Web 3.0 Ecosystem

Jun Kyun Choi (KAIST, Korea)

Professor, Department of Electrical Engineering, KAIST
Director, KAIST-MEGAZONECLOUD Research Center
for Intelligent Cloud Computing Convergence

jkchoi59@kaist.ac.kr

Contents

01

Web 3.0 Overview

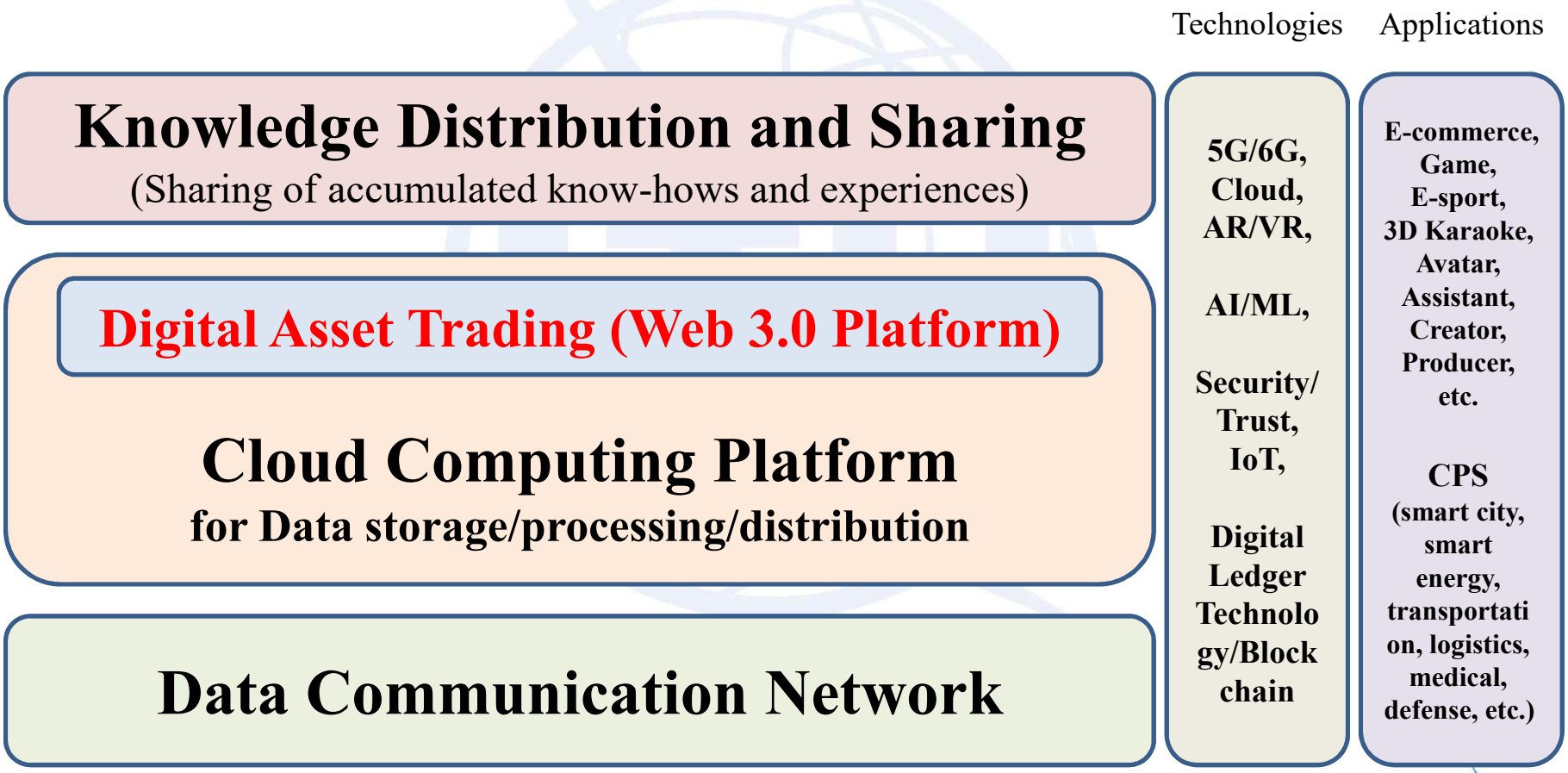
History to Web 3.0

- **History of World Wide Web**
  - Web 1.0 (1980)
    - Access Web page by using HTML/HTTP
    - Search engine for document, file, and email, file transfer
  - Web 2.0 (1990)
    - Chatting and sharing of user created contents (blog, social media, Youtube)
    - Large scale data center, web hosting service, SNS service
    - Global scalability of high speed Internet and cloud computing platform
- **Web 3.0 (2022) as Foundation of New Internet**
  - **New Internet for transaction of Digital Assets**
    - Immutable, distributed, secure, transactional ledger as the foundation of a New Internet
    - **Tokenized smart contract-based commerce**
  - Key Features and Technical Issues
    - Trading from Digital Art to On-line Game
    - Transactional Governance with Democratization and Transparency
    - **DAO (Decentralized Autonomous Organization),** not central clearing mechanism
    - **Data Ownership** and disclosure of transaction records of digital assets

