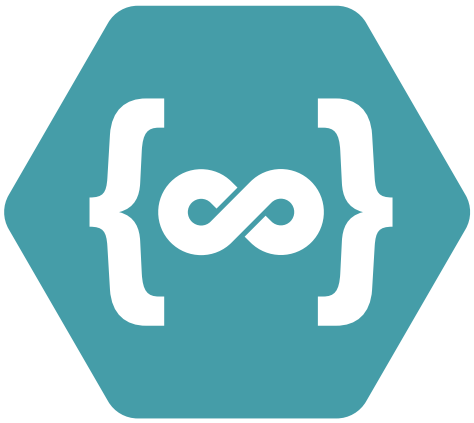
KMX Network

Korea Mainnet X Project



CY2CODE

2023.05

Ver. 1.x

1. Overview

The era of the fourth industrial revolution that combines manufacturing and information and communication (ICT) is coming. After the first industrial revolution (18th century), the second industrial revolution (19th-20th century), the third industrial revolution, which was based on computer and Internet, the fourth industrial revolution (late 20th century), which is now facing innovation in IoT, artificial intelligence, and blockchain-based industrial structure.

Since the advent of PCs in the mid-1980s, the paradigm of ICT has been changing every 10 years, such as the PC era, the Internet era, the mobile era, and the hyper-connected era, and the current technical future interests will be big data, IoT, artificial intelligence, and blockchain.

Based on these future interests, KMX aims to provide a platform that can easily access the future of the 4th Industrial Revolution. It provides blockchain-based KMX ecosystem platform for all users to use the 3rd and 4th industrial revolution technologies.

2. Introduction

Through blockchain technology, the second Internet revolution, we can give trust to information beyond information sharing in the Internet era.

Through this information trust network, the authenticity of information can be checked, the information can be protected, and the transparency of transactions between individuals can be secured through the transaction ledger.

Based on this, blockchain is a "shared ledger technology" that verifies the validity of transactions, distributes and shares transaction details, and authenticates encryption storage of information from the existing central control system to the distributed system.

It is a technology that makes transactions transparent based on smart contracts with tangible and intangible assets held by participants in such blockchain business networks.

When someone mentions blockchain, there will be many people who think of Bitcoin due to the influence of the media and reckless speculators.

However, Bitcoin is only an encryption currency using blockchain technology. In other words, the equation "Bitcoin = blockchain" is established, but the opposite is not established.
Blockchain is, in a word, a "distributed database."

Blockchain network participants decide the right data through agreement and store the same value. A unit of data is called a block, and a block contains several pieces of data. These data are not just stored, but are made into a hash through a hash function. And information including this hash value is stored together in the next block.

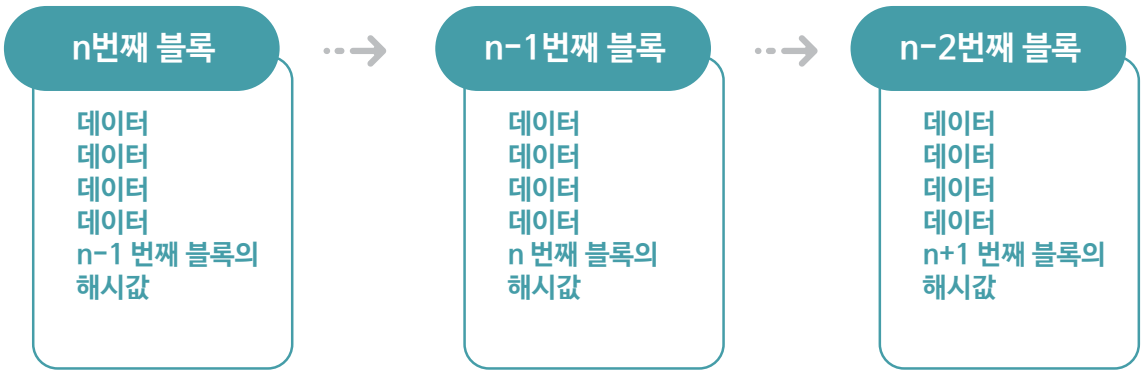


Figure 1 Structure of Blockchain

The most important technologies in blockchain are encryption and P2P.
It is confirmed that the block is not modulated using the hash function, which is a one-way encryption, and the block is propagated to all nodes through P2P.
This is why blockchain technology is seen as a future technology.
It is impossible to modulate existing data because everyone has the same unmodulated data. And anyone can access existing records, so transparent services can be provided.
In addition, through smart contracts, autonomous applications that operate on distributed networks can be created rather than traditional client-server methods.
However, in the commercialization of blockchain, there are technical problems to be solved, such as "delayed agreement problem", "unknown responsibility material", and "security of surrounding technologies".

When applying blockchain technology to the existing "central control business network," there are problems such as "processing speed," "failure recovery," "system blocking," and "scalability."

There are many advantages, but from these various perspectives, it should be possible to embrace the diversity of business models

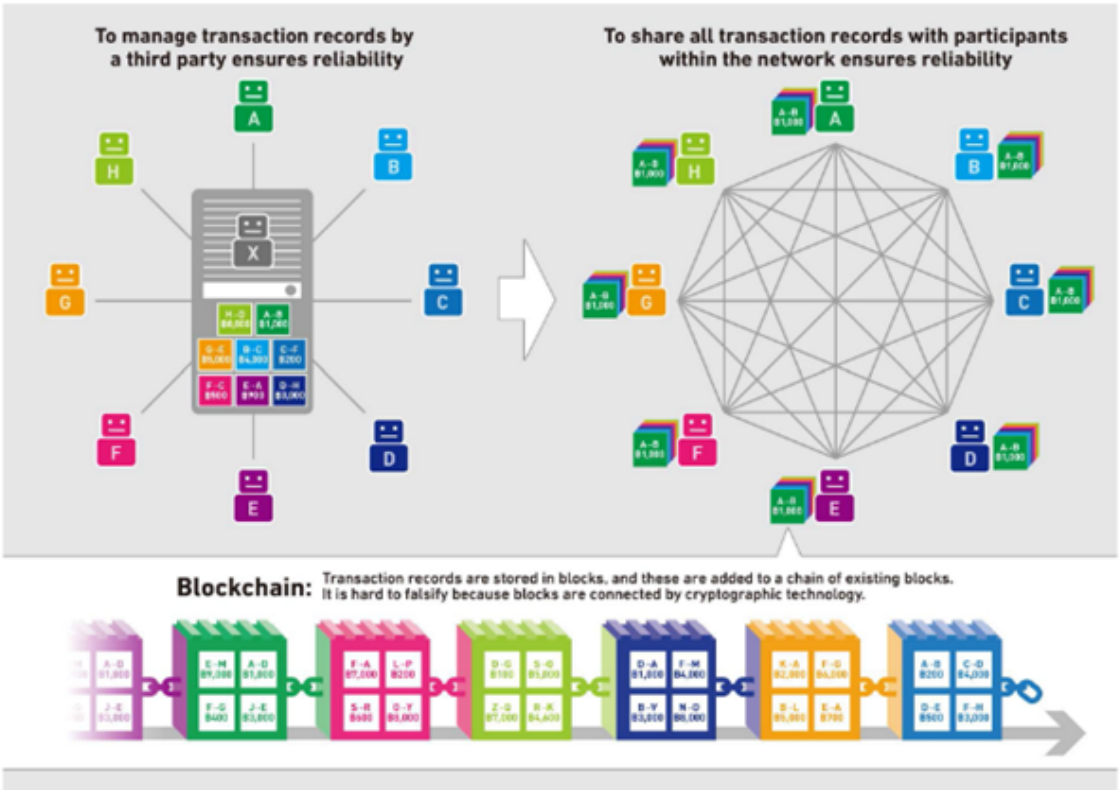


Figure 2. Technical Structure of Blockchain: Japanese Commerce Department

3. Overview of KMX

With the increasing number of connected and location-dependent technologies, our privacy and safety have become highly dependent on the accuracy and validity of location information.
While various attempts have been made to eliminate the need for centralized entities to control the flow of location data, all attempts have relied on the integrity of the devices that collect this data in the physical world.
To ensure a high level of data certainty for location information, we use a new formula that relies on a zero-knowledge proof chain. And we created an ecosystem of KMX networks based on reliable encryption locations.

