. Therefore, it is more reasonable to licence rather than sell the ownership of digital assets. Appropriate tracking

or authentication mechanisms are required even if licensing is done. Otherwise, unacceptable situations may arise during the digital asset transaction.

Review of existing data modelling

When digital data formats were first invented, there were some arguments about character sets depending on the language. The electronic documents had also suffered from many formats that were intended to be used as printed output. During the development of computer network, documents had been distributed in electrical forms rather than printed materials. After the improvement of electric display technologies, it is possible to view documents on screen instead of printing them. However, using electronic documents for final presentation instead of distributing and printing on paper had some problems of multiple incompatible file formats. Even more problems are associated with the complex file formats of different word processing, spreadsheets and graphics software.

Telecommunications and broadcasting applications use electronic document formats for recording and transmission, which include analogue and digitized content. The content can be delivered over transmission channels, encoded in digital form, recorded for storage and processing, and displayed on the screen. For audio/video applications, data serialization model such as MPEG is used to reduce the overall transmission volume.

For Internet applications, most file formats are designed for sending, downloading and processing on the local computer system with digital data storage. Most Internet files can be useful in web applications, but some electronic files are easily accessible only through a web browser. Depending on the type of web pages and web applications, the document formats can be modified or processed to be displayed on the screen. For web applications, the extensible markup language/resource description framework (XML/ RDF) format standardized by the W3C should be used. Technically, an XML Schema is an abstract collection of metadata consisting of a set of schema components, mainly elements, attribute declarations, and complex and simple type definitions. Some file formats such as hypertext markup language (HTML), scalable vector graphics, and source code are used with defined syntaxes. On the web, the Multipurpose Internet mail extensions (MIME) header, comma-separated value (CSV), XML, and Javascript object notation (JSON) data formats are used. The uniform resource locator (URL) is used to identify the accessible location of a web page.

Recently, unstructured file formats of raw sensor data have been widely used by dumping memory or collecting sensor data from IoT devices.

For the identification-related applications by using IoT, the identifier can be used to process the recognition or identification of sensors, devices/systems, and people, as well as objects such as file and application software. A variety of identification codes, including standardized barcodes, are increasingly being used in the industry. Biometrics, iris and voice recognition technologies are being used for identification. Theft and counterfeiting of critical or expensive items such as drugs, food, repair parts, or electronic components will be reduced because manufacturers will be able to know the location of their products.

For the location-based applications, geographic data formats are used to capture, store, manipulate, analyse, share, and display spatial or geographical information. Geographical data is used for location-based services such as transportation/logistics, real estate, public safety, crime mapping, national defence, and climatology. Geospatial data represents real world objects such as roads, land, trees, houses, buildings, and waterways. Also, abstract references such as images, vectors, points, lines, and polygons are mapped to location attributes. A new hybrid data method can identify physical locations by combining three-dimensional vector points in physical space. This location information becomes more realistic and visually descriptive. Recently, the web page with large amounts of geographic data have allowed users to create custom applications and make complex spatial information, which is called the mashup application of the web. An editable map of the geographic data is used to provide street maps, aerial/satellite imagery, geocoding, search, and car navigation. The Open geospatial consortium (OGC) is currently developing open standards for global geospatial

data. The global navigation satellite system (GNSS) provides location and time information for specific applications such as weather forecasting, e-commerce, e-maps and e-navigation.

In computer science and mathematics, the entity-attribute-value (EAV) model is a data model for describing entities where the number of attributes (properties, parameters) that can be used to describe them is potentially vast, but the number actually applicable to a given entity is relatively small. This model is known as the object-attribute-value model, the vertical database model, and the open schema. This data representation is analogous to space-efficient methods of storing a sparse matrix, where only non-empty values are stored. EAV's data type provides a limited set of data types, such as byte, Boolean, Datetime, double and string, in addition to splitting numeric data into int, long, or float. It also defines custom data types such as phone number, e-mail address, geocode, and a medical record. Cloud computing systems provide data stores based on the EAV model, where any number of attributes can be associated with a given entity. XML provides a framework on top of an EAV design and builds an application that has to manage very complex data sets when using EAV models.

Data modelling for digital assets

To create a new digital asset or to convert an existing digital file into a digital asset, the following should be defined: First, each digital asset must have an identifier. For example, it must declare a filename or identifier and include metadata such as author, registration date, creation type, etc. Second, the ownership of digital assets must be declared. In order to know who owns a digital asset, the owner of the asset must be identifiable through the file header or related link information. Third, to protect privacy, individuals or organizations that own digital assets must not be directly identified. This refers to technologies such as Distributed Identifiers (DIDs) that make it impossible to identify owners without legal procedures. Fourth, if special conditions are required when providing, accessing or disclosing digital assets, such as the European GDPR, these restrictions must be explicitly expressed within the digital asset.

Firstly, digital asset identifiers are important in the data modelling of digital assets. They are also known as data tags or data indexes. Data indexes are used to collect, analyse, and store digital assets to enable fast and accurate search engines. Without a data index, search engines would have to scan all the digital assets in a database, which would take a lot of time and computing power. Data indexes enable cross-disciplinary classification and accumulation of concepts and knowledge in linguistics, cognitive psychology, mathematics, and information science. In terms of data modelling, metadata formats can provide an appropriate description of digital assets to inform their use and related applications. Data schemas can be described as thought or behaviour patterns that represent categories of digital assets and the relationships between them. Data schemas represent a set of grammar rules for digital assets in XML/RDF format. They include more specialized rules that express the content of elements and properties of digital assets. Data models of XML/RDF-based digital assets can be indexed, searched, stored, or cross-referenced.

Second, when a digital asset is created, the ownership of the digital asset must be declared. There must be a record of who originally created it and who modified it. The data modelling for the ownership declaration can be recorded in the header of the digital asset or through a separate semantic link. There must be strict restrictions on changing the ownership record of the digital asset, and changes in ownership must be traceable.

Third, in order to protect privacy in the data modelling of digital assets, the creation or trading of digital assets should not contain information that can identify the actual owner. On the other hand, if the encrypted ID or key of the digital asset is damaged, the ownership of the digital asset cannot be recovered normally. In other words, if the ID or key of the digital asset is lost, information that can confirm the ownership of the digital asset must be required in order to recover the digital asset. In this case, privacy may be exposed during the process of recovering the digital asset. Of course, privacy exposure can be controlled to a reasonable extent, but it cannot be completely protected.

8 Overall ICT infrastructure and procedures for digital asset trading

8.1 Stakeholders for digital asset trading

Producers and owners of digital assets

Anyone who creates a digital asset must declare ownership of the digital asset by registering it in a private/public repository. As with patents, unregistered digital assets are not recognized as property. Neutral organizations that operate private/public repositories will go through a registration process to check whether the digital assets have violated any laws, including whether they have been copied in the right way.

To sell digital assets, the terms of the transaction, including the price, must be disclosed. If a buyer wants to review the content or quality of a digital asset, limited access to the digital asset must be provided through a neutral organization. Proof of ownership of the digital assets must also be verified. Neutral authorities can verify the ownership of the digital asset on behalf of the buyer.

Buyer

In order to buy a digital asset, the first decision that needs to be made is whether it is worth buying, whether it is for simple consumption of the digital asset, whether it is for resale to others, or how it can be used after purchase. The buyer must also examine the pricing and terms of purchase, including licensing terms with various options. It should also be checked whether trading in the digital asset is prohibited from being traded or is subject to regulatory restrictions. There may be legal penalties for buying digital assets that are not allowed to be traded.

If the quality or performance of the digital asset does not meet the terms of the original contract, the terms of withdrawal or return of the transaction should be reviewed. In addition, once digital assets have been sold, it is virtually impossible to cancel the transaction, so stricter transaction terms need to be established.

After purchasing digital assets, it is necessary to check the term and conditions to ensure that the digital assets can be shared within your own company or family. In addition, if a seller requests privacy, the privacy policy should be reviewed before trading digital assets. Sometimes, the rules that buyers should follow may be stricter when it comes to transactions involving digital assets. In the case of untrustworthy buyers, there needs to be a means of tracking whether transaction terms (including licences) have been breached.

Buyers receive digital assets upon payment according to agreed transaction terms. Purchased digital assets are protected by their own private key. The buyer must protect the privacy of the seller during the process of purchasing digital assets. In other words, the privacy requested by the seller, such as who bought what digital asset from whom, should be protected.

However, there is a controversial issue from the buyer's perspective. When negotiating a digital asset transaction, the seller's privacy information may be exposed regardless of whether or not the digital asset is purchased. If the seller's credit or trustworthiness is not good or when verifying the ownership and quality of digital assets, much of the seller's privacy information may be exposed. In particular, in this case, even if the buyer does not make the final purchase, a significant amount of the seller's privacy information may be exposed. If the seller's credibility is questioned, the seller has no choice but to disclose the privacy information. In other words, buyers of digital assets can obtain a lot of privacy information about the seller. This method is currently common when attempting to acquire other companies or when purchasing expensive physical assets. When buying digital assets, the breach of confidential business or privacy information can be more serious.

Agent (option)

Trading digital assets is not as simple as selling goods. Digital asset transactions require the trust of both the seller and the buyer, and privacy must be maintained between both parties. In addition,

because most digital assets are delivered in the form of digital files, it is actually very difficult to cancel a transaction.

Therefore, most sellers or buyers who do not understand digital asset trading may rely on agents. First, sellers of digital assets can use agents to sell their digital assets on their behalf. Agents need to understand how much digital assets are worth and whether they can easily be sold at a high price. In addition, the agent will analyse the trust level of the buyer and find the most effective way to collect payment. Even if the digital asset is only licensed, the agents can monitor whether the licence is working properly. Second, buyers can search for digital assets they wish to purchase through agents. Agents need to know transaction terms, including ownership of digital assets. If there is a problem with the digital asset, the agent can help the buyer cancel the contract. Third, the most important role of the agent is to protect the privacy of the seller or buyer of digital assets as much as possible. Agents can also help resolve most contractual and legal process issues. If agents leak various privacy information acquired during the process of brokering a transaction, they may be subject to legal sanctions. While it is difficult to track inappropriate activities, it is relatively easy to manage agents. This allows some restrictions to be imposed on what digital asset transactions can be brokered based on the agent's level of trust.

Digital asset trading providers

Digital asset trading providers configure all environments for digital asset trading contracts. They verify the seller's ownership of the digital assets and confirm that the transaction is legal. They prepare each step of the digital asset transaction and record the transaction details. They protect privacy information and block inappropriate transactions. In addition, they also pay fees and taxes after the transaction is completed, and follow compensation procedures in the event of transaction cancellation or breach of the transaction agreement.

Certificate authority (verifiable registry)

Digital asset trading requires a neutral organization to verify ownership of digital assets and certify/approve the transaction process. Like courts, they have the authority and responsibility to ensure that the digital asset trading ecosystem is well served. To achieve this, it is necessary to manage registration and authentication procedures for all digital assets registered in public and private repositories. Therefore, a neutral certification authority should resolve all legal issues arising from digital asset trading.

Classification of emerging web service providers

In general, emerging web service providers can be classified as follows:

– (type 1) network or infrastructure-based emerging web service providers
– (type 2) cloud or application platform-based emerging web service providers
– (type 3) individual or peer-to-peer (P2P)-based emerging web service providers
– (type 4) public or neutral organization-based emerging web service providers.

8.2 Architectural concept for emerging web services

Figure 4 shows the architectural concept for emerging web services. Users have digital wallets to store digital assets and digital currencies. Offline digital assets, including physical assets such as buildings or cars, can be sold through the digital wallets of individuals or organizations. Users should first register their IDs with an emerging web service provider to sell or buy digital assets. A specific region or application service provider may have repositories/storage to store customers' digital assets. However, users within a specific regions or application platform must also register their IDs in order to trade digital assets. Users may sometimes rely on emerging web agents to avoid the difficulties of trading digital assets through emerging web service providers. This is similar to trading stocks safely through a broker. emerging web service providers should store the digital assets registered by users

in a location suitable for trading. emerging web service providers should also facilitate digital asset trading by providing functions such as ownership or licence management, key and password management, digital asset verification, digital asset trading, and monitoring for inappropriate or abnormal behaviour.

Emerging web services require individual/organizational IDs to be registered with the emerging web service provider. Additional registry information about the ID, such as digital asset items and transaction methods, transaction restrictions or limits, etc., is also registered. Registry options may include how to recover the ID without identity verification (KYC) in case of loss of the ID or password. Naming services for individual/organizational IDs are also required to easily find trading partners. Although based on the DAO philosophy, strict management of ID and registry information is required. This is because it is necessary to prevent identity theft, ID registration for inappropriate transactions, and false naming in order to maintain trust in the IDs.

Emerging web service providers need to store digital assets that individuals or organizations want to trade. If the amount of digital assets is too large or there is no need to transfer them to the emerging web service provider's storage device, only the storage location information of the digital assets is sufficient for sale. If there are many digital assets to trade, categories or menus for digital assets can be prepared to make them easy to find. In addition, customers' digital assets can be stored in other locations to reduce the risk of loss. Of course, unauthorized access to other people's digital assets should also be prevented.