Web 3.0 Applications (Examples)

- **Digital Currency**
  - Similar to multiple bank accounts for digital assets
- **Decentralized Finance (DeFi)**
  - Digital Ledger technology for smart contracts without human intervention
  - Similar markets like currency exchange, loan, investment, gambling, etc.
- **Decentralized Social Media (DeSo)**
  - Monetization of Social Influencer
  - New market for digital assets trading on SNS platform
- **Decentralized Gaming (GameFi)**
  - Monetization of game money, items, experience points, and game assets (NFT)
- **Decentralized Metaverse**
  - Create new virtual assets through AR/VR

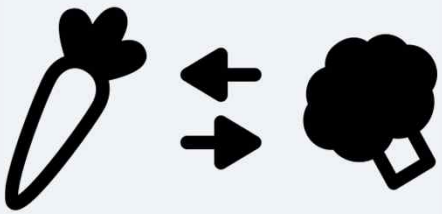
Ecosystem of Future Knowledge Society

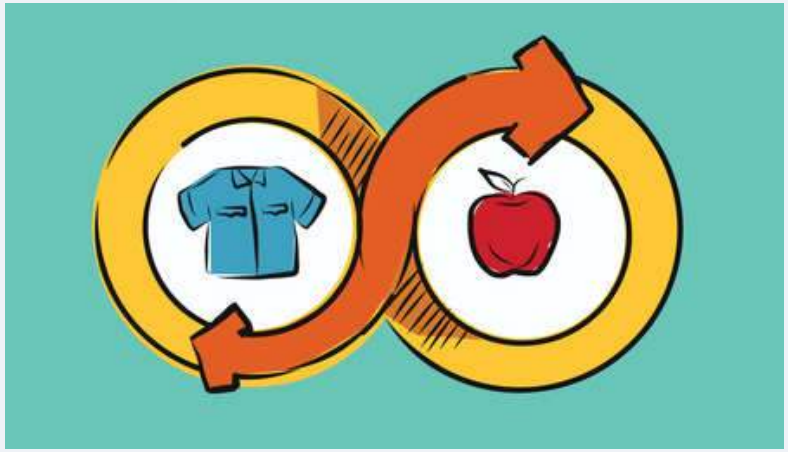


Evolution of Trading

Exchange of Goods

Direct exchange of goods produced





Transaction using Currency

Stone Age : shells, sheepskin

Middle Age : Gold, Silver, Coins

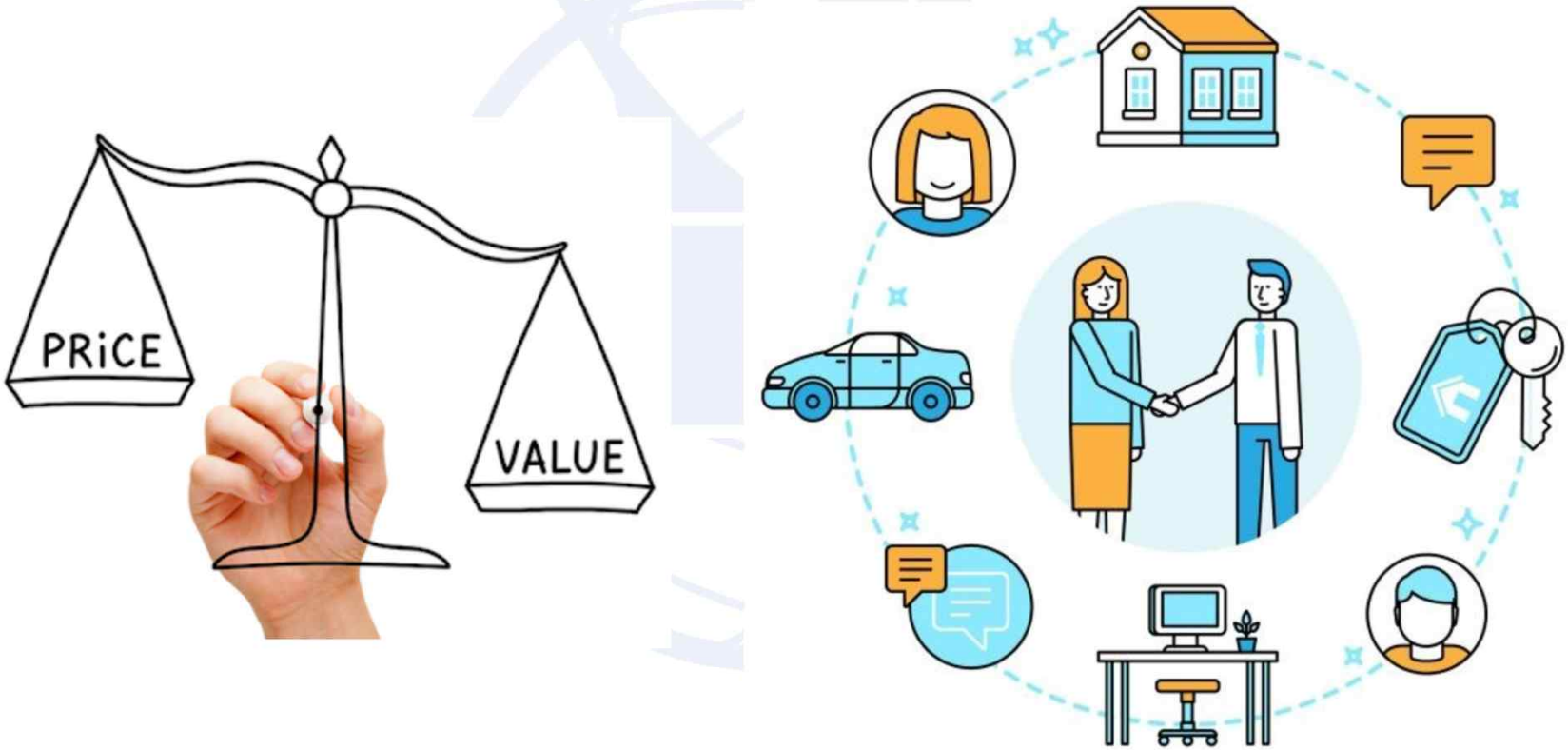
Modern: Paper Money, Stock, Bond

Future: **Digital Currencies, Coupons, and Tokens**

What is the Digital Assets ? (Wikipedia)

- **Definition of Digital Assets**