KMX is an abstraction that enables the identification of layered locations across many device classes and protocols.

It provides blockchain ecosystem platforms such as blockchain technology, integrated electronic wallet security, digital source verification system, multimodal, distributed integrated authentication private, and public blockchain technology.
A new set of encryption mechanisms, known as Proof of Origin & Bound Witness, that combine real-world data collection capabilities into systems that use applications today, is key to this technology.

The emergence of blockchain-based unreliable smart contracts has significantly increased the need for trust services to mediate contract outcomes.
Most smart contracts rely on a single set of trustworthy oracles to settle the contract's outcome.

This is not a problem if both parties can agree on the authority and corruption of the stated trust. In most cases, however, the appropriate trust does not exist.In addition, due to the possibility of error or damage to the trust, it cannot be considered as having the authority.

Blockchain technology basically has time information (Timestamp) trust, but it lacks trust in location.
It depends on the components of the relay, storage and processing, or trust in the

location of the physical world item
All of these components are error-prone and corrupt, and are at risk of data manipulation, data contamination, data loss, and collusion.
As a result, the following problems exist:

Both the certainty and accuracy of the transaction location are negatively affected by the lack of a distributed location trust with no trust.

Platforms such as Ethereum and EOS have been used extensively for key escrow-related cases for fundraising in ICO format and for the right to safely mediate interactions online.

However, all platforms are currently focused only on the online world, not the real world, due to the problematic nature of information channels and the integrity of data that can be corrupted.
The KMX network has been working to develop concepts that allow developers to interact with the real world as if they were APIs to create smart contracts for blockchain platforms.

The KMX network is the world's first KMX protocol that allows two entities to trade centrally in the real world without third parties.

Thanks to abstraction, developers don't have to validate locations. We were able to create a protocol that contained a new use case that was not possible until today.

The KMX network is deployed through a customer-oriented business environment based on an existing infrastructure consisting of over 1,000,000,000 devices distributed worldwide.
KMX's Bluetooth and GPS device Internet allows consumers to place physical tracking signs on items they want to track (e.g., keys, luggage, bicycles, and pets) every day. If they lose or lose something, they can check the exact location in the smartphone application.

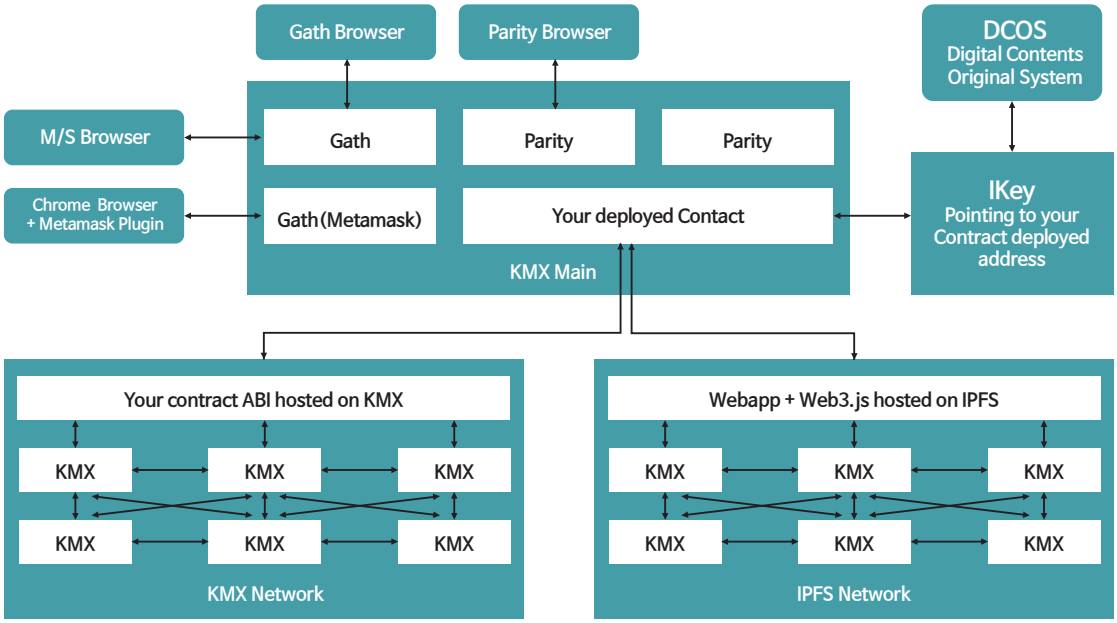


Figure 3 Differences in KMX Network Block Information

3.1. Proof of Location

The concept of a demonstrable location has evolved since the 1960s.In the 1940s, there was a ground-based radio navigation system like LORAN.

Today, there are location services that stack multiple media and triangulate them or prove their location through GPS and IP services.

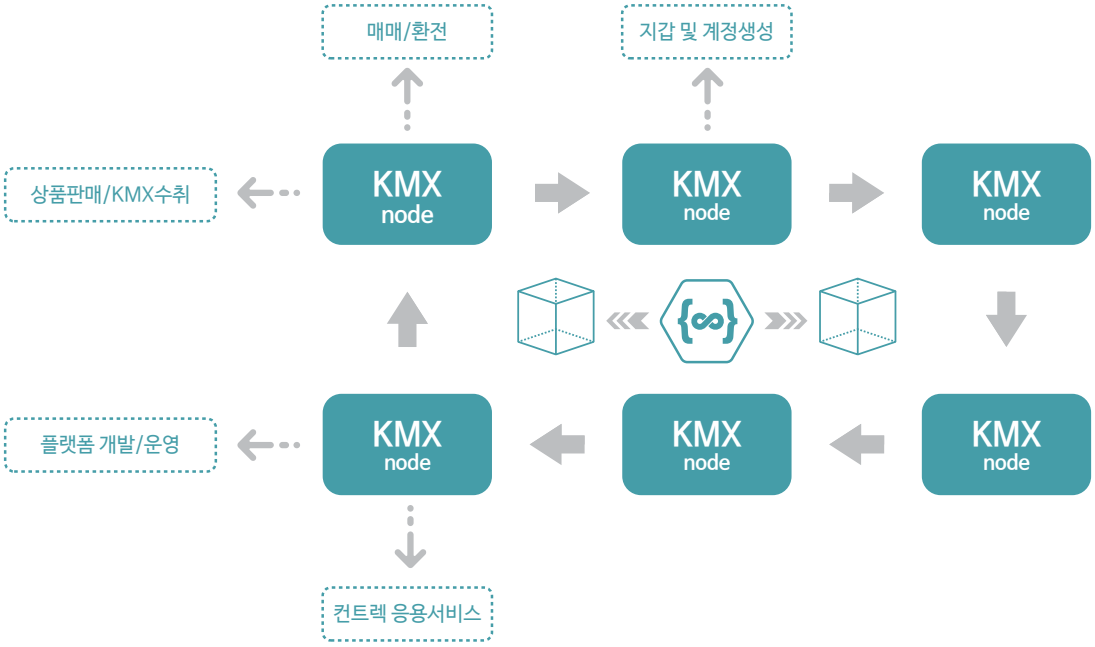
KMX Network has made it possible to develop smart contracts at the actual contract site using patent-registered technologies such as "digital content original System" and 4 other patented technologies and multimodal technologies.

We focused on the application of bridging locations and the creation of all digital content on the blockchain world Internet and the use of smart content. In other words, "Digital Content Original Sytem Key (DCOS: Ikey) is applied to smart content block information.

By using Nodes of all blockchains, transaction location information as well as transaction time information is automatically generated when user-to-user transactions are made.

Therefore, trust between anonymous users can be further improved.

This is the same when trading through an exchange using an electronic wallet.