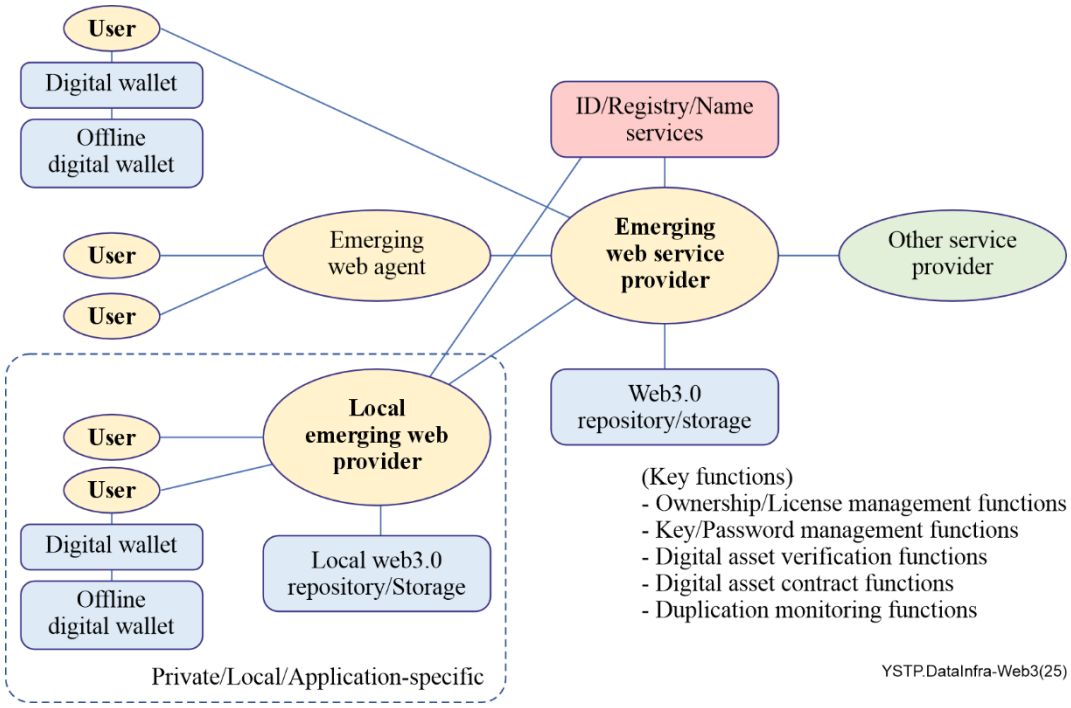

Figure 4 – Architectural concept for emerging web services

When a user wants to purchase another person's digital asset, the user must find the digital asset he or she wants to purchase through the menu or search provided by the emerging web service provider. If the content, quality, and price of the digital asset are appropriate, the user expresses his or her intention to purchase to the emerging web service provider. The emerging web service provider then verifies the ownership or authenticity of the digital asset and initiates the transaction. At this time, the emerging web service provider must check whether there are any problems with the transaction agreement for the digital asset, the payment method for the transaction, or legal issues. If the ownership of the digital asset is not transferred but only a licence agreement is concluded, the emerging web service provider must continuously monitor whether the licence agreement is being

violated. In addition, additional procedures are required if physical objects such as buildings or cars are transferred or only temporary usage rights are granted through digital asset transactions. The emerging web service provider must monitor whether the appropriate contractual terms are met to ensure secure digital asset transactions, and collect fees and pay taxes when the transaction is completed. If the user makes a transaction directly without relying on the emerging web service provider, the user must comply with all of the above contractual terms.

8.3 Components of a trustworthy data infrastructure for emerging web

The trustworthy data infrastructure for the emerging web accommodates existing and future network environments so that everyone around the world can participate. A distributed cloud environment on a wired or wireless network is required to store, process, and transmit data. The user's device for emerging web can be any device capable of exchanging digital assets over the network, not only a traditional smartphone. The application software installed on the user's device must enable consumers to easily find appropriate digital assets. It must provide a means to protect privacy, conduct secure transactions, and make payments. Additionally, purchased digital assets must be stored in a digital wallet, a secure digital storage.

A decentralized cloud platform can safely and securely store digital assets. The cloud platform should provide an environment for trading digital assets. Appropriate procedures are needed to search for digital assets, verify ownership or copyright, trade digital assets, and make payments. AI/ML algorithms may also be installed to block counterfeiting or inappropriate activities in digital asset trading.

The classifications for trading digital assets over a trustworthy data infrastructure are shown in Figure 5. First, there are the digital assets themselves, such as audio/video files or documents. Second, when digital assets are traded, the transaction records with the contract details should be recorded. Finally, traditional currency or cryptocurrency such as Bitcoin is required to pay for the transaction.

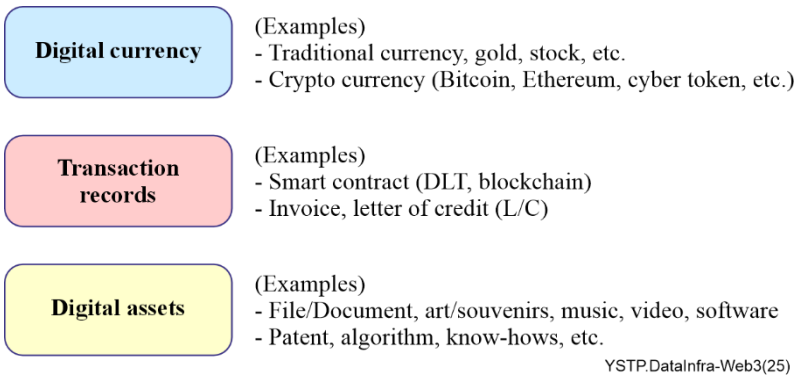

Figure 5 – Classification relating to digital asset trading

8.4 Overall procedure of digital asset trading

The basic principle of digital asset trading is not to trade with untrustworthy parties. If the other parties lose trust in digital asset trading, they will not be able to enter the digital asset trading market. Therefore, loss of trust should be considered the biggest cost factor. For this reason, digital asset trading fundamentally requires a trustworthy data infrastructure.

The procedure for digital asset trading is divided into the following five steps.

- (**Registration**) Registration and ownership verification of digital assets
- (**Contract**) Contract for digital asset transactions
- (**Payment**) Payment for digital assets
- (**Approval**) Approval of digital asset transactions and payment of taxes

- (**Refund**) Cancellation and refund of digital asset transactions

Registration

Registration of digital assets in public/private repositories requires a standardized registration form. Digital asset types (e.g., files, audio/video, AR/VR images, art, software, ideas, algorithms, and combinations of these, etc.) need to be classified. In addition, the owner of the digital asset, the registration date, and the registration location must be registered. During the registration process, the origin and provenance of digital assets should be verified and authenticated. If the authenticity of a digital asset is unclear, or if it is difficult to verify ownership, it is necessary to investigate whether similar registration attempts have been made in other regions or institutions.

Contract

To trade digital assets, the (storage) location of the digital asset is verified. Depending on the type of digital asset, it may be difficult to change the location. It is also necessary to confirm whether ownership is being transferred or only granting the right of use (licence) is being granted. Licence terms including geographic area, frequency, and time of use, need to be negotiated. It is also necessary to confirm whether the transaction is direct between users or through an agent. In the case of transfer of ownership, it should be clarified with the registrar how the seller's digital assets will be transferred to the buyer's digital storage, and when and how ownership will change. It is also necessary to decide whether to make the details of the transaction public or keep them private.

Payment

In digital asset transactions, payment can be made using with a means of value agreed upon by the other party, including traditional currency, gold, stocks, and cryptocurrency, etc. However, when paying, there is a possibility that the value of digital assets may fluctuate depending on the payment date or payment method. In addition, payment methods and fees may vary depending on the intermediary bank or exchange.

Currently, there are various payment methods and conditions in the financial system. When paying for digital assets, it is necessary to negotiate payment terms and penalties. In particular, digital asset transactions require stricter terms because they are much more vulnerable than existing physical assets. When a digital asset contract is terminated, there is no proper means to recover the digital asset and reestablish ownership. In addition, once digital assets are acquired, it is easy to create similar digital assets that imitate them, making it expensive to monitor inappropriate activities.

Approval

When a payment has been made for a digital asset transaction, the transaction must be approved. Once the transaction is complete, the transaction fee and taxes for the transaction should be paid. If there is a problem with an approved transaction in the future, the authorizing body should intervene to resolve the legal issue.

Refund

Since digital asset transactions are much more vulnerable than traditional e-commerce, there may be an increase in contract cancellations and refund requests. There are many refund issues related to the quality of digital assets, contractual issues, and payment issues, etc. In addition, issues of cost and means of detecting inappropriateness, including piracy, need to be addressed when granting ownership or licences as well as trading.

Contract termination and refund issues arise not only from sellers of digital assets, but also from individuals or organizations that purchase those digital assets. It is essential for refunds to monitor whether contract terms are being violated during the process of digital asset trading. In other words, if an individual or organization that is not under legal control, such as a hacker, purchases digital assets and then engages in inappropriate activities, there is no way to stop them.

9 Technical features and key capabilities for digital asset trading

9.1 Technical features for digital asset trading

A new way of managing digital assets for trading is changing the way we work online. It is making it easier for creators to sell their work directly to fans, for businesses to track their goods in a transparent way, and for ordinary people to have more control over their online identities. While there are still some challenges to overcome, decentralized digital asset management (D-DAM) is a key part of the exciting changes taking place in the emerging web world. A decentralized approach is essential to support a system where digital assets are distributed across multiple nodes or servers in a network rather than stored in a single central location. This approach can use blockchain technology and smart contracts to manage users' digital asset portfolios.

Its primary objective is to build trust, efficiency and transparency into the overall lifecycle management of clients' digital assets. Clients are the sole custodians of their digital assets on a platform. There is no central authority or bank involved in the process of digital asset trading. It simply enables digital ledger technology to enable transparency of transaction through specific protocols to ensure data integrity. However, these distributed platforms come with scalability issues and technology risks. Therefore, this approach requires the following key features over traditional centralized systems:

– Ownership and control: Users have true ownership of their digital assets with control over access and permissions.
– Security: Blockchain's immutability and cryptography protect assets from unauthorized access and tampering.
– Transparency: All transactions and activities are recorded on the public ledger, ensuring accountability and auditability.
– Interoperability: Systems can be designed to seamlessly interact with other blockchain applications and services.
– Efficiency: Automated processes through smart contracts streamline asset management tasks.

There are several ways to implement a decentralized approach, including peer-to-peer networks, blockchain-based distributed storage, cloud-based distributed storage and hybrid models. It's necessary to allow users to manage their digital assets transparently and autonomously using blockchain technology, secured by smart contracts. They operate as non-custodial platforms, giving users full control and ownership of their assets. They can delegate access their assets and decision-making to the platform. These platforms can manage a variety of digital assets, including actively managed funds, passive funds, indices and structured baskets. Leveraging blockchain technology, they can generate higher revenues and numerous benefits for emerging web stakeholders.

While traditional solutions offer a familiar and established approach, an emerging web-based solution can offer a more secure, scalable, and resilient alternative that leverages the power of decentralization and blockchain technology. With these characteristics in mind, decentralized digital asset trading for the emerging web should be designed to support the following benefits:

– Enhanced security: Blockchain's immutability and cryptography protect assets from fraud and theft against data breaches and unauthorized access.
– Enhanced transparency and trust: All transactions are recorded on the public ledger, providing greater transparency and accountability.
– Reduced costs: Eliminating intermediaries can significantly reduce transaction fees.
– Improved efficiency: Automated processes through smart contracts streamline transactions and reduce administrative overhead.
– Greater control: Users have direct control over their digital assets, increasing autonomy and privacy, eliminating central points of control and associated risks.

– New revenue models: Enables innovative ways to monetize and share digital assets.

The decentralized digital asset trading mentioned above has the potential to revolutionize the way we manage and interact with digital assets in the emerging data ecosystem for the emerging web.

9.2 Key capabilities for digital asset trading – technical considerations

Emerging web services must provide secure digital asset transactions from digital asset creation to transactions, ownership management, and prevention of non-appropriate activities. The following four core capabilities are required for emerging web services:

– ID management: User authentication, authorization management, KYC functions
– Digital asset management: Creation, storage, transfer, ownership registration, tracking, encryption of digital assets
– Trading management: smart contracts, compliance, tracking of inappropriate activities
– Security management: Digital asset protection, encryption key management.

ID management: technical considerations

– KYC procedures for user registration (ID verification, facial recognition, etc.)
– Multi-factor authentication (2FA, two-factor authentication)
– Role based access control (RBAC)
– De-identification of ID (DID: decentralized identity) and privacy protection.

ID management is a critical component of any digital asset trading platform. It ensures the security and integrity of transactions by verifying user's identities and controlling access to sensitive information. First, individuals or organizations must register their IDs to initiate digital asset trading. KYC procedures require verification of an individual or organization ID, which can be a government-issued ID, passport, or driver's licence. To register an ID, facial recognition technology can be used to compare the submitted photos with a live image. Biometric authentication can use biometric data (e.g., fingerprints, iris scans) for strong authentication. Live cameras can be used to prevent spoofing attacks (e.g., using video analysis or interactive communication). However, the privacy information collected in this process must be managed securely. Compliance with data protection regulations (e.g., GDPR, CCPA) should be ensured.

Second, multi-factor authentication, such as 2FA (two-factor authentication), can be used to prevent unauthorized access to individual or organization IDs. 2FA features can use authentication via text messages (SMS), one-time password generators, or email. hardware security modules (HSMs) can be used to securely generate and store authentication tokens. Different authentication methods can be selected according to the user's convenience. A security key is required for secure multi-factor authentication.

Third, RBAC defines the access control method when accessing an ID. It should clearly define the access control rights according to the user's responsibilities and authority. When the appropriate authority is granted, the access rights to the digital asset transaction are allowed. The method of access control may vary depending on whether physical objects or software/algorithms are involved. Access rights can be differentiated by the user type (e.g., business-to-consumer (B2C) or business-to-business (B2B)), digital asset category, security level, and legal access rights. In addition, legal access rights may include confidential information such as user registration options, passwords, or user biometrics.

Fourth, anonymization technology for ID is necessary to protect privacy. Currently, the DID technology is being standardized by W3C. By using DID, the actual individuals or organizations that own the ID are not disclosed to the public. In DID, a verifiable credential is presented to prove the user's identity. Authorities should store credentials and prevent counterfeiting and tampering of IDs. Credential information of IDs can be stored in a decentralized manner according to the DAO

philosophy. This can reduce the risk of hacking or data leakage from centralized ID management systems and maintain a reliable ID system.

If an ID is lost, identity authentication or an appropriate verification method is required to recover it. The core issue of ID management is to prevent ID duplication. It is also necessary to prevent the theft of other people's IDs or the creation of multiple IDs for malicious purposes.

Digital asset management: technical considerations

– Ownership and metadata management (title, description, creation date, size, etc.)
– Version management
– Watermark, digital signature creation and verification
– Digital wallet (distributed storage of digital assets and offline wallet).

The most important thing in digital asset management is ownership registration. With the concept of DAO, public authority (e.g., the government) manages digital assets according to individual or organization IDs. Ownership registration can use blockchain technology to immutably record ownership information. This is similar to depositing money in a bank account (equivalent to a user ID). Ownership is the registration of digital assets (represented by the digital asset object ID) to the owner's ID. If a digital asset is split between multiple owners, this should be specified when the digital asset is registered. When digital assets are sold, the digital asset object ID is registered to the buyer ID. DLT is necessary to manage ownership transparently and securely when trading digital assets. In addition, all transaction history needs to be securely tracked and managed using smart contract technology. At this time, the widely used TTP (Trusted Third Party) technology can be combined or added. The emerging web service provider must record all changes while individuals or organizations can create, modify, update, transfer, and delete digital assets. To facilitate the purchase of digital assets or the acquisition of licensing rights, emerging web service providers may provide digital asset menus or search engines.

To register digital assets, metadata such as the name, description, creation date, size, format, and keywords of the digital asset are recorded for that ID. The metadata can be standardized in a structured format (e.g., JavaScript object notification for lined data (JSON-LD), RDF) for easy indexing and searching.