  - Anything that exists only in digital form with a distinct **usage right** or distinct **permission for use**
    - (note) Data without that right is not considered an asset
  - (Digital appliances for acquisition, storage, transmission and exchange) personal computers, portable players, tablets, smartphone, all apparatuses being able to carry digital assets
- **Types of digital Assets**
  - Software, photos, logos, illustrations, animations, audiovisual media, presentations, spreadsheets, digital drawings, word documents, e-mails, websites and many other digital formats
- **Regulations related to Digital Assets**
  - **Copyright and authority**: Papers, books, patents, etc.
  - **Identification of transaction (or authentication)** : social security number, personal ID, biometric information, etc.
  - **Privacy Protection** : legal problems when exposed arbitrarily
  - Documents with special conditions while disclosure, transfer, and access, etc.
    - Legitimate reward is specified when profits occur
    - Like GDPR, certain areas, people or business areas are prohibited from being disclosed, etc.

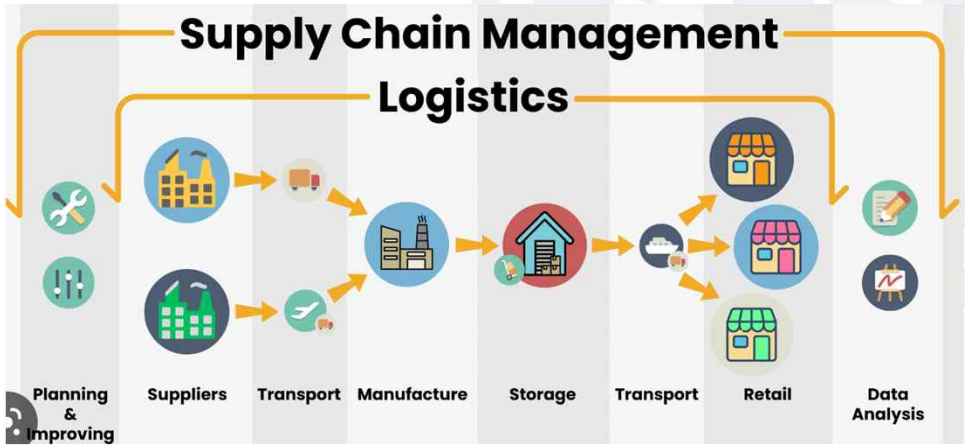
Calculation of the Value of Digital Assets