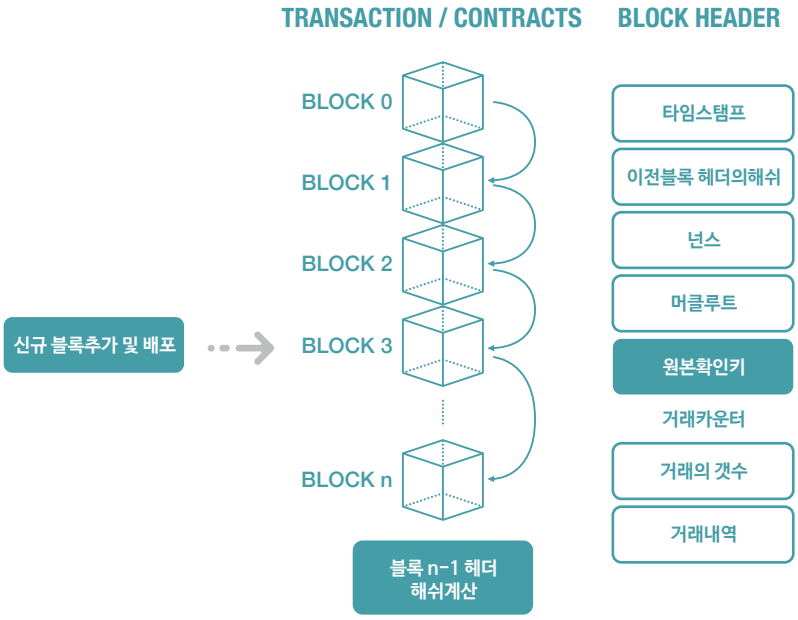


Figure 4 Application of digital content original system technology : Digital content original key

Reliable location proof is one of the most challenging things to implement. Even if there are many participants who can prove each other's location, there is no guarantee that they will have to go to Civil at any point in the future, and it is difficult because they rely on most reports.

If a special hardware device, such as a private key being compromised when a user attempts to open a private key or change the software, is implemented, it can have greater security, but at the same time, it is not impossible to spoof signals such as GPS or IP.
Proper implementation of this requires many alternative systems, accuracy for many different data sources, and sufficient project funding.

In summary, location proof leverages strong properties of blockchain such as timestamp and decentralization. It can also be understood as combining with an o-chain, positional recognition device that can resist blocks.

We consider the area of cryptographic location technology as Crypto-Location.

The Crypto-Location system faces the same problem, just as the weakness of smart contracts revolves around trusts that have a single cause of failure.

A vulnerability in current encryption location technology is centered on o-chain devices that report the location of objects.
In smart contracts, o-chain data sources are trusts.o - A chain data source is a special type of trust information called LocatorP (Sentinel).

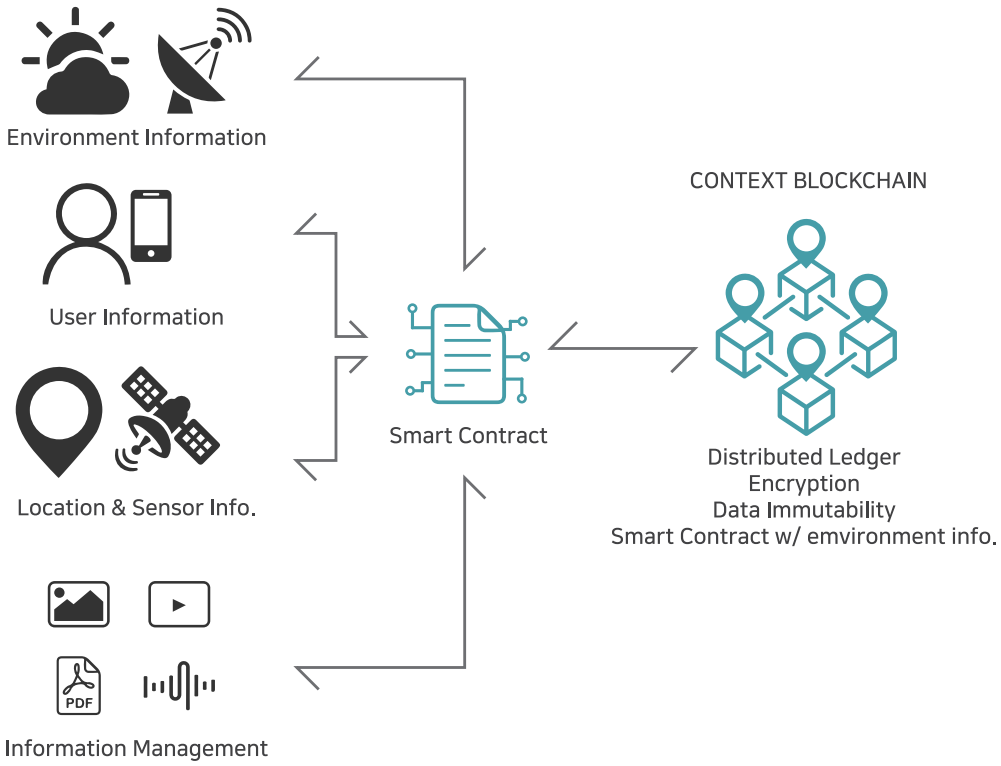
In the real world, the core surrounding the KMX Network is based on location-protocol-based, lossless, location-based evidence.

3.1. Application of patent technology for context blockchain

It is a Context blockchain that increases the reliability of transactions by recording environmental information at the time of transaction beyond the limits of smart contracts of second-generation block chains such as Ethereum and EOS, which only recorded time stamps.

Environmental information refers to information such as 5W1H (When, Where, Who, What, Why, How) necessary for real-life transactions.

This provides the basis for using blockchain in real life by ensuring the reliability and transparency of transactions.



3.1.1. (Contract apparatus and method of blockchain using digital contents original key) Patent registration number: 10-21785830000

A blockchain type contract terminal and method using a digital content original confirmation key are used.

Input module that receives the contract details of the target to be contracted;

Location information collection module that collects location information in real time at the time of the contract of the above target;

A contract generation module that generates a contract using the contract information received by the input module and the location information collected in real time by the location information collection module;

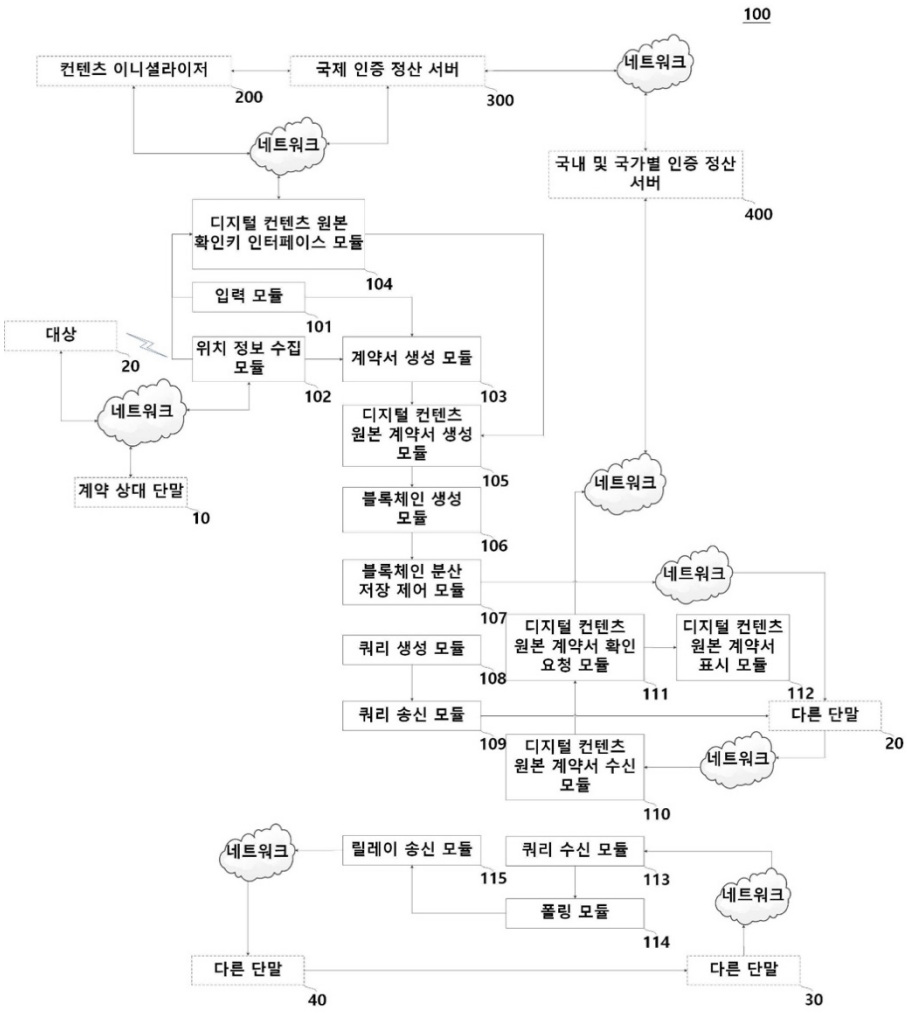
A digital content source verification key module that provides the contents initializer and international authentication settlement server

with the contracts entered by the input module and the location information collected in real time by the location information collection module