Second, the emerging web service provider should manage versions when the content of the digital asset is changed or updated. If digital assets are used in multiple locations, either as a licence, or as a result of changes by the owner, the change must be recorded. In addition, appropriate digital asset management is required when integrating, splitting, or reconstructing multiple digital assets into one.

Third, watermarks or digital signatures should be applied to prevent counterfeiting. This prevents unauthorized duplication of the digital asset. So far, various watermarking and digital signature technologies using blockchain or AI technologies have been investigated.

Fourth, digital assets may be stored in a location specified by the emerging web service provider or in a location specified by the individual or organization. In this case, redundant storage must be possible to prevent the loss of digital assets. Digital wallets should allow digital assets to be stored on-chain (e.g., using a custodial wallet) or off-chain (e.g., using a hardware wallet). Mobile IDs or mobile driving licences can also be stored in digital wallets. Digital wallets need strong security mechanisms to protect against hacking and theft. In addition, real-world assets (RWAs), such as real estate, commodities, or intangible assets, can be traded within emerging web services and tokenized using blockchain technology.

For the future emerging web market, DLT will need to support different file formats such as images, videos, music, and documents, as well as cryptocurrencies. In addition, metadata formats can be extended to provide semantic knowledge links based on the type and content of digital assets. The emerging web service provider platforms should be scalable to accommodate the significant increase in digital asset transactions. It can also support the creation, storage, management, and trading of

digital assets in geographically distributed environments, allowing expansion to global markets as well as smaller regional or application-specific environments.

Trading management: technical considerations

– Transparent management of transaction records using DLT
– Licence tracking of digital asset contracts
– Fee calculation and payment linkage
– Detection and notification of transaction breaches

Emerging web service providers need to keep all digital assets transaction records immutable and transparent. Trading management should consider supporting a wide range of digital asset types, including NFTs, tokens, and real-world assets. First, the creation, modification, update, deletion, and transfer of digital assets must be recorded. In addition, the transaction history of digital assets must be searchable by various conditions such as date, asset type and counterparty. Transaction records based on DLT in line with the DAO philosophy must be transparently disclosed. Emerging web service providers need a transaction management platform based on DLT. In order for users to trade digital assets securely and easily using smart transaction technology, excellent user interfaces and security technologies are required.

Second, where only the right to use digital assets (i.e., the licence) has been acquired, it is necessary to determine whether they are being used in accordance with the terms of the licence agreement. Licence tracking requires the implementation of digital rights management (DRM) mechanisms to control access to licensed digital assets. The emerging web service provider needs to monitor compliance with licence terms and take appropriate action if necessary. Most traditional media, such as movies, music, and dramas, have rights that can only be used in certain regions or spaces. Similarly, licences for digital assets may have regional or territorial restrictions. Decentralized finance (DeFi) protocol can be developed for lending, borrowing and other financial services for trading digital assets.

Third, a fee system should be established based on the transaction type, the asset value and the transaction amount of the digital assets when a transaction is completed. Fees can be integrated with different payment methods (e.g., cryptocurrencies, fiat currencies, or credit cards). Fees can be automated by using smart contracts to calculate and collect fees. In addition, the payment of fees should comply with financial regulations, including anti-money laundering (AML) laws and KYC requirements.

Finally, it must monitor whether there are any violations of transaction rules, such as unauthorized transaction positions or transaction amounts. Emerging technologies such as AI/ML and augmented reality can be updated and enhanced for trading management. The most difficult part of digital asset trading is the transaction cancellation or disputes over the transaction contract. Therefore, buyers should thoroughly check the cancellation policy or disputes before starting the transaction. Emerging web service providers should check that there are no problems with the content or quality of the transaction items to prevent problems. However, when approaching for the purpose of obtaining information about a product or seller (even if there is no actual intention to purchase), special care should be taken not to disclose the seller's privacy information.

In addition, when considering the future of the digital asset trading environment, it is necessary to consider the nature of digital assets, which include intangible knowledge such as software and algorithms, and physical assets such as images, videos, and music. Second, participants in the digital asset trading market include not only individuals or organizations, but also B2B business players such as art, education, games, and asset brokerage companies. Third, it is necessary to consider the scalability of emerging web businesses, which can be regional, national, or global businesses. In addition, the number of participants in the emerging web market can grow to hundreds of millions. In a distributed business environment, scalability and distributed storage technology for emerging

web services are important. Fourth, differentiated access control and security management mechanisms are essential depending on the trust level of the user.

Security management: technical considerations

– Establishing an encryption algorithm and key management system
– Regular security audits and vulnerability remediation
– Defence against distributed denial of service attack (DDoS) attack, establishment of a backup system

First, security is at the heart of digital asset management. This determines the level of trust in the emerging web service business. In particular, security management is very important when dealing with high-value digital assets or protecting privacy that users consider sensitive. Many encryption algorithms (e.g., advanced encryption standard (AES)-256, Rivest-Shamir-Adleman (RSA)) have been developed and various key management systems are used to prevent data leakage or unauthorized access, but it is difficult to provide complete security with technical solutions alone. In general, it is effective to use multiple security algorithms with some level of operator intervention. However, the problem arises from the capital expenditures (CAPEX) / operational expenditures (OPEX) cost of security mechanisms. Due to the burden of operational costs, important security systems may not be installed despite the risk of security accidents. Even if some security solutions are installed, they cannot be perfect, and the operating cost of the security solution is not cheap, so the effectiveness of the security cost must be closely analysed. If expensive digital assets are being traded or too many people are trading at the same time, the damage caused by a security accident is significant, so stricter security management is required.

In addition, when security mechanisms are complex and difficult to use, various security incidents occur. If the operator can easily manage the security system without inconveniencing the user, many security incidents can be prevented. Therefore, it is important to build a differentiated and gradual security system according to the level of security risk and the level of trust of the user (user confidence). In conclusion, it is necessary to conduct more detailed security checks only for users who are likely to behave abnormally based on past records.

Second, security systems such as detecting system vulnerabilities, blocking intrusion attempts, and establishing backup solutions are important to block intruders. Regular vulnerability scans should identify potential weaknesses in the emerging web system. In particular, it is important to block malicious attacks by hackers, install the appropriate security solution according to the security level, and keep it updated.

Third, to deal with DDoS attacks, malicious traffic should be filtered out based on patterns and anomalies. Regular backups of digital assets stored on emerging web service providers should be kept in a physically separate location from the main emerging web service platform. Backup systems should be tested regularly to ensure the recovery plan of the emerging web system in the event of a disaster. Offsite storage can be used to store backups.

10 Value evaluation and profit sharing of digital assets

Until recently, monetizing different types of data such as images, music, videos, and files has been challenging. However, the emerging digital asset ecosystem promises to foster new value creation and enable monetization by transforming unique ideas and know-how into digital assets.

To trade effectively and generate revenue, digital assets must embody added value. Simply transferring or sharing digital assets is not enough to create a vibrant trading environment. Digital assets can reinterpret existing data from a new perspective or give it new meaning through additional processing, integration, and functionality.

Tradable digital assets need to stimulate interest, curiosity, and enjoyment. Therefore, effective promotion of their inherent value is essential. People should be excited about these assets, see their potential and be inspired to innovate and add a creative touch.

Intelligent future user interface/user experience (UI/UX) tools will help transform ideas into digital assets. Devices such as cameras, keyboards, mice, computer graphics (CG), video editors, and audio mixers will be enhanced with AI capabilities. As these advanced AI-integrated tools evolve, they will simplify the creation of new digital assets by intuitively understanding human intent from subtle cues such as heartbeat, breath, voice, hand gestures, and facial expressions. Digital assets created in this innovative way will be traded online, similar to how we personalize and exchange items enriched with our ideas at DIY (do it yourself) flea markets.

10.1 Valuation of digital assets

Digital asset valuation is the process of assessing the economic value of digital assets that are circulated and traded in the marketplace. This establishes an objective value for digital assets, thereby facilitating their circulation and trading in the marketplace. The value of an asset is a measure of the economic benefits derived from production, distribution, trading, and use. In the case of digital assets, the value may vary depending on the purpose of the valuation or the owner. Therefore, valuation is an activity of assessing the value of digital assets in the market, based on generally accepted valuation techniques and models, expressed in terms of rating, grading, scoring, etc. However, valuation is meaningless for items that are not tradable, as it is difficult to expect economic benefits. For example, historical artefacts or certain assets whose ownership cannot be transferred are not considered assets.

In order to evaluate digital data as a digital asset, it should be recognized as an intangible asset through valuation. Also, the evaluation results should be credible. There are generally three standards for valuing digital assets: cost, market, and revenue.

Firstly, similar to the cost of tangible assets, cost-based valuation determines the value by estimating the cost to produce a digital asset. These include labour costs, software and hardware usage fees, and other indirect costs associated with creating and manipulating digital assets. In cases where direct production costs are difficult to estimate, the value may be derived based on the opportunity cost of reproduction, which estimates the current cost of reproducing the digital asset using the same or similar methods.

Next, the market value approach involves comparing and analysing the value of similar digital assets traded in the market to determine value. This approach is the most reliable, as it follows market principles and is useful when there is a sufficient database of similar asset transactions and an active market for trading digital assets. The market value of a digital asset can be assessed if it's possible to compare its characteristics and quality with those of the sample transactions. When comparing, it is important to make appropriate adjustments for significant differences in terms of the transactions.

Lastly, if a digital asset has not yet been traded and therefore has no market value, its value should be based on the expected revenue it can generate. Expected revenue is determined by customers' willingness to pay. For example, the value of a digital photo card of a famous singer may vary based on the singer's reputation, popularity, preference, fan club membership, number of followers, etc. The key variables that reflect the characteristics of the digital asset should first be estimated and then quantitatively converted to determine the value of the asset.

Valuation and disclosure of digital assets are the basic steps in trading digital assets. The problem is that trading decisions often have to be made without looking at the entire data. In addition, even if some of the content is directly verified, the responsibility for incorrect valuations lies entirely with the individual, which hinders the expansion of trading. Therefore, the expansion of the digital asset trading market requires reasonable transactions based on the disclosure of the value of digital assets. Fundamentally, trust in producers, intermediaries, and sellers plays a crucial role.

10.2 Value dynamics and investment in digital assets

It is well known that intangible assets are more difficult to value than tangible assets. One reason for this is that the value of intangible assets tends to fluctuate depending on how they are used. For example, intellectual property rights such as patents, which are a typical example of intangible assets, can increase in value tens or hundreds of times when commercialized. Similarly, the value of the digital assets we deal with can vary greatly depending on the situation. This characteristic allows profits to be made by exploiting changes in value, making digital assets a viable target for investment.

In the financial market, intellectual property (IP) rights are now seen as an investment. A prime example is the use of patents as collateral for bank loans, leading to the creation of IP-backed securities, which allow patent holders to raise funds by utilizing their patents. However, not all intellectual property rights are eligible, only those that are in use. IP rights that a company owns but does not exploit are difficult to value and therefore have a high degree of uncertainty as assets. Conversely, if the value can be proven, digital assets can also become targets for value investment and their development into financial products is possible.

The value of digital assets can be structured to include a fixed value based on cost and a variable value based on usage and interest. The exact value of a digital asset can be calculated by summing the current value accumulated from the past and the expected future value discounted to the present. In other words, the market for digital assets can be structured in a similar way to the current stock market, and investors need to be forward-looking for digital assets that are likely to be in demand in the future. Even in areas that are currently undervalued or of little interest to most people, the intrinsic value or future potential value can be very different. Therefore, it can be expected to see the emergence of digital asset specialists who forecast changes in the value of digital assets based on technology, society, and market demand.

10.3 Value creation in digital assets

1) Creating new value in digital assets through technological innovation

By harnessing the power of data analytics, we can create new value in existing digital assets, including advances such as noise reduction, feature extraction, and enhanced privacy protection. In addition, the application of AI/ML techniques to the processing of raw data enables the generation of sophisticated N-tier data, using esteemed mathematical frameworks such as those of Turing or Ramanujan, alongside predictive and inferential methods based on Heinrich's Law. Furthermore, this approach enables the transformation of previously non-digitized expertise into tangible digital assets from a wider range of fields, including healthcare, transportation, energy, and the environment. Training data for the autonomous operation of physical machines, such as automobiles and aircraft, can also be transformed into valuable digital assets.

2) Creating value synergies by combining digital assets

New value is created through the interaction and convergence of digital assets. This is similar to how various ingredients come together to create new dishes. For example, the convergence of gaming and AR/VR sports has the potential to unlock breakthrough medical treatments. Similarly, the synthesis of cumulative knowledge and expertise from various academic fields can lead to innovative educational methods. Furthermore, advertising and marketing could move beyond their traditional role as promotional tools and become catalysts for creating new cultural phenomena when combined with social events.

3) Creating value through new approaches to digital assets

Digital assets will create new value not only through their transactional exchange, but also within the structure of the trading processes itself. This is, that is, the acts of buying and selling, combined with the tasks of valuing, comparing, sharing, and promoting these assets, may become a cultural phenomenon in itself and reflect a playful endeavour. Furthermore, the process of creating digital

assets will be a creative activity similar to assembling Lego blocks, where the imagination has no limits.

10.4 Trading and negotiation model for digital assets

Various models for trading digital assets can emerge in the near future. First, digital asset trading is an extension of existing e-commerce methods. It is expected that online e-commerce, currently used worldwide, will expand to digital asset trading. Second, a new digital asset trading model expands the concept of knowledge sharing. The software development method is widely used in the open-source community, and is free for anyone to use, but a fee is charged for monetization. What is jointly developed by several people will be monetized later and the profits will be shared. Third, stock trading will expand to include digital assets. Just as Bitcoin was recently approved, many digital assets such as game items, comics, and graphic art can be traded like stocks.

As new technologies emerge, various models for trading digital assets may emerge. New digital assets suitable for applications such as medicine, health, art, music, and games may be invented. In addition, new digital asset trading technologies that meet the requirements of DLT may be developed. As a new digital asset trading ecosystem evolves, new forms of digital assets can stimulate the five human senses. Digital assets with added AI/ML technology can be applied to mobile vehicles and buildings.

The following classifications can be considered to define the trading model for digital assets:

– By type of digital asset (e.g., digital file/material, audio/video, art/music, patents, product, land, car, etc.)
– By trading model (e.g., licence only without transfer of ownership, free or conditional licence, usage period and limit, privacy, legal regulation, etc.)
– By technology and platform (e.g., e-commerce, game, medical/health, SNS/music/video, file/document, etc.)
– Compatibility with existing on-/off-line commerce and sharing economy
– Development of technology to support new DLT.

10.5 Profit sharing in digital assets trading

The method of sharing profits from digital assets may have relied on the existing online platforms to calculate and distribute revenue. This approach is inherently platform-dependent, leaving users vulnerable to changes in platform policies. The problem with platform-dependent digital asset trading methods is that users who generate profits outside the platform or are not recognized by the platform may be completely excluded from profit distribution. To solve these limitations, a digital asset trading system based on the DAO principle should be built to track the ownership and use of digital assets and ensure fair profit distribution among asset owners, users, and traders.