(note) Traditional supply and demand economics do not apply

Positive Cycle of Digital Asset Productivity

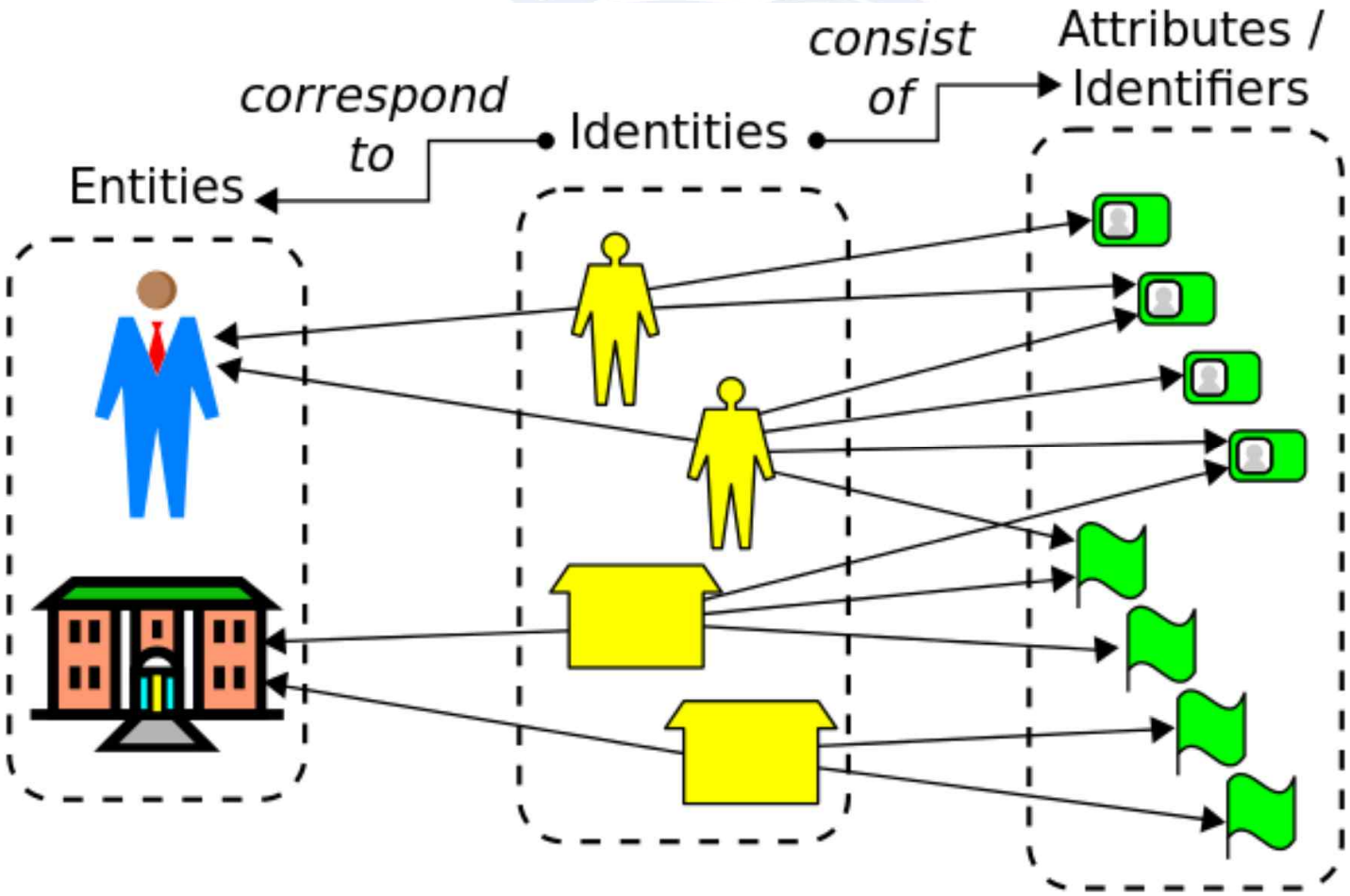
- **New Value Chain of Profits and Margin of digital asset trading**
  - Existing Market : Manpower + Capital + Factory Process Improvement
  - Digital Asset Market: **People + Digital Currency + Platform** Innovation



02

Technical Issues for Web 3.0

Relationship between Entities, Identities and Attributes / Identifiers



(note) https://www.researchgate.net/figure/Relationships-among-Entities-Identities-and-Identifiers_fig1_265188437

Classifications for Digital Asset Trading

Digital Currency
(Token)

- Bitcoin, Ethereum
- Token, etc.

Transaction Records
(Invoice)

- Smart Contract (Blockchain)
- DLT-based Wallets
- Tax, etc.

Digital Assets
(File, Documents)

- Audio/Video/Text Files
- Art, logo, email, Web site
- Product, Software, algorithms, etc.

(Key Questions)

- When creating Digital Asset ? (identification, ownership, privacy, etc.)
- How are Digital Assets being traded ? (copyright, reward, license, etc.)