Digital content source contract generation module that combines the digital content source verification key received from the above digital source verification key interface module with the contract generated by the above contract generation module to generate a digital content source contract;

A blockchain generation module that generates a blockchain by encrypting a contract generated by the digital content original contract generation module;

A blockchain distributed storage control module is configured to transmit the blockchain generated by the blockchain generation module to another terminal in a P2P method so as to distribute and store the blockchain generated by the blockchain generation module on a
network.



3.1.2. (Contract apparatus and method of blockchain using location information) Patent registration number: 10-21203300000

Blockchain type contract terminals and methods using location information are used.

Input module receiving contract details of the target to be contracted;

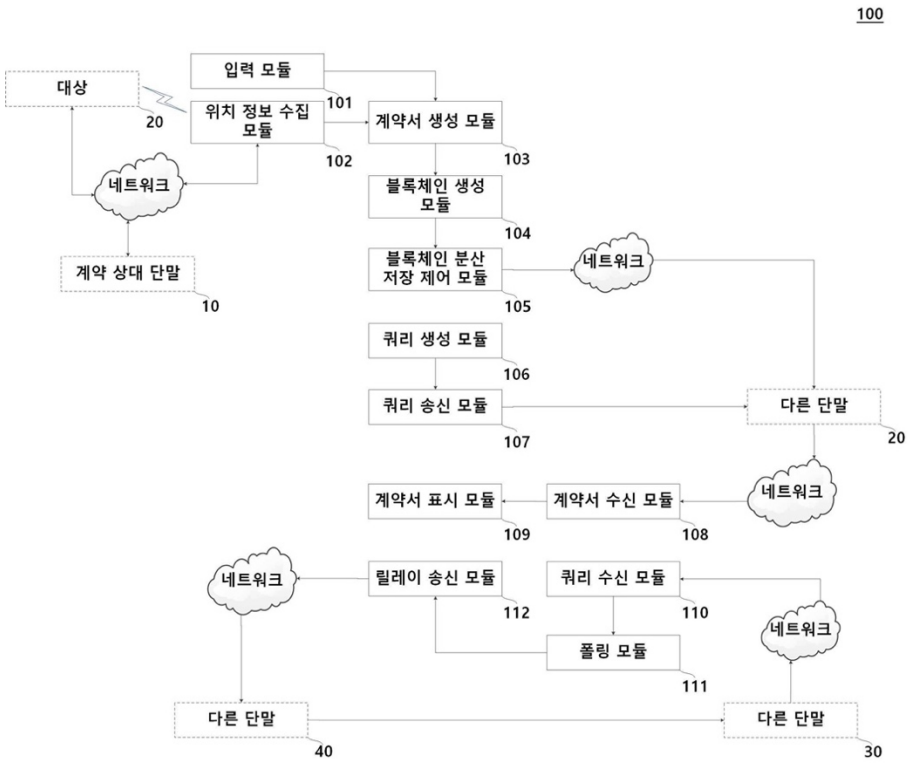
Location information collection module that collects location information in real time at the time of the contract of the above target;

A contract generation module that generates a contract using the contract information received by the input module and the location

information collected in real time by the location information collection module;

A blockchain generation module that generates a blockchain by encrypting a contract generated by the contract generation module above;

A blockchain distributed storage control module is configured to transmit the blockchain generated by the blockchain generation module to another terminal in a P2P method so as to distribute and store the blockchain generated by the blockchain generation module on a network..



3.2. Application of patent model technology for "digital content original verification technology"

Unlike the concept of original verification in the real world, a model that recognizes three layers of conceptual models through digital content

original verification on the Internet is presented.

Information layer

It refers to structured information such as census data and employment data (most common data "concept") and unstructured information such as data sheet press releases and regulatory guidelines (including digital content and digital documents).

Platform Layer

- It includes the entire system and process for managing information.

  These include digital content management systems and Web Application Programming Interface, application Cleanet (X) development, hardware (mobile equipment or PC) used to access information, and services that support critical IT functions such as human resources or financial management.

  Web API refers to a machine-to-machine interaction system in a network and is related to the transmission of data.

  Strategic Principles: Four important principles necessary to facilitate the above transformation

  an information-driven approach
  It means moving away from the dimension of "digital content" management and converting to open and separate (discontinuous) data and continuous digital content management.

  Data and content are tagged, shared, and secured in the most useful way for users of the information, and presented as convergence.

  Shared Platform Approach

  It supports collaboration both within and between agencies.
  Consistent standards are applied through cost reduction and efficient development.
  Consistency is guaranteed in the way in which information is produced and

distributed.

- A user-centric approach:

It supports collaboration between websites and mobile applications, applying consistent standards and ensuring consistency in the way in which information is produced and distributed through cost reduction and efficient development.

- Security and privacy platforms:

Digital content services can be delivered and used safely and securely, and changes can be induced to protect information and personal information..

3.2. DCOS-Digital Contents Original System

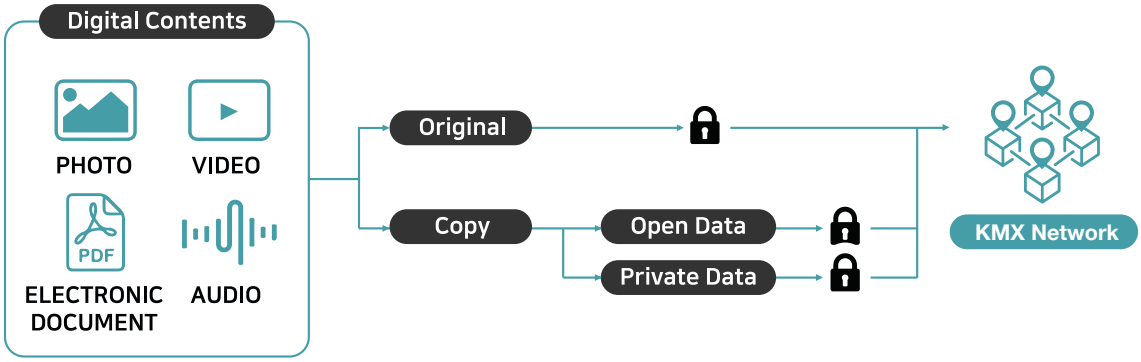
It is a system that controls the entire process of generating, recording, distributing, and discarding digital content (e-documents, videos, sound sources, photos, program sources, etc.) generated online and offline.