The profit-sharing process for digital asset transactions should be designed according to agreed standards among stakeholders. Transaction data should be transparently recorded and made available for verification when necessary. Blockchain or other DLT technologies are essential to ensure the reliability of contracts made between the parties.

Profit-sharing criteria should be adjusted to the nature of the transaction, the roles of stakeholders, and their respective priorities. Factors such as the contributions of each participant, the risks borne by asset providers, and the operating costs of the platform should all be considered. These criteria can be quantified and used to define distribution ratios that reflect the outcomes of stakeholder negotiations.

Smart contracts can automate profit distribution. These contracts encode the agreed-upon rules for profit sharing and automatically execute when certain conditions are met. This ensures quick and efficient distribution while minimizing the possibility for disputes. To maintain flexibility, smart

contracts must be updated to accommodate changes in stakeholder agreements or changing circumstances.

10.6 Value evaluation and growth of digital asset trading

Digital asset transactions require the prior evaluation of assets. To ensure that these assets serve as reliable foundational data for valuation, it must be possible to trace and aggregate the cash flows generated by the assets. For companies, this process is enforced through accounting standards such as international financial reporting standards (IFRS) or generally accepted accounting principles (GAAP), which mandate the preparation and disclosure of financial statements. Similarly, for buildings, information such as location, officially disclosed land prices, and rental income is made publicly available in accordance with legal regulations. However, when it comes to royalties generated from the licensing of asset usage, the scale and details of these contracts remain opaque.

The same principle should apply to digital assets, whereby all transactions must be recorded consistently (standardized) and transparently aggregated. While companies undergo audits by accountants to verify financial data, it is often impractical to dispatch auditors for every case of asset usage. This makes it crucial to ensure that revenue streams related to asset usage (e.g., royalty payments) are transparently and reliably recorded. Therefore, to effectively manage revenue and, furthermore, enable the creation of additional added value, it is essential to implement transparency and standardization of contracts through mechanisms such as usage tokens that represent cash flows of transactions. Moreover, the use of smart contracts can further enhance the reliability of these agreements.

If an evaluation model is built on this foundation, digital asset transactions are expected to become more active. The general public typically demands a minimum amount of information for making transactions. For example, assets such as academic papers or digital images are difficult to trade without expert appraisal since there are no clear criteria for determining their value. People often worry about whether the artwork they purchase might hold little value, which hinders the initiation of transactions. However, even for assets with no established market value, providing basic reference data for valuation can encourage individuals to assess and trade the assets based on their own judgments. In some cases, individual perspectives on potential asset returns may even surpass those of experts.

The activation of asset-based token trading markets holds the potential not only to increase the tradability of assets but also to create much greater value. Some assets gain significantly more meaning and utility when combined with others than when they exist independently. For instance, payment data from restaurant businesses becomes far more valuable when combined with menu sales data, allowing for the identification of marketing targets. Similarly, combining regional stay data from telecommunications providers with card payment data from financial institutions can yield valuable insights into the tourism industry of specific regions.

From this perspective, a digital asset ecosystem with an active trading market can create synergies through the dynamic integration of data. Tokenization would enable the trading of a wide range of data – from minor, previously untradeable data to large-scale datasets – leading to an explosive increase in the quantity of tradeable data. If digital assets are designed with tokenization in mind from the creation stage and are distributed into appropriately sized units for trading, the liquidity of digital assets will naturally improve. Increased liquidity can exponentially raise the probability of meaningful combinations between digital assets, ultimately driving the geometric growth and expansion of asset value.

11 Applications for digital asset trading

Emerging web technologies for digital asset trading have the potential to transform a variety of markets and user experiences. First, digital asset trading can make trading in capital markets more convenient and faster. It can streamline the online electronic trading process combined with digital

currency. Second, digital ledger technology can improve the security and efficiency of trading various types of digital assets, including traditional assets such as physical goods, stocks, and bonds. Tokenization of these physical assets can represent ownership more efficiently and clearly. Third, smartphones and web-based applications can enable a wider audience to purchase products, trade digital assets, and make payments with tokens. In particular, the convenience of mobile devices lowers the barrier to entry for participating in the emerging web market. Fourth, digital content that can be traded can include all types of digital assets, such as photos, music, animation, comics, videos, and artwork. Fifth, the creation of new cyberspaces using augmented reality/virtual reality (AR/VR) devices can provide metaverses and virtual experience platforms where users can interact and engage with digital content.

Decentralized finance (DeFi) applications

DeFi is an eclectic mix of DLT, digital assets and financial services that aims to disintermediate finance. DeFi is revolutionizing finance, starting with exchanges, derivatives, asset management, lending, insurance and digital coins. Unlike traditional finance, which relies on intermediaries to manage and process financial services, DeFi operates in a decentralized environment. Decentralized applications (dApps) are built on public, permissionless blockchains, and services are typically encoded in open-source software protocols and smart contracts.

DeFi eliminates the high fees charged by banks, brokerages, and other financial institutions. DeFi enables faster and more efficient transactions, reduces counterparty risk, increases transparency through greater functional interoperability, improves accountability, gives stakeholders more control, and enables permissionless and rapid innovation. In addition, as an open-source protocol, anyone can build on top of the platform, providing the opportunity for an additional return on investment that far exceeds the benefits offered by traditional markets. The financial service industry will accelerate the adoption of emerging web in order to support new financial services based on smart contracts on distributed ledger networks.

Decentralized finance (DeFi) innovation enables P2P lending without intermediaries in the lending and borrowing process. Second, decentralized finance can provide various compensation when agricultural production changes due to climate or weather changes. Third, decentralized insurance contracts can provide coverage for various risks arising from digital asset transactions.

While digital asset trading technology offers immense potential, it is crucial to approach it with caution and a clear understanding of the risks involved. As the emerging web technology matures, it is likely to become an integrated part of the future financial ecosystem.

Tokenized real-world assets (RWAs) applications

Emerging web technology can improve existing online or offline transaction methods (e.g., real estate, cars, art, electronics, books, etc.). In addition, if buildings or cars can be easily used with simple tokenized usage contracts without complex transaction contracts, the utilization of physical assets will increase and the value of real assets will increase. A new transaction method for real world assets can revolutionize the way gold and silver or stocks were traded, or the way agricultural products produced by oneself were traded in the market. The emerging web technologies for real-world asset trading can offer additional benefits, such as fractional ownership and increased liquidity, in addition to the benefits of transparency and transaction costs.

– (**Real estate**) Real estate can be traded as fractional ownership of the real-world asset through tokenization. Many small shareholders can own large buildings or real assets that they would not be able to afford on their own through small, tokenized ownership rights. This allows small shareholders to easily make large investments in places like the stock market. In addition, tokens can be issued to easily raise the necessary funds when large-scale social overhead capital (SOC) investments are required, such as road and railway infrastructure. Using emerging web technology, it is possible to achieve much greater benefits in terms of cost efficiency and transaction activation than the existing stock or bond markets.

– (**Art and collectibles**) Physical assets, such as paintings or rare collectibles, can be jointly owned by multiple people through tokenization. Artists can create and sell unique digital art pieces as non-fungible tokens (NFTs), providing a new revenue stream. Furthermore, they can establish provenance, avoiding the risk of piracy. Using emerging web technology, it is easy to secure ownership and usage rights for secondary creations or derivative works as well as the existing art.
– (**Commodity tokenization**) Commodities such as gold, oil, and agricultural products can be jointly owned by many people using tokenized digital assets. This allows for shared ownership and easier trading of these assets. For example, instead of physically storing and trading gold, investors can trade digital tokens representing ownership of a specific quantity of gold. This can improve efficiency, reduce storage costs, and increase liquidity.

Supply chain management applications

Emerging web technology is for managing transaction records and the movement of goods in the transaction value chain. It is necessary to provide transparency in the transaction of goods, track the status of transactions in real time, and prevent inappropriate activities or fraud. In addition, since more than tens of billions of transactions are made every day, transaction automation technology is required according to the terms of the contract. emerging web technology can reduce costs and improve efficiency in the transaction value chain of digital assets and the existing logistics industry.

– (**Track and trace**) emerging web technology enables tracking of goods and digital assets as they move through the transaction value chain. Each step from origin to delivery can be transparently recorded. This allows businesses and consumers to monitor the location and condition of their products in real time, improving visibility and accountability. This is especially useful for high-value items, perishable goods, or products that require special handling conditions. In addition, files such as certificates, transaction contracts, and software can be tracked in the same way.
– (**Provenance verification**) emerging web technology can be used to verify the authenticity and origin of a product. By recording key information about the history of a product, such as the date of manufacture, the origin of the material, and certification, using DLT, consumers can easily verify the origin of the product and confirm that it is not counterfeit. This is essential for industries that handle luxury goods, pharmaceuticals, and food, where counterfeiting is a serious problem.
– (**Smart contracts for payments**) Smart contracts are self-executing contracts whose terms are written directly into the code. In supply chain management, smart contracts can automate payments when certain conditions are met. For example, a supplier can be automatically paid when the goods are delivered and recorded on the blockchain. This eliminates the need for manual processing and reduces the risk of payment delays or disputes.

Identity and credential verification applications

Emerging web technologies can enhance user control over identity and credential verification. Users want to have safe and secure control over their personal information. They also need to prevent unintentional sharing of personal information across multiple organizations in a distributed environment. They need to prevent inappropriate forgery of personal/organizational identifiers or inappropriate use of certificates. They also need interoperability so that numerous identifiers or certificates created by organizations or individuals in cyberspace can be used across different regions or organizations.

– (**Self-sovereign identity**) Self-sovereign identity (SSI) allows individuals to control their own digital identity without relying on a central authority. Organizations and individuals can store their personal data in a secure digital wallet, which stores their digital credentials. They can selectively share certain information (e.g., the age at which they can purchase age-restricted products) with the verifier without revealing unnecessary details. This gives users

more control over their data and reduces the risk of data breaches that can occur on centralized platforms.

– (**Secure credential sharing**). emerging web technologies enable organizations to share credentials securely and privately. When individuals need to prove certain attributes (e.g., education, professional qualifications), they can present verifiable credentials issued by a trusted, neutral authority. Organizations can verify the authenticity of credentials without storing or accessing the underlying personal data. This improves privacy and reduces the burden on neutral organizations to manage and protect sensitive information.

Corporate actions and capital markets applications

Emerging web technology offers significant potential to modernize and improve efficiency in corporate actions and capital markets by automating processes, increasing transparency, reducing costs, and enhancing security.

– (**Tokenized securities**) Traditional financial instruments such as stocks, bonds, and other assets are represented by digital tokens. This process offers several advantages. First, it allows a wider range of investors to participate by dividing their ownership into smaller tokens. Second, trading on emerging web platforms is faster and more efficient than traditional stock exchanges, potentially increasing liquidity. Third, smart contracts can automatically enforce regulatory requirements, reducing manual oversight and potential errors. Fourth, trade settlement can be much faster, potentially in near real time.

– (**Dividend Payments**) Smart contracts can automate the distribution of dividends to token holders. When a company declares a dividend, the smart contract automatically calculates and distributes the appropriate amount to each token holder based on their holdings. This eliminates manual processing, reduces administrative costs, and ensures timely and transparent payments.

– (**Voting**) emerging web technology provides a secure and transparent platform for voting. Each token can also represent a vote. The voting process is recorded on the blockchain, creating an immutable audit trail that increases transparency and prevents fraud. This can lead to several benefits. First, making voting more accessible and convenient can encourage greater participation. Second, it increases trust and accountability by providing a clear and auditable record of every vote. Third, it eliminates the costs associated with traditional voting processes.

Decentralized autonomous organizations (DAOs) applications

DAOs provide a new way to organize and manage organizations, projects, and even virtual worlds, empowering communities and promoting greater transparency and accountability. The main features of DAOs are: Decentralization with no single governing authority; Smart contracts are automatically encoded and executed according to emerging web rules; All transactions and decisions are transparently recorded; Decisions are made through consensus and voting of members.

– (**Collective decision-making**) DAOs facilitate decentralized governance and decision-making. Instead of relying on a central authority, decisions are made through consensus and voting by DAO members. This allows for more decentralized and transparent governance, where all participants have a say. The rules of a DAO can be written into smart contracts, which can automatically execute decisions based on agreed-upon rules.

– (**Community-driven projects**) DAOs can be used to fund and manage community-driven projects. Members can contribute funds based on the DAO's philosophy, which can be used to support projects that align with the DAO's goals. This allows for more transparent and accountable funding, as all transactions are recorded. It also gives people the power to directly support projects they believe in. These projects can be anything from open-source software development to local community initiatives.

– **(DAO-powered worlds)** The DAO philosophy of emerging web empowers community members to govern, develop, and evolve their virtual worlds. That is, decisions about the rules, economy, and content of the virtual world are made collectively by DAO members, rather than by a centralized platform provider. This allows for a more engaging and immersive experience for virtual world participants.

Applications for decentralized social networking services

– (**Social tokens**) Influencers can create their own digital social tokens that fans can use to invest in the success of their proposed activities. These tokens can be used to develop exclusive content or ideas, participate in community governance, or simply support the activity. These tokens can grant holders a variety of benefits, such as access to behind-the-scenes content, early access to releases, or the ability to participate in voting and decisions. Social tokens can be traded to allow users to invest in the potential of creators and communities.

– (**NFT-based content**) Influencers can tokenize their content as NFTs, such as exclusive photos, videos, or digital art. Tokenizing digital contents enables to collect unique digital items from favourite creators. Also, NFTs can be bought, sold, and traded on social networking service platform, creating the potential for secondary markets and price appreciation.

– (**Creator economy platforms**) A social networking platform with emerging web features allows creators to directly monetize their content by sending cryptocurrency directly to creators. Creators can also offer exclusive content or community access through paid subscriptions. Integration with e-commerce allows for direct sales of physical or digital contents.

Gaming applications

Emerging web technologies can give players ownership of in-game assets. They can create a game economy similar to Real-World Assets, where game items have real-world value. In addition, play-to-earn models can reward players for their participation. Furthermore, if interoperability between different game platforms is possible, digital asset trading between different game platforms becomes possible.

– (**In-game economies**) In-game items such as land, characters, and goods acquired or owned by game players can be traded in the form of digital assets. Land, characters, and other assets can create a digital asset economy within the game. Game players can create their own marketplaces where they can own these items and trade them with other players. Furthermore, items within the game can be linked to other game platforms for trading.