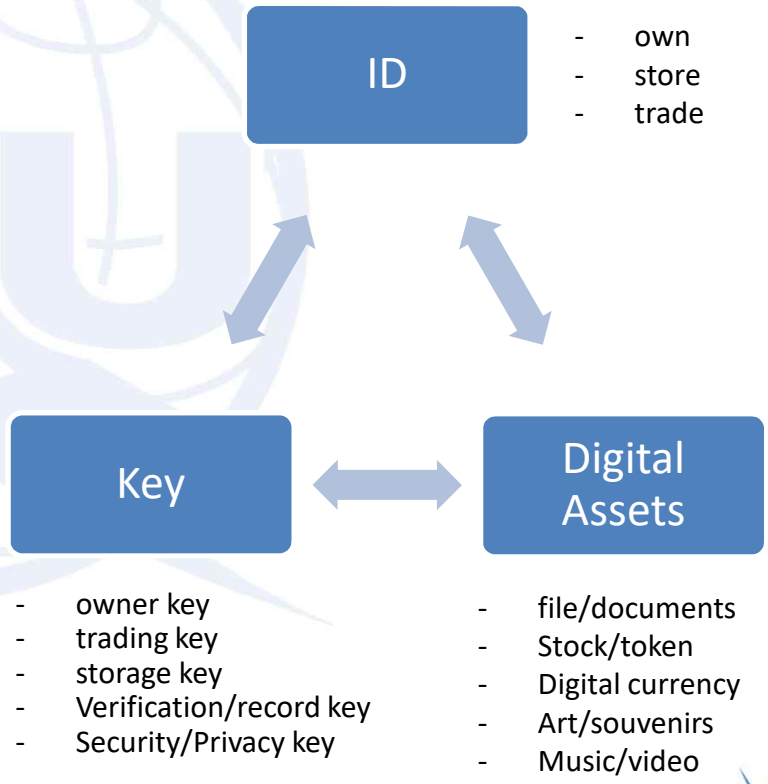
ID Provisioning for Digital Assets

- **Two types of Identification for Digital Assets**
  - **Person/Organizational Identity**
    - e.g., personal identification numbers, social security numbers, and company registration number, etc.
  - **Digital Object Identifiers**
    - e.g., bank accounts, email address, SNS/SMS IDs, token/coupon IDs, and company/community IDs
    - Physical products like building, cars, electric appliances, book, digital files, and audio/video materials, etc.

    (note) existing products are identified by their own identification mechanism such as E.164, SNS/SMS, Email, ISBN/ISSN, and GS1.
- **Verification and Authentication of Digital Identities**
  - (creating new digital assets) digital object identifiers are mapped with person/organizational identities
  - When a person uses **multiple IDs**, Avoiding Sybil Attacks may require KYC (Know Your Customer)
- **ID binding and provisioning for digital asset transactions**
  - Verify their **ownership** while trading digital assets
  - After transacting a digital asset, the digital asset is bound to another person/organizational identity
  - Digital ledger technology including blockchain should be used for **safe and secure transactions**.
  - To protect **privacy**, individuals/organizations should be protected to hide who participates in the digital asset transactions

Relationship among Id, Key, Digital Assets

- **Safe and Secure Binding among ID – Key – Digital Asset**
  - When creating digital assets, **Two Types of IDs** with the corresponding keys should be created and linked.
  - When trading digital assets, the **transaction ID** can be created and recorded
  - **Private/Public Keys** are used for transactions, storage, verification, protection, security, etc.
  - **ID Verification/Certification** process is intended to protect fraud and illegal behaviors



Relationship between ID and Keys for Digital Asset Trading

- **Relationship between personal/organizational identities and digital object identifiers**
  - Digital object identifier is associated with a corresponding person/organizational identity to ensure **ownership**.
  - Each digital asset has a unique digital object identifier
  - One person/organizational identity can have multiple digital assets
- **Private/Public Keys for digital asset trading**
  - Needed to access, control and transfer digital assets
  - **Private keys** are used to access and manage their own digital assets.
  - **Public keys** are used to transfer digital assets to others when transacting.
  - The recipient of the digital asset must use private key to prevent unauthorized access
  - If one key for multiple digital assets is stolen, all digital assets using the same key can be stolen.

Trust level of person/organizational identity or digital object identifier

- **Trust Level of IDs**
  - Both for person/organizational identity and digital object identity
  - Provide DAO-based regulatory guidance and trading policies
  - Determined at creation instance, initially Zero Trust
  - Update after a successful digital asset transaction

- **Verification Procedures of Trust Level**
  - No guarantee of digital asset trading without verification
    - May linked to KYC (Know Your Customer) and iris recognition
  - Trust level can have a higher value if there is a trust measure accumulated elsewhere
    - Highly trustworthy through an appropriate verification process