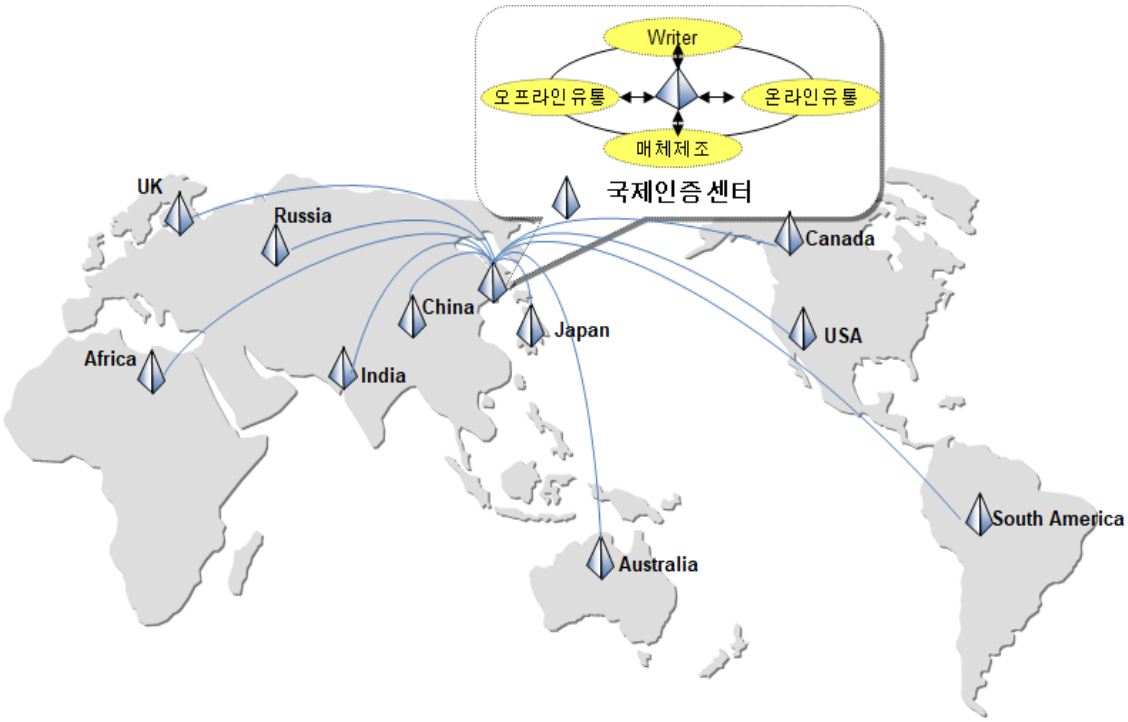
Collected data is stored as a source and a copy, the original is stored on its own system, and the copy is distributed. A system that fundamentally prevents distortion and deterioration of data by making it possible to always verify the source of the distributed data.

It is a key technology that includes not only life cycle management of digital content but also settlement.

Combined with spatio-temporal blockchain technology, it can prevent forgery/modification of documents issued by the government and government offices such as resident registration copies, real estate register copies, and seal certificates. In addition, it is a technology patent system that can be used for problems related to re-use of issued documents and for managing program source copyrights. (Patent registration number: 10-20120092270~4)

- 10-1355077 System for creating and certifying and method thereof
- 10-1356210 System for registering the original of digital contents and method thereof
- 10-1355080 System for syndicating the original of digital contents for personal users and method thereof
- 10-1355081 System for syndicating the original of digital contents for contents provider and method thereof
- 10-1356211 System for creating the original of digital contents and calculating the fee of the same and method thereof





〈 Coverage concept: Recording online/offline content and controlling the entire process until disposal〉

3.3. Application of multimodal patent technology

A multimodal search method, a multimodal search device, and a recording medium are provided. According to this multimodal search method, it may transmit a search request using user information, the sensing information, and the received user input information. Since the search is performed based on comprehensive information on the user and surrounding environment as well as user input for search, it provides more necessary and satisfactory search results to users.

Multimodal patent registration

• 10-1518385 Multimodal Search Method, Multimodal Search Device, and Recording Media

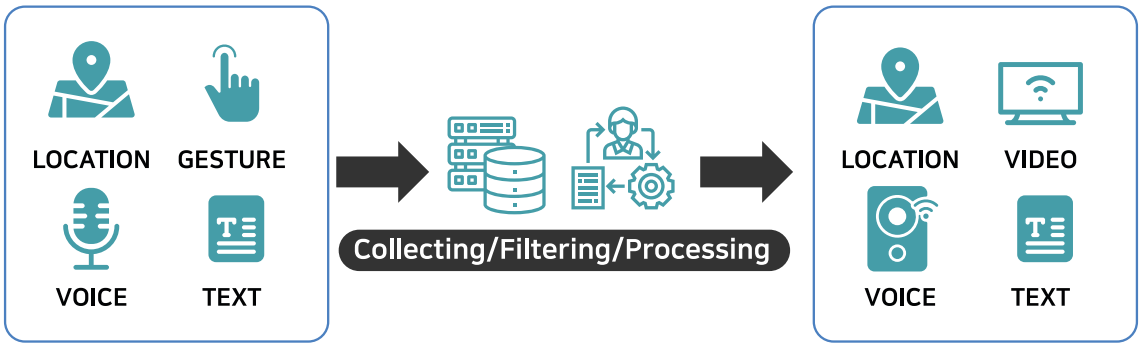


Figure 5 The concept of multimodal interfaces

4. KMX Network Platform Configuration and Technology

KMX Network is designed to use both private and public blockchain, and the basic construction is as follows.

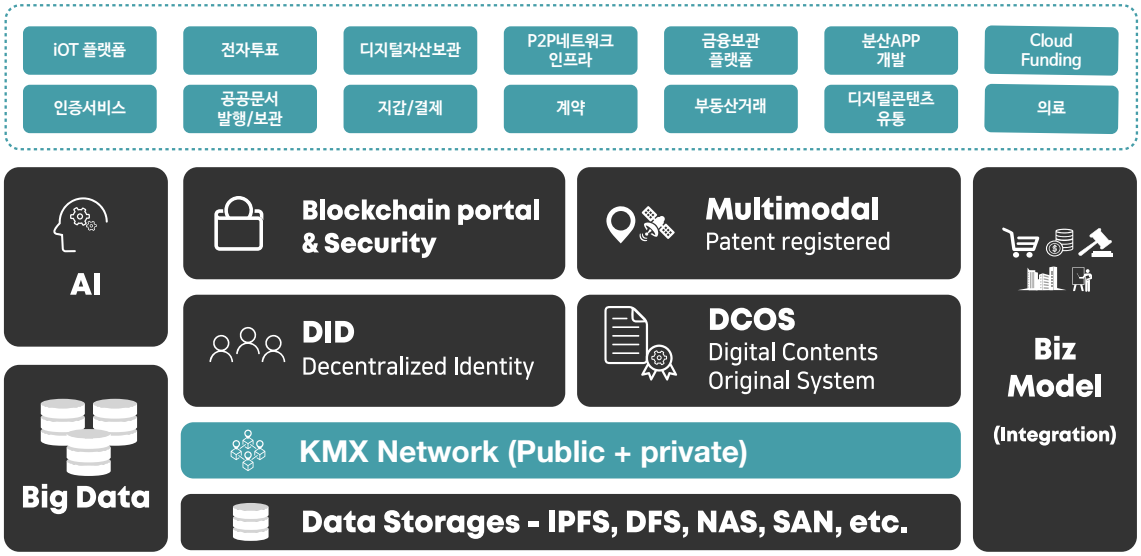


Figure 6 Basic Structure and Technology of KMX Network Platform

4.1.IPFS (Inter Planetary File System)

It is a P2P distributed file system that attempts to connect all computing devices to the same file system.

- IPFS is a similar concept to the web
- IPFS provides a content addressed block storage model with high throughput using content addressed hyperlinks.
- It is a generalized form of Markle DAG, a data structure that can build versioned file systems, blockchains, and archival web pages.
- IPFS exchanges incentive blocks, combining distributed hash tables and self-authentication namespace.
- IPFS does not have a single point of failure, and each node does not need to trust each other.
- Interplanetary File System (IPFS) is a new hypermedia distribution protocol that addresses content and IDs.
- IPFS enables the creation of fully distributed applications.
- It aims to make the Web faster, safer, and more open.

4.2.KMX Network

The goal of the network is to create an attack-resistant and reliable distributed location proof system. KMX Network's basic technology is designed based on the concept of patent-registered "digital content original verification technology and its method" and four other technologies.
The system provides the highest possible certainty when dealing with available data. Depending on the components of the system, this is done with a set of abstractions that significantly reduce the risk of location recognition through a zero-knowledge proof chain.