– **(NFT-based items)** Game developers can create unique non-fungible tokens (NFTs) that represent in-game items such as weapons, armor, or virtual land. This ensures scarcity and verifiable ownership of these items. Players can then buy, sell, and trade these NFTs in-game or external game platforms. This allows players to potentially earn revenue within the game.

– (**Play-to-earn models**) Cryptocurrency can be earned by achieving certain goals or gaining experience while playing the game. This is a key aspect of GameFi where players can earn crypto tokens or other digital assets by playing the game. This can be achieved through various mechanisms, such as completing quests, winning battles, or contributing to the game's ecosystem. This model encourages player engagement and creates new economic opportunities within the gaming world.

– (**Tokenized in-game currencies**) Game developers can create an interoperable game token that can be used across multiple games, fostering a vibrant gaming ecosystem. Game developers can create their own tokens or use existing ones as in-game platform. This can create game tokens that can be used across multiple game platform, fostering a larger and

more interconnected gaming ecosystem. Game tokens can allow players to participate in the platform's revenue sharing.

Metaverse and virtual experiences applications

Emerging web technologies can contribute to the development of an interconnected and economically viable metaverse. Users can own digital assets within the metaverse, including land, items, and experiences. Virtual economies can emerge as new ways to generate revenue and value. Immersive experiences can create more engaging and interactive virtual environments. There are new marketing and advertising opportunities through metaverses and virtual experiences that consumers can actively participate in. However, interoperability issues that connect different virtual worlds and experiences must be addressed.

– (**Virtual land ownership**) Users can purchase and own virtual land, creating digital real estate that can be developed and monetized. Digital real estate can be developed, customized, and monetized in a variety of ways, such as building virtual stores, hosting events, or renting out space. This will create a digital economy within the metaverse that is similar to a real-world real estate market.
– **(Token-based access)** Access to certain areas of the metaverse can be controlled through token-gated access, creating exclusive experiences. Users who hold a specific token (often an NFT) can gain exclusive admission. This can be used to access exclusive concerts, private parties, or premium contents.
– **(Metaverse integration)** Games can integrate with the metaverse, allowing players to use their in-game assets (characters, items, etc.) across different virtual worlds. This creates a more interconnected and persistent gaming experience, where tokens or artifacts earned in one game can have the same value in other virtual environments. This allows for interoperability and a more integrated metaverse experience.
– **(Virtual events)** Organizers can host a variety of virtual events within the metaverse, including concerts, conferences, exhibitions, and product launches. Tickets to these events can be sold as NFTs, providing verifiable ownership and potentially creating a secondary market for ticket resale.
– **(Virtual experiences)** Users can create and sell immersive virtual experiences, such as virtual tours of historical sites, educational simulations, or interactive storytelling experiences. These experiences can be monetized through direct sales, rentals, or subscriptions.
– **(Virtual advertising)** Brands can advertise their products and services within virtual worlds, reaching a new audience. This can take various forms, such as virtual billboards, sponsored events, or interactive product placements within virtual environments.

The emerging web applications for the digital asset trading are summarized as follows:

Decentralized finance (DeFi):

– Aims to disintermediate finance by operating in a decentralized environment using dApps, smart contracts, and open-source protocols.
– Offers benefits like lower fees, faster transactions, reduced counterparty risk, increased transparency, and greater user control.
– Enables P2P lending, provides compensation for agricultural losses due to climate change, and offers decentralized insurance for digital asset transactions.

Tokenized real-world assets (RWAs):

– Improves existing transaction methods for assets like real estate, cars, art, and commodities through tokenization.

– Benefits include fractional ownership, increased liquidity, transparency, and reduced transaction costs.
– Examples:
  - **Real estate:** Fractional ownership of properties, easier fundraising for large-scale infrastructure projects.
  - **Art and collectibles:** Joint ownership, new revenue streams for artists through NFTs, provenance verification.
  - **Commodities:** Shared ownership and easier trading of commodities like gold and oil.

Supply chain management:
– Enhances transparency, traceability, and efficiency in supply chains.
– Examples:
  - Track and trace: Real-time monitoring of goods and digital assets throughout the supply chain.
  - Provenance verification: Verifying the authenticity and origin of products.
  - Smart contracts for payments: Automating payments upon fulfilment of predefined conditions.

Identity and credential verification:
– Gives users greater control over their digital identities and credentials.
– Examples:
  - Self-sovereign identity (SSI): Users control their data and selectively share verified credentials.
  - Secure credential sharing: Organizations can verify credentials without accessing underlying personal data.

Corporate actions and capital markets:
– Modernizes and improves efficiency through automation, transparency, and security.
– Examples:
  - Tokenized securities: Fractional ownership, increased liquidity, automated compliance, faster settlement.
  - Dividend payments: Automated distribution of dividends to token holders.
  - Shareholder Voting: Secure and transparent voting process recorded on the blockchain.

Decentralized autonomous organizations (DAOs):
– Provide a new way to organize and manage organizations, projects, and virtual worlds.
– Key features: Decentralization, smart contract-based rules, transparency, community governance.
– Examples:
  - Collective decision-making: Decentralized governance through proposals and voting.
  - Community-driven Projects: Funding and managing projects through community contributions.
  - DAO-powered worlds: Community governance of virtual worlds.

Decentralized social networking services:
– Empowers creators and gives users control over their data and digital assets.

– Examples:
  - Social tokens: Influencers create tokens for fan engagement and investment.
  - NFT-based content: Tokenizing content for verifiable ownership and trading.
  - Creator economy platforms: Direct monetization through tips, subscriptions, and merchandise sales.

Gaming (GameFi):

– Gives players ownership of in-game assets and creates real-world value.
– Examples:
  - In-game economies: Trading of in-game items as digital assets.
  - NFT-based items: Unique and tradable in-game items represented by NFTs.
  - Play-to-earn models: Earning cryptocurrency through gameplay.
  - Tokenized in-game currencies: Interoperable currencies across multiple games.

Metaverse and virtual experiences:

– Creates interconnected and economically viable virtual worlds.
– Examples:
  - Virtual land ownership: Buying, developing, and monetizing virtual land.
  - Token-based access: Exclusive access to areas or events through token ownership.
  - Metaverse integration: Using in-game assets across different virtual worlds.
  - Virtual events: Hosting and ticketing virtual events using NFTs.
  - Virtual experiences: Creating and selling immersive virtual experiences.
  - Virtual advertising: Brands advertising within virtual worlds.

In conclusion, emerging web technologies can transform various industries by promoting decentralization, transparency, security, and user empowerment. They highlight the potential for new economic models, enhanced user experiences, and increased efficiency across diverse sectors.

Appendix I

Data processing and considerations in data modelling of digital assets

Types of digital asset include, but are not exclusive to: software, photography, logos, illustrations, animations, audiovisual media, presentations, spreadsheets, digital paintings, word documents, electronic mails, websites, and a multitude of other digital formats and their respective metadata. The number of different types of digital assets is exponentially increasing due to the rising number of devices that leverage these assets, such as smartphones, which are conduits for digital media. New digital assets, including certain types of cryptocurrency and non-fungible tokens, are created every day.

Any structured information that defines a specification of any form of digital asset is referred to as metadata. In the representation of digital assets, catalogues, inventories, registers and other similar standardized forms of organizing, managing and retrieving resources are also applied with containing metadata. The metadata can be stored and contained directly within the file, and it refers to or independently from it with the help of other forms of data management. The more metadata assigned to an asset, the easier it gets to categorize it, especially as the amount of information grows. The asset's value rises the more metadata it has for it becomes more accessible, easier to manage, and more complex.

The platform to manage the data of digital assets supports a software function to store, manage, retrieve and distribute digital assets, and it provides the following functions (see Figure I.1):

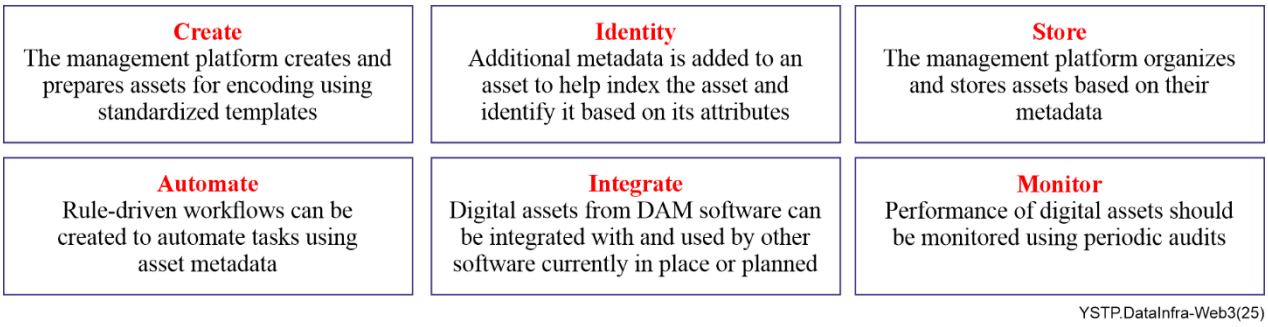

Figure I.1 – Functions for digital asset management

I.1 Data fabric processing in data modelling of digital assets

Data fabric is an approach to data management. Its approach to handling data is based on the way information is stored in the human brain, using principles like plasticity and continuous reorganization to optimize the connections between points of data and create a more efficient data structure. A data fabric is a conceptual or overarching architectural design being popularized by today's data architects to help with overall data connectivity and enterprise data management. A data fabric model is inherently structured to facilitate the coming together of various data environments through the use of a more holistic or unified architecture design. Data fabric as an architectural approach is really about simplification. A fabric model is designed to simplify data access in an organization allowing for easier self-service data access and consumption across the enterprise.

The emergence of IoT, rise in unstructured data volume, and increasing frequency and complexity of analytics requests the need for a more flexible data management solution. Data fabric offers a new solution, supporting dynamic delivery of semantically enriched data. By weaving together data from internal silos and external sources, data fabric creates a network of information to power countless business applications, AI, and analytics across your enterprise. Thus, an enterprise knowledge graph of data model is the key ingredient to transforming existing data infrastructure into a data fabric. The

platform to support data fabric accomplishes this through a unique combination of graph, virtualization, and inference.

I.2 Data mesh processing in data modelling of digital assets

Data mesh is an architecture that relies on a decentralized approach to data management with data as a product, where functional teams are responsible and accountable for their data domains. The goal of a data mesh in digital asset management is to streamline and simplify access to enterprise data and digital asset data make it easily accessible by consuming parties and applications in the organization.

Organizations have multiple data sources from different lines of business that must be integrated for analytics. A data mesh architecture effectively unites the disparate data sources and links them together through centrally managed data sharing and governance guidelines. Business functions can maintain control over how shared data is accessed, who accesses it, and in what formats it is accessed. A data mesh adds complexities to architecture but also brings efficiency by improving data access, security, and scalability.

Data mesh architecture for digital asset attempts to solve these challenges by empowering business units to have high autonomy and ownership of their data domain. The benefits of data mesh architecture are given below.

– **Decentralized data processing**: A data mesh transfers data control to domain experts who create meaningful data products within a decentralized governance framework. Data consumers also request access to the data products and seek approvals or changes directly from data owners. As a result, everyone gets faster access to relevant data, and faster access improves business agility.

– **Increased flexibility**: Centralized data infrastructure is more complex and requires collaboration to maintain and modify. Instead, the data mesh reorganizes the technical implementation of the central system to the business domains. This removes central data pipelines and reduces operational bottlenecks and technical strains on the system.

– **Cost efficiency**: Distributed data architecture moves away from batch processing, instead promoting real-time data streaming adoption. You improve visibility into resource allocation and storage costs, resulting in better budgeting and reduced costs.

– **Improved data discovery**: A data mesh model prevents data silos from forming around central engineering teams. It also reduces the risk of data asset getting locked within different business domain systems. Instead, the central data management framework governs and records the data available in the organization. For example, domain teams automatically register their data in a central registry.

– **Strengthened security and compliance**: Data mesh architectures enforce data security policies both within and between domains. They provide centralized monitoring and auditing of the data sharing process. For example, you can enforce log and trace data requirements on all domains. Your auditors can observe the usage and frequency of data access.

Emerging web applications in various types of business digital asset request to consider the following principles to adopt the data mesh paradigm.

– **Distributed domain-driven architecture**: The data mesh approach proposes that data management responsibility is organized around business functions or domains. Domain teams are responsible for collecting, transforming, and providing data related to or created by their business functions. Instead of domain data flowing from data sources into a central data platform, a specific team hosts and serves its datasets in an easily consumable way. For example, a retailer could have a clothing domain with data about their clothing products and a website behaviour domain that contains site visitor behaviour analytics.

– **Data as a product**: For a data mesh implementation to be successful, every domain team needs to apply product thinking to the datasets they provide. They must consider their data

asset as their products and the rest of the organization's business and data teams as their customers. For the best user experience, the domain data products should have the following basic qualities.

– **Discoverable**: Each data product registers itself with a centralized data catalogue for easy discoverability.
– **Addressable**: Every data product should have a unique address that helps data consumers access it programmatically. The address typically follows centrally decided naming standards within the organization.
– **Trustworthy**: Data products define acceptable service-level objectives around how closely the data reflects the reality of the events it documents. For example, the orders domain could publish data after verifying a customer's address and phone number.
– **Self-describing**: All data products have well-described syntax and semantics that follow standard naming conventions determined by the organization.
– **Self-serve data infrastructure**: A distributed data architecture requires every domain to set up its own data pipeline to clean, filter, and load its own data products. A data mesh introduces the concept of a self-serve data platform to avoid duplication of efforts. Data engineers set up technologies so that all business units can process and store their data products. Self-serve infrastructure thus allows a division of responsibility. Data engineering teams manage the technology while business teams manage the data.
– **Federated data governance**: Data mesh architectures implement security as a shared responsibility within the organization. Leadership determines global standards and policies that you can apply across domains. At the same time, the decentralized data architecture allows a large degree of autonomy on standards and policy implementation within the domain.

I.3 Data catalogue processing in data modelling of digital assets

Data catalogue will be an important element of data management to find the data asset they need across an organization's entire source, which can be disparate and difficult to navigate. Implementing a successful data catalogue can make a big difference in the speed and quality of data analysis by allowing you to quickly find the data you need. And similarly, in emerging web environment, data catalogue will provide users with all sources in the right format, in the right view, and at the right time with the right level of control. The data catalogue will support to make it possible to find and immediately use all information from various sources in a multi-cloud context in terms of building and deploying models in a real-time context.

I.4 Data modelling considerations of digital assets

Multiple operations of data mesh are expected for data modelling of digital assets, and an its ownership mechanism is applied to digital assets. In emerging web environments, the following considerations are necessary to create digital assets using data mesh and other data processing efficiently in terms of data modelling principles.