Public and Private Repository of Digital Asset

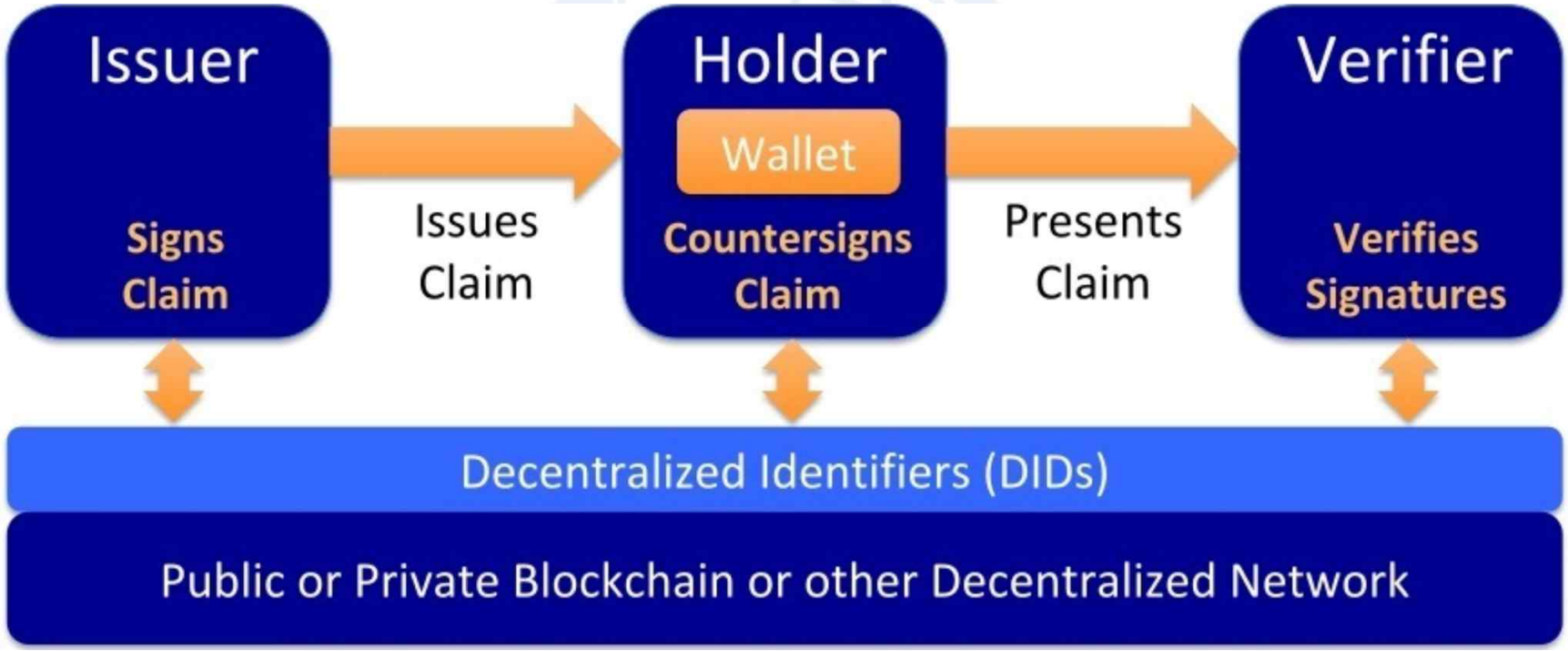
- **Why Public or Private Repositories are needed ?**
  - All digital assets should be registered for trading, just like displaying products in a mart
  - A digital asset sold globally should be identifiable by anyone in the world
  - Registered in that local repositories while trading within a small geographic area
- **Registration Process of public/private repository**
  - Declare person/organizational identity to clarify ownership
  - Check whether the digital asset is fraudulent or illegally copied
- **Private repository operated by the company**
  - Digital assets are traded only on a private platform provided to the company
  - The company is held responsible for any problems arising from digital asset trading
  - Governments only need to monitor whether digital asset transactions are illegal
- **Public repository suitable for the global environment**
  - A national-level public repository is required to exchange digital assets owned by different companies or individuals
  - **The DAO-based same regulations** between countries are required between numerous digital asset platforms domestically or internationally

(note) Recently, Europe enacted the MiCA (Market in Crypto-Assets) Act.

DAO (Decentralized Autonomous Organization) Philosophy

- **DAO (Decentralized Autonomous Organization) philosophy**
  - No particular companies or countries should regulate the trading of digital assets
  - All transactions of digital assets around the world are transparently disclosed.
- **Privacy operated by neutral organization, not company nor government**
  - Privacy protection for the transaction details of all digital assets is required
    - Decentralized Identifier (DID) or Zero Trust technologies have emerged.
    - In the W3C DID standards, **verifiable credential** should go through strict procedures to protect privacy since it may try to tell not only whether a particular DID value is correct, but also what kind of person and what organization the DID is.
- **Confronts the regulations monitoring fraud and illegality**
  - Access to investigate illegal activities should be blocked unless **strict procedures** are followed. Secret access to private/public repository should never be allowed.
  - When an individual or organization attempts to access a private/public repository, if the purpose is not normal process, it should be **blocked or disclosed to the public** for what purpose and which data is being accessed.

Decentralized IDentifiers (DIDs)