The KMX Network system provides an entry point to the protocol of the connected device that provides high certainty for location data through an encrypted proof chain .This is issued by the user.

Transactions are called queries. "To retrieve location data from a blockchain platform with SMART CONTRACT capability, the aggregator of the KMX Network listens to queries issued in the contract and gives the most accurate answer: Resend encryption credentials to this collector. These collectors reach an agreement on the best answer and then provide the response back to the smart contract. This network of components is at a specific X.Y. coordinate at a given time, providing the most reliable and reliable certainty.

The KMX Network has four basic components: LocatorP (Location Data Collector), ConnectorP (Data Properties), StoreP (Data Storage), and SniperP (Response Information).

LocatorP collects location information through sensors and other means.
KonnectorP takes this data from LocatorP and provides it to StoreP.

The archivist stores this information for SniperP to analyze.
SniperP generates a response to a query.In addition, StoreP analyzes location-heuristic teaching methods to assign accuracy scores.

SniperP then delivers these answers back to smart contracts (so SniperP acts as a trust).

The accuracy score, Origin Chain Score, is determined by a zero-knowledge proof known as Origin Chain of Proof.

This chain guarantees two or more pieces of data from the same source without revealing basic information.

Each component that follows the query path creates a unique Proof of Origin and then reconnects to each component that connects the data.

Proof of Origin is a new format for building a set of encryption guarantees along the network's repeater path for high reliability of real data.

This proof of origin (Proof of Origin Chain) encapsulates the content that can be held in any location data up to the first device from which the data is collected.

In the next section, let's look at how Proof of Origin works.

To establish a mechanism for decentralization agreement among dividers, the KMX Network relies on a common invariant blockchain known as the KMX Main Chain, which stores data and query transactions collected from SniperP and related source scores.

Before we go into detail about the functionality of the entire system, we will clearly define responsibility for each component of the network.

LocatorP

LocatorP is a position witness. They observe data heuristic teaching.And it creates a time ledger to ensure the certainty and accuracy of the heuristic teaching method. The most important aspect of LocatorP is that it produces a ledger that can determine whether different components originate from the same source.

They do this by adding Proof of Origin to the relay chain of evidence.

Because the KMX Network is a reliable system, LocatorP must provide honest location information. This is done by combining reputation and payment components.

LocatorP is rewarded with the KMX Network Token when the information answers the query. To increase the chances of receiving a reward,someone must create a ledger that matches their colleagues and provide Proof of Origin to identify the source of someone's location information.

ConnectorP

ConnectorP is a location data transrider. They safely deliver the location ledger to the custodian at LocatorP.
The most important aspect of ConnectorP is that StoreP is confident that the heuristic methodology ledger received from ConnectorP has not changed.
A second important aspect of ConnectorP is the addition of an additional Proof of Origin.
Because the KMX Network is a reliable system, incentives must be provided to provide honest broadcasting of heuristic teaching methods. This is done by combining reputation and payment components. ConnectorP is rewarded with the KMX Network Token when the relayed information answers the query. To increase the chances of receiving a reward, someone need to create a consistent ledger with colleagues and provide Proof of Origin to identify oneself as a mediator in heuristic teaching.

StoreP

Archives store location information in a distributed form for the purpose of storing all historical ledger.

Even if some data is lost or temporarily unavailable, the system will continue to operate at the same time, albeit less accurate.

The archivist shall index the ledger to facilitate the return of bookkeeping data, if necessary.

Archives store only raw data and receive paid KMX Network Tokens for data retrieval and subsequent use.
Storage is always free.

Archives are networked.Therefore, the archivist is asked for data that is not included by other archivists.

StoreP can optionally store ledger information that is returned.

Most of these will be two types of archives: data stores in the data center and big data stores in the data center.

The archivist in the middle would be a hybrid. The choice to store data is not enforced, but can be done easily through IPFS or other distributed storage solutions.

Each time one StoreP hands over the material to another StoreP, a record archive fee is paid. Therefore, additional Proof of Origin is added to track payments.

If someone wants to increase the validity period for a search, they can set a minimum Proof of Origin level.
LocatorP, ConnectorPs, and StoreP costs should be adjusted to prevent data expansion.

SniperP

SniperP is the most complex part of the KMX network. SniperP's overall goal is to get the most accurate data for a query from the KMX Network and relay that data back to the issuer of that query.

SniperP polls its blockchain platforms (e.g., Ethereum, Stellar, etc.) for queries issued in the KMX Network Smart contract.

It then interacts directly with the StopreP network to obtain the response with the most accurate accuracy / impact score to find the response to the query.

They judge the source of the evidence as the best evidence. Respondents with the best score in the shortest time can create blocks on the default KMX Network Blockchain (KMX Main Chain) through Proof of Work.

Queries are prioritized by reward size and complexity.Therefore, the more answers, the higher the priority of the query.

The other SniperP reaches an agreement on the validity of the block and digitally signs the block.

SniperP, the block's coinbase address, will send transactions to smart contracts with answers along with accuracy scores.
It also sends a signature list of other SniperP to prevent attackers from issuing fake information.

4.3. End-to-End Functionality

The responsibilities of each component have been described in detail, so here is a general example of how the system works.

(LocatorP Gather Data)

LocatorP gathers the actual location navigation methods. LocatorP prepares its Proof of Origin to chain over its nodes.

(ConnectorPs Gather Data From LocatorP)

Collect the required data from the Online LocatorP and add Proof of Origin to the chain. Then make it available to the person who keeps the network records.

(StoreP Index/Assemble Data from ConnectorPs)

ConnectorP continuously sends information to StoreP. StopreP is stored in a distributed store with a location-heuristic teaching method index

SniperP Fetches a User's Query)

SniperP investigated the queries sent to the Ethereum Smart Agreement and decided to begin the answer writing process.

(SniperP Collects Data From StoreP)

SniperP then decides to take the appropriate information from the StopreP network and perform the query.

(SniperP Formulates Answer)

Divine selects the Best Answer for queries that contain the best Origin Chain Score on the StopreP network.

(SniperP Proposes Block)

SniperP proposes a block of KMX Main Chain containing responses, queries, and KMX tokens (KMX) through Proof of Work.

When someone on the network digitally signs the content of a block, the coinbase account is updated to reach an agreement on a valid block, and the system displays Proof of Work.

(SniperP Returns Result to Query Initiator)
SniperP packages response, Origin Chain Score, and digital signature sets. And send it to adapter components that are securely connected to KMX smart contracts.

The adapter verifies that SniperP is not compromised and sends a set of digital agreements to a smart contract.

This occurs immediately after the block creation process. Coinbill SniperP will then receive the Coin payment.

(KMX Network Components Get Rewarded for Their Work)
Components that follow the Proof of Origin Chain pay for getting responses to queries.
In other words, LocatorP, ConnectorP, StoreP, and SniperP are all rewarded for their work at the time of transaction.

If the same query is requested more than once, more than one response can be generated. Because the response generated at any given moment is based on the heuristic teaching that the system can have at that time.

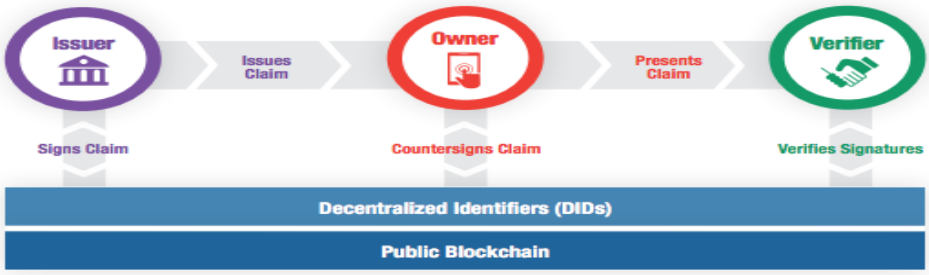
Two steps are required to submit an answer to the blockchain.

First, the analysis should be performed to determine the best answer to the query.