Setting data domain boundaries

Everybody uses their own definition of domain, sub-domain, or bounded context. Without clear guidance of data domains become too inter-connected, its ownership of data product becomes subject of interpretation, and its complexity will be pushed into domains by other domains.

Concrete classification of digital assets and interoperability standards

It is necessary to define what digital assets are. This requires you to clearly define your different distribution types (e.g., batch-, API-, and event-oriented), metadata standards and so on.

Maximization of wide consumption of digital assets

It is highly likely that the same digital assets will be used repeatedly by different domain teams and a wide range of use cases. As a result, you shouldn't conform their digital assets to specific needs. The primary design principle should be to maximize domain productivity and promote consumption. On the other hand, digital assets will have the capabilities to evolve based on user feedback and generate relevant work for them, so it can be tempting for teams to incorporate consuming specific requirements.

Setting specific guidance for data modelling on missing values, defaults, and data types

It should be heated debates on how missing and defaulted data of digital assets must be interpreted. For example, data is truly missing and cannot be derived, but the operation still expects a mandatory data value to be provided by an employee. If no guidance on how to handle the data modelling of digital assets is provided, a sprawl of descriptions and guidance will be created. Some might consistently provide incorrect values, others might provide random values, while others might provide no guidance at all. Therefore, it is necessary to introduce guidance on data that must be defaulted and formatted consistently throughout the entire data set of digital assets.

Data modelling of digital assets is required to support semantically consistent across all delivery methods (e.g., batch, event-driven, and API-based)

It is obvious to make separate guidance for batch-event and API-oriented data. Since the origin of data is the same for all distribution patterns, it is encouraged for you to make all guidance consistent for all patterns. It is required for all your domains to use a single data catalogue for describing all terms and definitions. This single source becomes the baseline for linkage (mapping) to all different digital assets.

Atomization of digital assets attributes

Digital assets attributes are atomic, and it must represent the lowest level of granularity and have precise meaning or precise semantics. These data attributes in an ideal state of digital assets are linked one-to-one to the items within your data catalogue.

Stable and decoupled from the operational/transactional applications of digital assets

Data of digital assets is required to remain stable and decoupled from the operational/transactional application. This implies schema drift detection, so no disruptive changes. It also implies versioning and, in some cases, independent pipelines to run in parallel, giving the data consumers time to migrate from one version to another.

Direct capture of digital assets from the source

Domains should not be allowed to encapsulate data of digital assets from other domains with different digital assets owners, because that would obfuscate digital assets ownership. Therefore, the data modelling of digital assets must be directly performed in the domain (source) of origin.

Consistent creation concept of new digital assets

It is requested to enforce the same data distribution principles. This means newly created data of digital assets that is to be shared must follow the same principles as outlined in this blogpost. Another concern is traceability, for instance, knowing what happens with the data. To mitigate the risks of transparency, ask data consumers to catalogue their acquisitions and the sequences of actions and transformations they apply to the data. This lineage metadata should be published centrally.

Encapsulation of metadata to support data security

For data security, it is necessary to define a data filtering approach: reserved column names, encapsulated metadata, product metadata, etc. If such a reserved column name is present in any of these datasets, it can be used for fine-grained filtering. Consequently, access can be permitted on only

non-sensitive data or the data can be filtered. A virtual view of digital assets, for example, can be created for a consumer. The same holds for classifications or tags.

Introduction of some enterprise consistency

Introducing some enterprise consistency might help in a large-scale organization in which many domains rely on the same reference values. Thus, it is necessary to consider introducing guidance for including enterprise reference values. For example, currency codes, country codes, product codes, client segmentation codes, and so on. If applicable, you can ask your data product owners to map their local reference values to values from the enterprise lists. The similar approach is to support master identification numbers, which link mastered data and data from the local systems together.

Digital assets versioning for time-variant and non-volatile concerns

In digital assets versioning for the time variant and non-volatile concerns, it will be considered to prescribe how digital assets must be delivered and are consumed downstream. For example, digital assets after they arrive are versioned, compared, forked into read-optimized file formats, and transformed into slowly changing dimensions preserving all historical data from previous data products. In all cases data remains domain-oriented, so no cross-cutting integration is allowed to be applied before any consumption takes.

Use of digital assets blueprints

What is the strategy for creating digital assets? Should it be facilitated with a platform, or must domains cater for their own needs? The creation of digital assets is performed through an interactive process, which can be best facilitated based on digital asset blueprint in emerging web environments. Its balanced approach is requested to be achieved by designing and providing blueprints with the most essential capability of data modelling required for integrating and serving digital assets out to different domains, while giving autonomy for the optimization of data modelling of digital assets. The blueprint can be instantiated for every domain or a set of domains sharing some cohesion.

Clarification of patterns for overlapping domains

For digital assets shared across domains, it is necessary to perform the granularity and logically segmenting data domains of digital assets. Decomposing domains is especially important when domains are larger, or when domains require generic-integration logic. In such situations it could help to have a generic domain that provides integration logic in a way that allows other subdomains to standardize and benefit from it. A ground rule is to keep the shared model between subdomains small and always aligned with the ubiquitous language. Figure I.2 shows those patterns of examples.

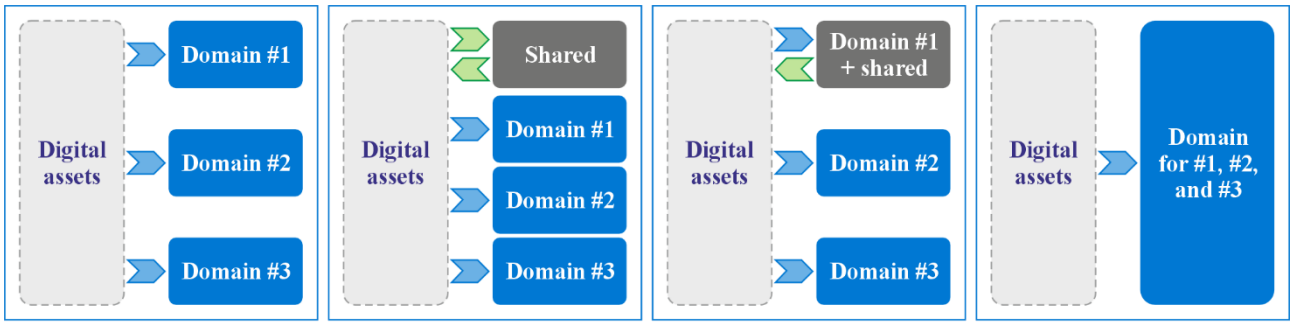

Figure I.2 – Clarification of patterns of digital assets (example)

1) **Separate way pattern**: as a design pattern, it can be used if the associated cost of duplication is preferred over reusability. This pattern is typically a choice when reusability is sacrificed for higher flexibility and agility.

2) **Partnership model pattern**: the integration logic is coordinated in an ad hoc manner within a newly created domain. All teams cooperate with and regard each other's needs. A big commitment is needed from everybody because none cannot change the shared logic freely.

3) **Customer-supplier pattern**: can be used if one domain is strong and willing to take ownership of the data and needs of downstream consumers. The drawbacks of this pattern can be conflicting concerns, forcing downstream teams to negotiate deliverables and schedule priorities.

4) **Conformist pattern**: can be used to conform all domains to all requirements. This pattern can be a choice a) when the integration work is extremely complex b) no other parties are allowed to have control c) or when vendor packages are used.

Appendix II

State of arts of emerging web activities

NOTE – Thi appendix was written with the assistance of artificial intelligence.

II.1 Standard activities combining identity management and blockchain

The integration of identity management and blockchain technology has led to a variety of innovative applications. In Table II.1, some technical items that combine these two technologies are detailed.

Table II.1 – Technical items combining the identity management and blockchain technology

Item	Process	Example
Decentralized identity verification	Users create digital identities on blockchain platforms, which are verified by trusted parties using cryptographic techniques.	A user shares a blockchain-based identity with a bank to open an account.
Self-sovereign identity (SSI)	Individuals control their own identity and issue verifiable credentials on a blockchain.	A university issues a digital diploma on a blockchain, which graduates share with employers.
Supply chain transparency	Blockchain tracks product movement and verifies participant identities.	A food manufacturer tracks ingredient origins and certification authenticity.
Credential issuance and verification	Organizations issue digital credentials (licences, diplomas, etc.) on a blockchain, which are verified using cryptographic techniques.	A government agency issues a blockchain-based driver's licence, verified by authorities.
Access control	Blockchain manages access to resources by verifying identities.	A company controls network access using blockchain-based authentication.
Voting and elections	Blockchain secures elections and verifies voter identities to prevent fraud.	A government conducts elections using blockchain-based digital identities.

IETF activities combining identity management and blockchain

– **CBOR (concise binary object representation):** IETF has developed CBOR, a binary serialization format that is widely used in blockchain applications. CBOR provides a compact and efficient way to represent data structures, making it suitable for use in identity management systems.

– **HTTP signatures:** IETF has defined HTTP Signatures, a mechanism for signing HTTP messages. This can be used to verify the authenticity and integrity of identity-related messages, such as those used for authentication or authorization.

– **OAuth 2.0:** While not specifically related to blockchain, OAuth 2.0 is a widely used authorization framework that can be combined with blockchain-based identity systems. OAuth 2.0 provides a way for users to grant third-party applications access to their data without revealing their credentials.

W3C activities combining identity management and blockchain

– **Verifiable credentials (VCs):** W3C has developed a specification for VCs, which are digital credentials that can be issued, transferred, and verified using blockchain technology. VCs can be used to represent various types of credentials, such as driver's licences, passports, or academic degrees.

– **Decentralized identifiers (DIDs):** W3C has defined DIDs, which are unique identifiers that can be used to represent individuals or organizations. DIDs are independent of any central authority and can be resolved using a decentralized network.
– **ActivityPub:** While not directly related to identity management, ActivityPub is a W3C standard for social networking that can be used in conjunction with blockchain-based identity systems. ActivityPub provides a way for users to control their own data and interact with decentralized social networks.

II.2 Standard activities combining DRM and blockchain

The integration of digital rights management (DRM) and blockchain technology offers innovative solutions for content protection, licensing, and royalty distribution. In Table II.2, some technical items that combine these two technologies are detailed.

Table II.2 – Technical items combining DRM and blockchain technology

Item	Process	Example
Content ownership and provenance	Blockchain records content ownership and provenance to prevent unauthorized distribution.	A musician records a song's creation date and copyright on blockchain to prove ownership.
Licensing and royalty payments	Smart contracts automate licensing and royalty payments, reducing intermediaries.	A content creator licenses their work to a streaming service using blockchain.
Anti-piracy and counterfeit detection	Blockchain tracks digital content distribution to detect unauthorized copies.	A movie studio tracks film distribution to identify piracy.
Content authenticity and verification	Blockchain verifies the authenticity of digital content to prevent fake content.	A news organization ensures the authenticity of articles to prevent fake news.
Supply chain transparency	Blockchain tracks digital content movement to ensure legal distribution.	A video game publisher monitors game distribution to prevent non-appropriate sales.
Decentralized content distribution	Blockchain enables decentralized distribution networks, reducing reliance on platforms.	A content creator distributes work directly to consumers, bypassing intermediaries.

IETF activities combining DRM and blockchain

– **HTTP signatures**: IETF's HTTP Signatures can be used to verify the authenticity and integrity of digital content, providing a layer of protection against tampering and unauthorized distribution.
– **Content security policy (CSP)**: CSP can be used to restrict the resources that a web page can load, helping to prevent unauthorized access to copyrighted content.
– **Digital signatures**: IETF's Digital Signatures can be used to verify the authenticity of digital content and its origin. This can be particularly useful in combination with blockchain-based DRM systems.

W3C activities combining DRM and blockchain

– **Web cryptography API**: This application programming interface (API) provides a standard way for web applications to perform cryptographic operations, such as encryption and decryption. This can be used to protect digital content and enforce DRM policies.

– **WebAssembly**: WebAssembly is a low-level language that can be used to run high-performance applications in web browsers. This can be useful for implementing complex DRM algorithms or cryptographic operations.
– **Web components**: Web components can be used to create reusable UI components for digital content delivery and consumption. This can help enforce DRM policies by restricting access to certain content based on user permissions.

II.3 Standard activities combining digital asset management and blockchain

The integration of digital asset management (DAM) and blockchain technology offers innovative solutions for secure, transparent, and efficient management of digital assets. In Table II.3, some technical items that combine these two technologies are detailed.

Table II.3 – Technical items combining digital asset management and blockchain technology

Item	Process	Example
Asset ownership and provenance	Blockchain records asset ownership and provenance for transparency and security.	A digital art gallery tracks ownership history to ensure authenticity.
Rights management and licensing	Smart contracts automate licensing agreements and royalty payments.	A photographer licenses images on blockchain, with smart contracts enforcing usage rights.
Asset tracking and traceability	Blockchain ensures a transparent and tamper-proof record of asset movement.	A luxury goods manufacturer tracks product journeys to prevent counterfeiting.
Asset tokenization	Digital assets can be tokenized for fractional ownership and trading.	A REIT tokenizes a property, allowing investors to buy fractional shares.
Anti-counterfeiting and authentication	Blockchain verifies digital asset authenticity, preventing fraud.	A luxury watch manufacturer authenticates each watch on blockchain.
decentralized data storage	Blockchain-based storage provides secure, decentralized alternatives to cloud storage.	A media company stores digital assets on a decentralized network for security.

IETF activities combining digital asset management and blockchain

– **HTTP signatures**: IETF's HTTP signatures can be used to verify the authenticity and integrity of digital assets, providing a layer of protection against tampering and unauthorized distribution.
– **Content security policy (CSP)**: CSP can be used to restrict the resources that a web page can load, helping to prevent unauthorized access to digital assets.
– **Digital signatures**: IETF's digital signatures can be used to verify the authenticity of digital assets and their origin. This can be particularly useful in combination with blockchain-based DAM systems.

W3C activities combining digital asset management and blockchain

– **Web cryptography API**: This API provides a standard way for web applications to perform cryptographic operations, such as encryption and decryption. This can be used to protect digital assets and enforce access controls.

– **WebAssembly**: WebAssembly is a low-level language that can be used to run high-performance applications in web browsers. This can be useful for implementing complex DAM algorithms or cryptographic operations.
– **Web components**: Web components can be used to create reusable UI components for digital asset management, providing a consistent and efficient user experience.