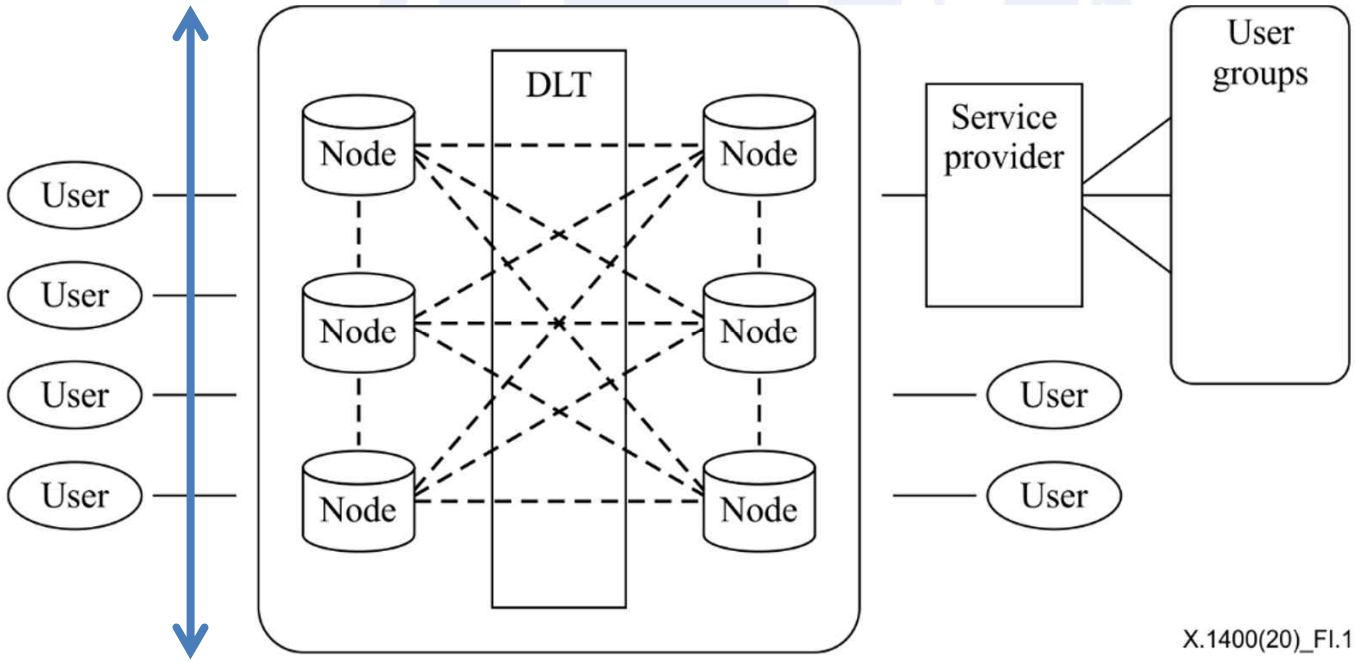


(note) https://en.wikipedia.org/wiki/File:Decentralized-identifiers-dids-the-fundamental-building-block-of-selfsovereign-identity-ssi-37-1024_DIDs-enable-digitally-signed-verifiable-claims.jpg

Demarcation Point for Privacy ?

→ Right-direction by using Hash Algorithm (Ownership, copyright, license, etc.)
← Prohibit to Left-direction for **Privacy Protection**

Demarcation Point



Stake Holders for Digital Asset Trading - 1

- **Digital Asset Producers and Owners**
  - Registration and Declaration of Ownership (**Certificate Authority, Verifiable Registry**)
    - Unregistered digital assets cannot be protected
  - Declaration of digital asset trading conditions and final approval of the transaction
    - The same rules may apply to p2p transaction between individuals
- **Buyer**
  - Keep the Procedures for safe transaction
    - Trading terms and payment methods
    - Private key management for transactions (including loss, replacement, new creation, etc.)
  - Keep Personal information and Privacy Compliance
    - Owner, Seller/Intermediary ID Disclosure and Privacy Policy Compliance
    - Keep DAO-based regulation of digital assets (including PII, confidentiality, parental control, etc.)
- **Agent (Option)**
  - Confirm digital asset ownership of customers who wish to sell
  - Search for digital assets preferred by customers who wish to purchase
  - Re-verification of digital assets (i.e. double check for fraud and forgery)
  - Transaction conditions and errors checking in smart contracts