When the system generates multiple responses, the node compares the responses and always chooses a better answer. Examples of simple queries include:
(Example: "Where were the nodes on the network at a specific time in the past? ")

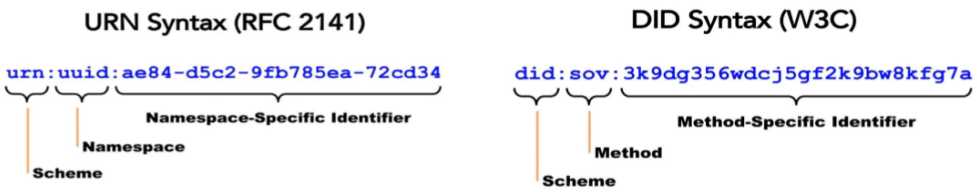
4.4.DIDs(Decentralized Identifiers)

It is the only identifier in the world that is registered in a distributed ledger technology or other form of distributed network without a centralized registrar.



〈Concepts and Structure of DIDs〉

- Verifiable Claim (VC): Verifiable claims and verifiable details.
- Issuer: Issue VC, issue VC to Holder.
- Holder: Hold the VC, keep the issued VC in your wallet, and counter-sign it when necessary.
- Verifier: Verify VC and validate signature.



〈Difference between DID and URN〉

Key features and benefits of DISs Architecture

Decentralization: The DID architecture is the only identifier in the world and includes public verification keys, service endpoints, and metadata. No central authority should be required or ID management failure problems should arise.

- Sovereignty: The DID architecture should give entities the power to control themselves and their digital identity without relying on external authority, whether human or non-human.
- Privacy: The DID architecture must protect the privacy of information from entities and be able to control other data to be gradually exposed.

• Security: The DID architecture must have sufficient security for members in accordance with the DID documentation at the guaranteed level required by members.
• Proof-based: The DID architecture should have cryptographic demonstration methods for authentication and authorization authority.
• Discoverability: The DID architecture should be able to find different DIDs to know and interact more about different entities.
• Interoperability: The DID architecture uses software libraries designed for interoperability in addition to existing tools.It should also ensure that DID infrastructure uses interoperability standards.
• Portability: The DID architecture should be a network-independent system that can use the digital identifiers of entities in any system that supports DIDs and DID methods.
• Simplicity: To meet these objectives, the DID architecture (quote Albert Einstein) should be "not simpler, but as simple as possible".
• Scalability: The DID architecture must be scalable without significantly interfering with interoperability, portability, and simplicity.

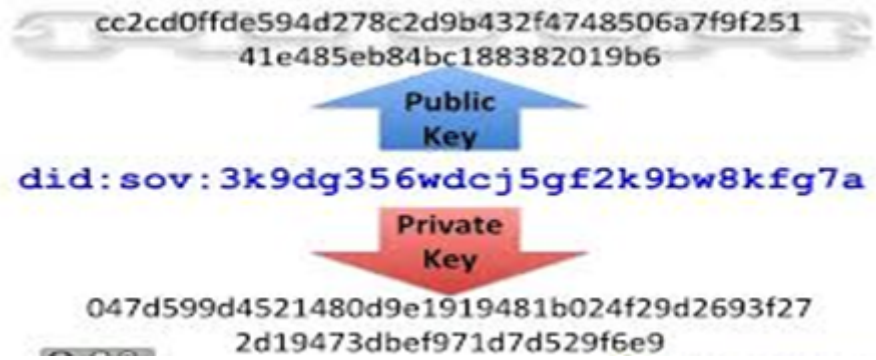


Figure 7 Relationship between DID and the Private Key and Public Key of the Electronic Wallet

4.5. Integrated e-wallet and security

The KMX Network fully secures personal assets (coin, bank, card, health, etc.) that are the basis for transactions, including integrated electronic wallets, according to its own security standards.

Supports DUKPT-based encryption key management

a. DUKPT(Derived Unique Key Per Transaction)
• This is a key management scheme that encrypts/decrypts using the One Time Encryption Key, which is generated each time by the Secret Master Key shared between the HSM server and the user terminal.

b. Why use the DUKPT method?
• All security uses its own encryption key.
• In the event of Key security management, the use of the strongest cryptographic algorithm is meaningless.
• The DUKPT method was designed on the premise that the same encryption key is not used in the encryption/decryption process.

c. DUKPT Features
• It supports encryption with a one-time key, which is used only once each time a user's forwarding information is sent.
• The same Secret Master Key is shared between the user terminal and the HSM server. : However, the master key is not used as an encryption/decryption key.
• Network Information Security: It supports secure layer and data encryption.

Create/Distribute Security Keys, Manageability

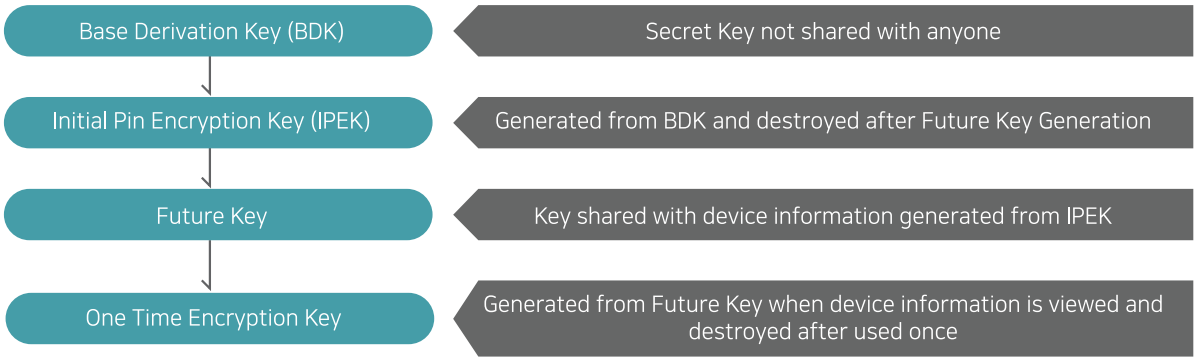


Figure 8 Process for generating security keys

a. Entering and managing the Secret Master Key (BDK)

• The HSM server is input through Cross-Check of the Key Component, which is secured by at least two people.

b. Key management

• Future Key is injected equally into all card readers in the manufacturing process. If the future key of the card reader is leaked to the outside, a new key can be created and replaced.

• If BDK is leaked, BDK itself can be replaced through a new Key Component.

• The Future Key of the terminal transmission information reads the terminal information every time and generates a new encryption key (One Time Encryption Key) when transmitting. It disappears after use.

Encryption/Decryption Support

a. Key generation and encryption transfer processing

• Terminal equipment

• As soon as the information is read, a one-time encryption key is generated from the Future Key injected into the Head and encrypted together with the terminal information data.

• The encrypted data is transmitted to the decryption server HSM together with the Key Serial Number (KSN).

b. Decryption processing

• Based on KSN, the HSM server decodes the data after separating the one-time encryption key and encrypted data through Future Key matching.

c. Encryption algorithm support

- Symmetric Key Algorithm Support: DES and Triple-DES
- Signature information: Applying ECC algorithms

4.6 Artificial intelligence technology based on big data

Based on artificial intelligence technology, it provides neural network-based pre-learned models and the latest machine learning services. It provides productivity and efficiency by applying it to various artificial intelligence applications of corporate customers.