II.4 Open-source projects combining identity management and blockchain

The intersection of identity management and blockchain technology (see Table II.4) offers promising solutions for secure, decentralized, and privacy-preserving identity verification. Several open-source projects are exploring this synergy:

Table II.4 – Technical items combining identity management and blockchain technology

Project	Focus	Identity management	Blockchain integration
Sovrin	Decentralized self-sovereign identity framework	Individuals control identity data, issue verifiable credentials, and share with trusted parties.	Built on Hyperledger Indy for secure, immutable identity verification.
SelfKey	Decentralized identity marketplace and wallet	Users create, manage, and share digital identities with verifiable credentials.	Built on Ethereum for secure transactions and decentralized governance.
uPort	Decentralized mobile identity wallet	Users store and manage identity data on mobile devices and issue verifiable credentials.	Built on Ethereum for a secure and decentralized identity infrastructure.
Civic	Decentralized identity verification platform	Users create, manage, and verify identities with verifiable credentials.	Built on Ethereum for secure, decentralized identity verification.
Identifi	Decentralized identity management platform	Individuals control identity data, issue verifiable credentials, and share for authentication.	Built on Ethereum for secure and decentralized identity management.

Key benefits of blockchain-based identity management

In Table II.5, the key benefits of blockchain-based identity management are described.

Table II.5 – Key benefits of blockchain-based identity management

Benefit	Description
Enhanced security	Blockchain ensures a tamper-proof, transparent record of identity data, preventing unauthorized access or modification.
Increased privacy	Users control their own identity data, reducing risks of data breaches and misuse.
Improved efficiency	Streamlines identity verification by reducing intermediaries, lowering costs, and increasing speed.
Greater interoperability	Enables seamless identity management across multiple platforms and organizations.

II.5 Open-source projects combining DRM and blockchain

The intersection of digital rights management (DRM) and blockchain technology (see Table II.6) offers promising solutions for content protection, licensing, and royalty distribution. Several open-source projects are exploring this synergy:

Table II.6 – Open-source projects combining DRM and blockchain

Project	Focus	DRM integration	Blockchain integration
LBRY	Decentralized content distribution and monetization platform	Uses decentralized content addressing system (DCA) for content protection.	Leverages the Bitcoin blockchain for secure transactions and content storage.
Synereo	Decentralized social network and content platform	Reputation system and smart contracts enforce licensing terms and prevent unauthorized distribution.	Built on Ethereum for secure transactions and decentralized governance.
RightsChain	Blockchain-based rights management for creative industries	Smart contracts automate royalty payments, enforce licensing, and protect IP rights.	Built on Ethereum, providing transparency, immutability, and security.
ContentGuard	Blockchain-based content protection and monetization platform	Offers DRM features like watermarking, encryption, and access control.	Uses blockchain to track content ownership, manage licensing, and facilitate transactions.
Copyrighted	Decentralized copyright management platform	Uses blockchain to create a public ledger of copyright claims to prevent infringement.	Built on Ethereum for transparency, immutability, and security.

Key benefits of combining DRM and blockchain

In Table II.7, the key benefits of combining DRM and blockchain are described.

Table II.7 – Key benefits of combining DRM and blockchain

Benefit	Description
Enhanced Security	Blockchain ensures a tamper-proof, transparent record of ownership and transactions, preventing unauthorized distribution of copyrighted material.
Improved Efficiency	Smart contracts automate content management processes, reducing intermediaries and streamlining workflows.
Fairer Compensation	Blockchain enables more transparent and efficient royalty distribution, ensuring fair compensation for creators.
Increased Transparency	Blockchain provides transparency into the content supply chain, allowing consumers to verify content authenticity and provenance.

II.6 Open-source projects combining digital asset management and blockchain

The intersection of digital asset management (DAM) and blockchain technology (see Table II.8) offers promising solutions for secure, transparent, and efficient management of digital assets. Several open-source projects are exploring this synergy:

Table II.8 – Open-source projects combining digital asset management and blockchain

Project	Focus	Digital asset management	Blockchain integration
Filecoin	Decentralized storage network	Decentralized platform for storing and managing digital assets, including images, videos, and documents.	Built on IPFS, uses the Filecoin blockchain for incentivizing storage providers and ensuring data integrity.
Storj	Decentralized cloud storage	Scalable and secure solution for storing and managing digital assets with distributed network for data redundancy.	Uses blockchain for facilitating payments between storage providers and users, ensuring transparency and trust.
IPFS	Decentralized content distribution and storage	Decentralized platform for storing and sharing digital assets, with content-addressing to ensure integrity.	Can integrate with various blockchain platforms to enable secure transactions and decentralized governance.
Daml	Domain-specific language for smart contracts	Creates smart contracts to manage digital assets, including intellectual property, financial instruments, and supply chain assets.	Deployable on various blockchain platforms, including Corda, Hyperledger Fabric, and R3 Corda.
Vault	Decentralized data storage and management platform	Secure, scalable solution for storing and managing digital assets with encryption and access controls.	Integrates with various blockchain platforms to enable secure transactions and decentralized governance.

Key benefits of combining DAM and blockchain

In Table II.9, the key benefits of combining DAM and blockchain are described.

Table II.9 – Key benefits of combining DAM and blockchain

Benefit	Description
Enhanced security	Blockchain ensures a tamper-proof and transparent record of asset ownership and transactions, preventing unauthorized access or modification.
Improved efficiency	Smart contracts automate digital asset management processes, reducing intermediaries and streamlining workflows.
Increased transparency	Blockchain provides greater transparency into digital asset supply chains, making it easier to track and verify ownership.
Reduced costs	Decentralized storage solutions lower the costs compared to traditional data centres and cloud storage providers.

II.7 Open-source digital wallet projects

Open-source digital wallets (see Table II.10) offer transparency, customization, and community-driven development. Here are some notable projects:

Table II.10 – Open-source digital wallets projects

Wallet	Focus	Features	Pros	Cons
MyEtherWallet (MEW)	Ethereum wallet	Supports ERC-20 tokens, custom token generation, hardware wallet integration	Highly customizable, extensive community support	Can be complex for beginners
Electrum	Bitcoin wallet	Lightweight client, HD wallet generation, supports various Bitcoin protocols	Fast and efficient, suitable for both beginners and advanced users	Limited features compared to other wallets
Exodus	Multi-currency wallet	Supports Bitcoin, Ethereum, ERC-20 tokens, user-friendly interface, exchange integration	Easy to use, visually appealing	Some features locked behind a premium subscription
Coinomi	Multi-currency wallet	Supports a variety of cryptocurrencies, shapeShift integration, Trezor hardware wallet support	Highly secure, customizable interface	Can be complex for beginners
Jaxx Liberty	Multi-currency wallet	Supports a wide range of cryptocurrencies, exchange integration, user-friendly interface	Easy to use, cross-platform compatibility	Some features limited compared to other wallets
Atomic Wallet	Multi-currency wallet	Supports many cryptocurrencies, staking, exchange integration, DApp browser	User-friendly interface, extensive features	Can be resource-intensive
Ledger Live	Hardware wallet companion	Connects to Ledger hardware wallets, user-friendly for managing cryptocurrencies and DApps	Highly secure, integrates seamlessly with Ledger hardware wallets	Primarily for Ledger hardware wallet users
Trezor Suite	Hardware wallet companion	Connects to Trezor hardware wallets, user-friendly for managing cryptocurrencies and DApps	Highly secure, integrates seamlessly with Trezor hardware wallets	Primarily for Trezor hardware wallet users

Appendix III

Use cases for digital asset transaction

III.1 Use case scenario

This clause provides use cases for digital asset trading, describing the following items:

– General description: The background of each use case, including classification of digital assets.

– Actors: Individuals or entities that play a role in each use case.

– Use case flow: A detailed flow of each use case.

Emerging web service providers mediate the storage and transaction management of digital assets and receive fees. They can perform additional functions such as access control, authentication, and auditing of digital assets to ensure safe and reliable digital asset transactions.

III.1.1 Description

The types of digital assets, which are data with proven ownership and value, can be classified into various categories. They can be classified according to the economic entity that owns the data and the sensitivity of the data as follows:

– **[Economic entity]** There are four major economic entities: households/individuals, firms, governments, and central banks. Some economists group governments and central banks together.

– **[Sensitivity]** High, low.

Table III.1 – Classification of use cases for digital asset trading

	Household	Business	Government
High sensitivity	Personal information, medical records, financial data, etc.	Software, transaction history, client information, etc.	Defence data, national security data, etc.
Low sensitivity	Photos, creative works (content), social media posts, etc.	Patents, IP, logos, creative works, contracts, etc.	Open data, creative works (content), etc.

III.2 Use case of (individuals – high sensitivity)

This use case illustrates a medical data trading scenario in which a user attempts to utilize a new service that requires access to their personal data. This emerging web service provider allows individuals, not hospitals, to store, submit, and trade their medical data. By maximizing the utility of medical data, the platform creates value for individuals who own the data, hospitals and doctors who generate the data, and companies that desire the data.

– **[Data provider]** Individual. An entity that manages their own medical records and sells or shares them when necessary.

– **[Data consumer]** Research institutions, pharmaceutical companies, insurance companies, etc. Entities that purchase or access individual medical data for clinical research or drug development purposes.

III.2.1 Use case flow

Figure III.1 illustrates the use cases for trading of medical digital assets with high sensitivity for individuals.

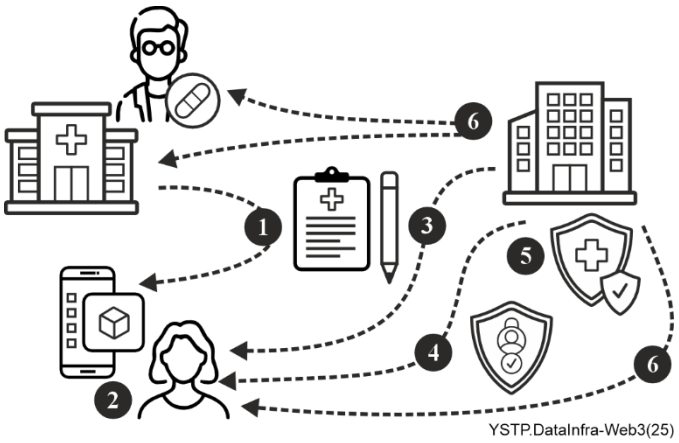

Figure III.1 – Use cases for trading of medical digital assets with high sensitivity for individuals

1) Data storage: Individuals transfer their medical data, signed by hospitals, to their personal cloud.
2) Data control: Individuals can easily manage their medical data through a mobile app and submit or trade it as needed.
3) Purchase request: Data buyers search for the required medical data. The request is sent to the data owner for approval.
4) Data transfer: Once the data owner approves the purchase request, the data is transferred from the personal cloud to the data requester. The individual's signature is included to ensure the source and integrity of the data, and the transfer is conducted through an encrypted channel for security.
5) Data verification: The data requester verifies the authenticity of the data using the public key.
6) Payment: After the data transaction, payment related to the data sales is automatically distributed to the individual, hospital, and doctor in real time through a smart contract.

III.3 Use case of (individuals – low sensitivity)

Use cases include IP marketplaces that facilitate digital content transactions, focusing on connecting creators, IP owners, and consumers. emerging web service platforms connect IP owners and creators, such as NFT holders, authors, and digital artists, with secondary creators and consumers, generating revenue through these connections.

– **[NFT holder]** An individual or organization that owns digital assets and can trade or grant usage rights through the IP marketplace.
– **[Secondary creator]** An entity that creates new content by modifying or combining registered IP and can trade it in the marketplace.
– **[End consumer]** An entity that purchases and consumes various content offered in the IP marketplace.

III.3.1 Use case flow

Figure III.2 illustrates the use cases for digital assets trading with low sensitivity for individuals.

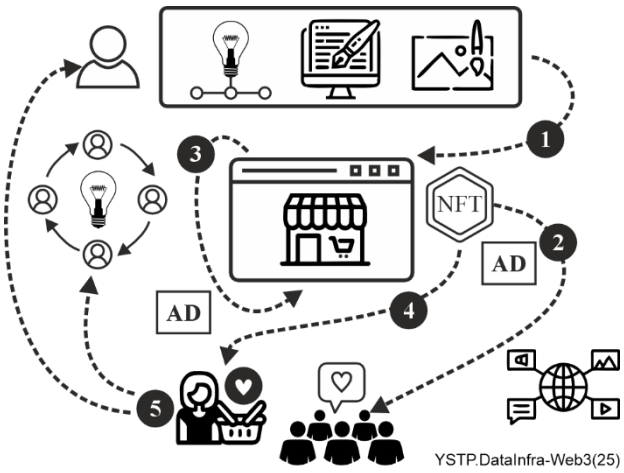

Figure III.2 – Use cases for digital assets trading with low sensitivity for individuals

1) IP registration: Creators and IP holders register their works on the platform. Ownership and usage rights of the content are clearly defined during this process.

2) Content distribution: The registered IP is distributed through various channels. Payment methods and revenue sharing are closely linked to each distribution channel.

3) Content utilization: Secondary creators use the registered IP to create new content, which can take various forms such as game assets, remix music, or comic books. Advertisers may insert advertisements into specific content during this process.

4) Consumer purchase: Consumers purchase and consume the content created by secondary creators. Transactions are executed through smart contracts, and the revenue is distributed among IP holders, secondary creators, and emerging web service providers.

5) Revenue distribution: Upon completion of all transactions, the emerging web service providers automatically distributes revenue according to a predefined sharing ratio, ensuring transparency through blockchain technology.

III.4 Use case of (firms – high sensitivity)

This use case aims to build a emerging web service platform where companies can securely trade business intelligence tools, data analysis algorithms, market prediction models or specific know-how developed internally. The emerging web service platform enables the exchange of highly sensitive knowledge and data between companies, allowing them to securely acquire the necessary information and technologies.

– **[Data providing firm]** A company that provides business intelligence tools, algorithms, or know-how with the intention of generating revenue.

– **[Data consuming firm]** A company that aims to enhance its business processes and strengthen its market competitiveness by utilizing externally provided business intelligence (BI) tools or data.

– **[Security and certification agency]** An entity responsible for verifying the integrity of the data and tools being traded and ensuring the security of the transaction process.

III.4.1 Use case flow

Figure III.3 illustrates the use cases for digital assets trading with high sensitivity for firms.