Stake Holders for Digital Asset Trading - 2

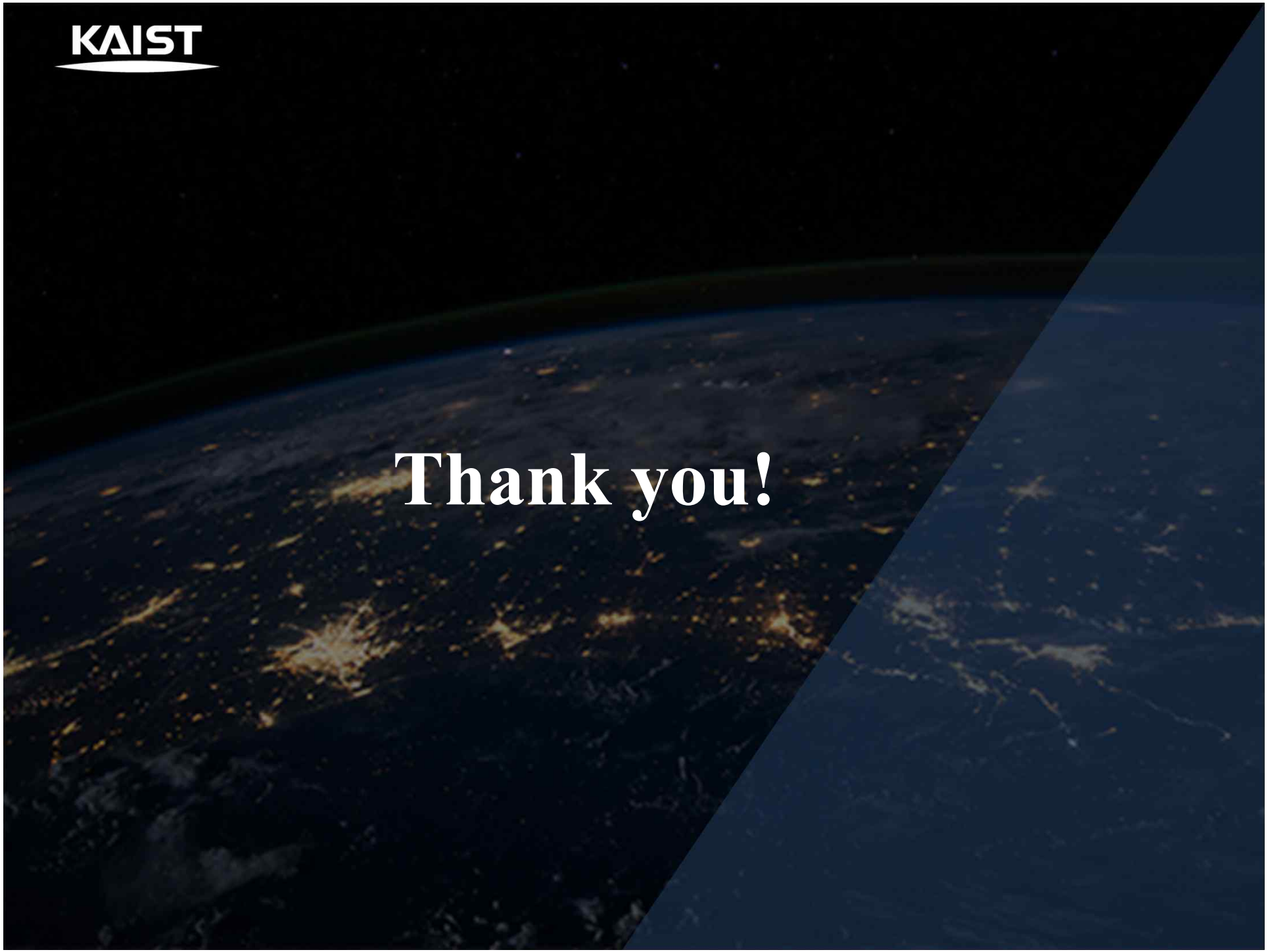
- **Platform Provider of Digital Asset Trading**
  - Provide digital asset trading platform including contract negotiation and settlement
  - Store and deliver digital assets including transaction records
  - Privacy protection and surveillance of illegal transactions (legal regulations)
  - Tax payment, damage and refund policy (legal regulations)
- **Certificate Authority (Verifiable Registry)**
  - Ownership registration of digital assets
  - Checking the correctness of registered digital assets
- **Web 3.0 Technology Developers**
  - Provide digital asset trading and negotiation platform
  - Provide web-based user applications for digital asset trading
  - Provide Smart contract to protect illegal transaction
  - Privacy protection and DAO-based regulatory guidance, etc.
  - Protect fraud, forgery, alteration of ID and digital assets

Technical Issues for Web 3.0 Standardization - 1

- **Identification of Digital Assets**
  - Compatible with existing ID mechanisms (e.g., URL, Email, SNS, E.164, GS1, ISBN, ISSN, etc.)
  - ID Creation and Naming of digital assets
    - Remember old human customs or habits such as people's name, dog nickname, etc.
    - Check KYC (Know Your Customer) based identity verification to prevent Sybil Attack
    - Registration, Operation, Verification mechanism of current W3C's DID (Decentralized Identity) are considered!
      - It notes that millions of new IDs are registered and revoked daily in globally distributed repositories
  - **DAO-based Public Repository** is essential for global ID provisioning of digital assets
    - Similar to the existing product or patent registration process
    - Globally distributed and deployed in conjunction with the DID system
    - Protect privacy and prevent fraud and illegal behaviors
  - **Open to public** for digital assets registered in Public Repository
    - Confidential and secret materials cannot be registered in public repositories
  - Private Repository is not a scope of international standardization ?
    - But, public repositories are essential to provide **interoperability** with other private/public repositories.

Technical Issues for Web 3.0 Standardization - 2

- **Trading and Negotiation Model of Digital Assets**
  - Depending on types of digital assets (e.g., digital file/materials, audio/video, art/music, patents, product, land, car, etc.)
  - Depending on trading model (e.g., license only without transfer of ownership, free or conditional license, usage period and limit, privacy, legal regulation, etc.)
  - Depending on technologies and platform (e.g., E-commerce, Game, Medical/Health, SNS/Music/Video, File/Documents, etc.)
  - Compatibility of existing on-/off-line and sharing economy trading models
  - Future of DLT/Blockchain technologies


KAIST
Thank you!