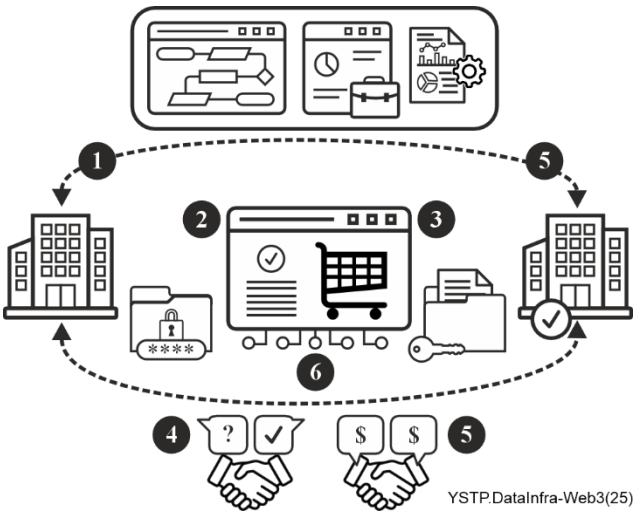

Figure III.3 – Use cases for digital assets trading with high sensitivity for firms

1) Asset registration: The data-providing firm registers its business intelligence tool, algorithm, or know-how on the emerging web service platform, along with details such as the asset description, available licence types, and pricing.
2) Asset verification: The emerging web service provider verifies the integrity and validity of the registered assets. Security and certification authorities are involved in this process to ensure the reliability of digital assets.
3) Purchase request: The company requesting the data searches the emerging web service platform for the required business intelligence (BI) tools or data and submits a purchase request. This request is forwarded to the data provider.
4) Negotiation and contract: Once negotiation takes place between the data provider and the demanding company and the terms of the transaction are confirmed, a smart contract is automatically executed.
5) Asset delivery: Once the contract is executed, the digital asset is securely delivered to the requesting company via the business intelligence tool or a secure channel. Cryptography is used to ensure the ownership and integrity of the digital asset.
6) Payment: Once the asset is received and verified by the demanding firm, payment is automatically processed through a smart contract. The emerging web service provider receives a transaction fee.
7) Post-transaction management: The emerging web service provider monitors the use of the data post-transaction to ensure compliance with the licensing terms. If any violation is detected, the emerging web service provider takes the actions specified in the contract.

III.5 Use case of (firms – low sensitivity)

This use case aims to establish an emerging web service platform where firms can securely trade IP assets (e.g., patents, trademarks, copyrights) with other companies. The emerging web service provider supports transparent evaluation, simplified transaction procedures, and legal protection and compliance, fostering cooperation and innovation among firms.

– **[IP provider company]** A company that seeks to generate revenue by selling or licensing its IP assets, such as patents, trademarks, and copyrights.
– **[IP consumer company] A** company that aims to acquire external IP assets for technology development, product improvement, or market entry.
– **[Legal and regulatory agency]** An entity that oversees compliance with legal regulations in IP transactions and provides legal support if necessary.

– **[IP valuation agency]** An entity that objectively evaluates the value of IP assets before transactions and provides reliable standards.

III.5.1 Use case flow

Figure III.4 illustrates the use cases for digital assets trading with low sensitivity for firms.

Figure III.4 – Use cases for digital assets trading with low sensitivity for firms

1) IP asset registration: The IP-providing firm registers its patents, trademarks, copyrights, etc., on the emerging web service platform, specifying the asset description, available licence types, and pricing.
2) IP evaluation: The emerging web service provider collaborates with professional evaluation agencies or AI to assess the value of the registered IP assets. This process reviews the legal protection status and market value of the IP assets.
3) Purchase request: The IP-demanding firm searches the emerging web service platform for the required IP assets and submits a purchase request. This request is conveyed to the IP-providing firm.
4) Negotiation and contract: Negotiations occur between the IP-providing and demanding firms, and once the transaction terms are confirmed, a smart contract automatically generates the agreement.
5) IP asset transfer: After the contract is executed, the ownership or usage rights of the IP assets are transferred to the demanding firm. Relevant documents and licences are provided to ensure legal protection.
6) Payment: Once the asset is received by the IP-demanding firm, payment is automatically processed through a smart contract. The emerging web service provider receives a transaction fee.
7) Post-transaction management: The emerging web service provider monitors the use of the IP assets post-transaction to ensure compliance with the contract terms and provides legal dispute resolution support if necessary.

III.6 Use case of (government – high/low sensitivity)

The government data can be categorized into public data and confidential data based on sensitivity. Public data is open to everyone and includes information like nationwide elementary school addresses and student numbers, and transportation routes.

National institutions managing public data set predefined usage limits based on copyright. They decide if commercial/non-commercial use, modification, and reprocessing are allowed. This data is provided to individuals, companies, or organizations upon request.

Once obtained, users can reprocess the data to generate profit within the allowed scope. The profits are transparently shared according to pre-agreed terms, allowing both the government and re-processors to create economic value.

– [Public institutions (government)] Manage public data and operate the digital asset platform.
– [Data management] Collect and classify data generated as public assets, storing and managing it in a form that can be provided.
– [Digital asset platform management] Operate and manage an emerging web service platform where reprocessed digital assets based on public data can be traded.
– [Data requester] Requests data managed by public institutions that can be reprocessed to create value. They reprocess this data to recreate it into valuable, tradeable digital assets. Particularly, they establish revenue-sharing policies based on their contribution and share profits accordingly.

III.6.1 Use case flow

Figure III.5 illustrates the use cases for digital assets trading with high/low sensitivity for government.

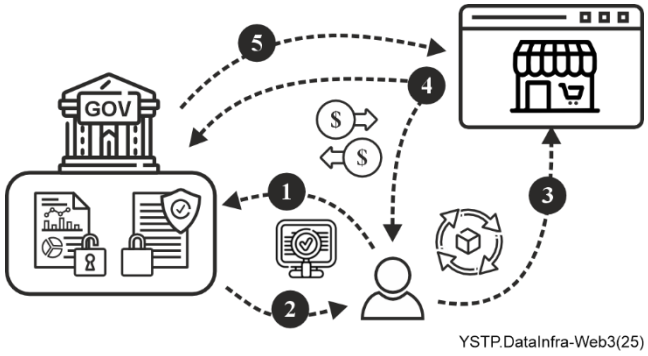

Figure III.5 – Use cases for digital assets trading with high/low sensitivity for government

1) Request: A data consumer requests data from a public institution.
2) Review/provision: The institution reviews the request and decides whether to provide the data based on its type, then proceeds with the provision if approved.
3) Reprocessing/upload: The consumer reprocesses the collected data and uploads it to a emerging web service platform, clearly indicating ownership.
4) Revenue sharing: If the digital asset is traded on the platform and generates revenue, the profits are shared accordingly.
5) Data and platform management: The public institution collects, stores, and manages the public data, including determining its availability and managing it by category.

Appendix IV

Emerging web-based digital asset trading system: royalty flow and digital asset valuation

IV.1 Registering digital assets and setting basic information

Every digital asset is given a unique ID and basic metadata when it is first registered. During this process, a smart contract that states ownership and usage rights is created and recorded on the blockchain to guarantee transparency and trackability. This also clarifies the relationship between the original asset and any related content created later.

– Metadata details: Unique ID of the asset, creator information, creation date, type of asset, available licence range, initial value, etc.

– Ownership and usage details: Owner's identity (ID), proof of ownership (e.g., KYC verification), scope of usage rights (commercial or non-commercial use, permission for resale), etc.

– Smart contract details: Metadata information, ownership and usage conditions, trade eligibility of the asset.

IV.2 Licence conditions setting (IP licence programming)

Each digital asset uses a Licence template called a programmable IP licence (PIP) to set conditions for reuse, commercial use, transfer, etc. PIP clearly defines the scope of use of the asset and issues a licence token including the permitted usage method and whether it can be traded. For example, if you want to reuse a part of a specific content, it automatically determines whether approval is required or whether royalties are charged based on the licence conditions of the asset. After the licence conditions are set, these conditions are automatically enforced through a smart contract, and users can utilize the digital asset according to the predefined conditions.

– Licence smart contract information: whether commercial use is allowed, whether non-commercial use is allowed, whether resale is possible, whether reprocessing and modification are possible, period of use, usage conditions (e.g., restricted use within a specific platform, available only in a specific company), revenue sharing ratio between the asset owner and the creator of the derivative content, royalty ratio, and distribution target.

IV.3 Revenue sharing and value assessment

When a derivative content of a digital asset is created, the derivative content issues a licence token that inherits the licence conditions of the original content, as well as a royalty token for revenue distribution. The revenue stream that occurs based on the relationship between the original asset and the derivative asset is managed through the token. The revenue generated based on the number of times a specific asset is used, or the frequency of transactions is distributed to the owner of the asset. For example, when a new content is created and sold by reusing a specific asset, the smart contract recognizes this and distributes the royalty to the owner. The revenue stream is transparently managed on the blockchain. Royalty token holders have the right to claim a portion of the revenue generated from the derivative asset, which allows the asset owner to generate continuous revenue.

– Royalty smart contract information: royalty payment criteria, payment method, payment cycle, distribution details, token balance.

IV.4 Creation of derivative content and inheritance of rights

Users of digital assets can create new content based on the original asset according to the licence conditions, and in this process, the rights set by the original asset are automatically inherited. Derived content inherits the licence linked to the original asset in the smart contract to manage whether it can

be used commercially, the scope of reuse, etc., and can be set to automatically pay royalties to the original asset owner if necessary.

– Derived content smart contract information: Whether content can be created based on this asset, types of permitted derivative content (e.g., image modification, text expansion, etc.), royalty rate, revenue distribution rate, tracking data for linking with the original asset, blockchain records for rights tracking, and control of specific usage scope.

IV.5 Continuous value assessment and market guidelines

The value of digital assets is continuously evaluated based on data such as the frequency of creation of derivative content, user participation, and transaction frequency, and this is used as the basis for ownership tokens that represent the right to own and transfer digital assets. AI/ML algorithms analyse the activity data of assets to evaluate the current value and future potential of the assets. For example, if the usage of a specific asset increases or the profitability of derivative content increases, the valuation amount of the asset, i.e., the ownership token, may be readjusted. This information can be reflected in the market in real time to provide guidelines so that asset owners (ownership token holders) can trade or hold at the appropriate time.

– Activity data information: past transaction data, usage patterns of derivative content, frequency of asset usage, number of derivative content creations, frequency of transactions, user interactions (e.g., comments, likes, views, etc.)

IV.6 Interoperability and global IP registry management system

All digital assets must be interoperable within the decentralized IP ecosystem and follow standardized protocols to be able to connect with various platforms (see Figure IV.1). There is a need to integrate and manage various information such as asset licensing conditions, royalty flow, and dispute resolution through an IP asset registration registry.

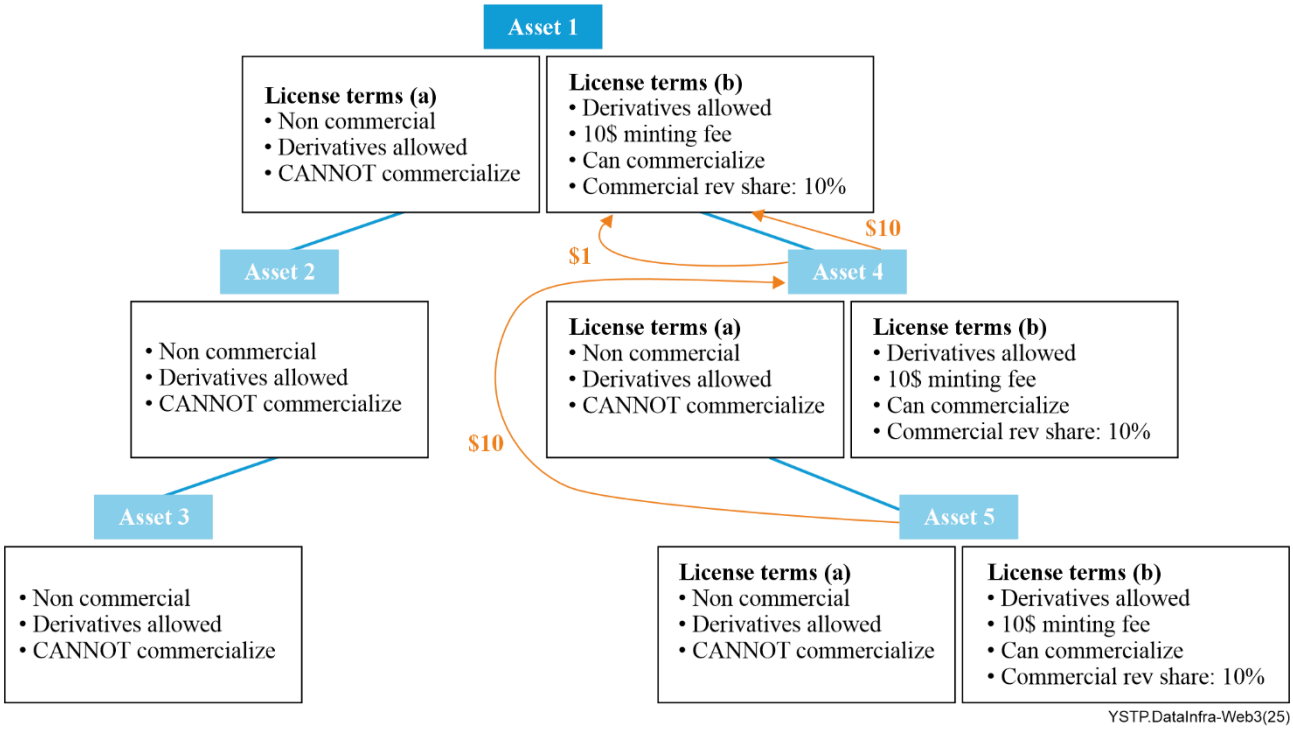

Figure IV.1 – Royalty flow and digital asset valuation

Bibliography

[b-AML] https://en.wikipedia.org/wiki/Anti%E2%80%93money_laundering

[b-CCPA] https://leginfo.legislature.ca.gov/ TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]

[b-CDPR] https://eur-lex.europa.eu/eli/reg/2016/679/oj REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

[b-CSV] https://en.wikipedia.org/wiki/Comma-separated_values

[b-DeFi] https://en.wikipedia.org/wiki/Decentralized_finance

[b-Digital Asset] https://en.wikipedia.org/wiki/Digital_asset

[b-DAO] https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

[b-Data Governance] https://en.wikipedia.org/wiki/Data_governance

[b-DID] https://www.w3.org/TR/did-core/

[b-EAV] https://en.wikipedia.org/wiki/Entity–attribute–value_model

[b-HTML] https://en.wikipedia.org/wiki/HTML

[b-IPFS] https://en.wikipedia.org/wiki/InterPlanetary_File_System

[b-JSON] https://en.wikipedia.org/wiki/JSON

[b-KYC] https://en.wikipedia.org/wiki/Know_your_customer

[b-MIME] https://en.wikipedia.org/wiki/MIME

[b-NFT] https://en.wikipedia.org/wiki/Non-fungible_token

[b-OGC] https://en.wikipedia.org/wiki/Open_Geospatial_Consortium

[b-RDF/XML] https://www.w3.org/TR/rdf-syntax-grammar/

[b-RFC1738] https://www.ietf.org/rfc/rfc1738.txt

[b-RFC3986] https://www.rfc-editor.org/rfc/rfc3986

[b-XML] https://en.wikipedia.org/wiki/XML