Ainesha Natural Language

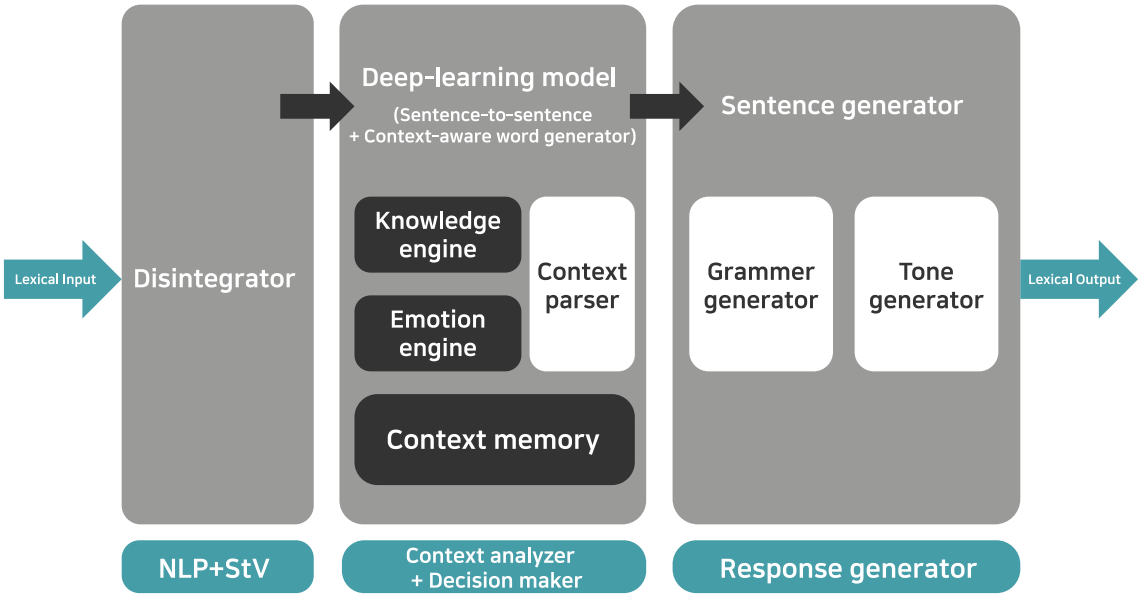
It is possible to grasp the structure and meaning of various languages through Word Embedding.Therefore, it can be used to extract the information contained in textual documents held by the enterprise. It can also analyze emotions or identify intentions contained in a language.

Ainesha Visual Recognition

It categorizes document images into thousands of categories (ex. resident registration copies, abstracts, etc.), and finds and reads the characters in the images.
It can also identify objects, symbol characters, behaviors, etc. in the image according to the purpose of use.

Ainesha Speech Recognition

It can be used in a variety of ways, such as converting the user's voice input into text or setting up the ability to manage it as a command through voice. It can also produce a natural voice similar to the real thing by synthesizing the voice of a particular speaker.


Lexical Input
Disintegrator
Deep-learning model
(Sentence-to-sentence
+ Context-aware word generator)
Knowledge engine
Emotion engine
Context parser
Context memory
Sentence generator
Grammer generator
Tone generator
Lexical Output
NLP+StV
Context analyzer
+ Decision maker
Response generator

5. KMX Network - Features and Benefits

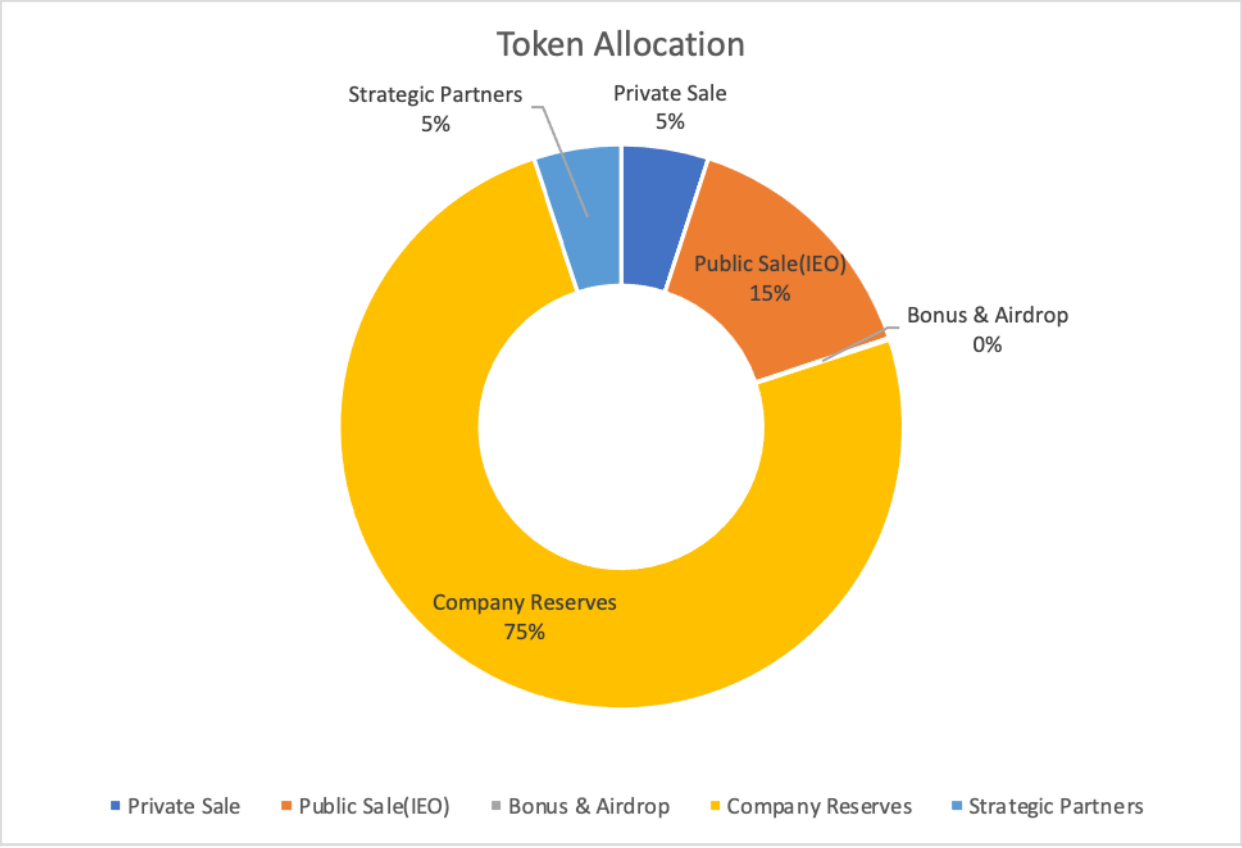
- Business Network: Transactions are agreed upon by business network participants.
- Asset tracking: transparent visibility of when/where/how transactions were performed by any participant
- Consensus: Provide trust by consistently sharing business network transaction information as a single view
- Immutability: Resolve disputes between participants quickly and easily
- Finality: flexible response to errors or fraudulent counterfeiting
- Advantages: time saving, cost saving, risk reduction, trust spread

6. Token Specification

Contents	Details
Blockchain Protocol	Ethereum (ERC-20)
Platform Name	Korea Mainnet X
Token Name	Korea Mainnet X
Ticker	KMX
Circulation Volume	20%
Total Volume	4,000,000,000
Investment Method	BTC, ETH
Voting Rights	No
Bonus	Yes
Refunds	No
Repayment	No
KYC/AML	Yes

7. Token Allocation

Contents	Percent	Quantity
Private Sale	5%	200,000,000
Pre-Sale	0%	0
Public Sale	14.9%	596,000,000
Bonus & Airdrop	0.1%	4,000,000
Company Reserve	75%	3,000,000,000
Strategic Partners	5%	200,000,000
Total	100%	4,000,000,000



8. Use of Proceeds

Contents	Percent
Development & Technology	50%
Management & Staff	15%
Administrative Expenses	5%
Business Development & Partnership	4%
Marketing	15%
Team & Advisor	10%
Legal, Accounting & Other Professional Services	1%
Total	100%

9. Intellectual Property Rights

DCOS

디지털 컨텐츠의 원본 생성 및 확인 시스템과 그 방법
(SYSTEM FOR CREATING AND CERTIFYING AND METHOD THEREOF, No : 10-20120092270)

디지털 컨텐츠의 원본 생성 및 정산 시스템과 그 방법
(SYSTEM FOR CREATING THE ORIGINAL OF DIGITAL CONTENTS AND CALCULATING THE FEE OF THE SAME AND METHOD THEREOF, No : 1020120092271)

디지털 원본 컨텐츠 등록 시스템 및 방법
(SYSTEM FOR REGISTERING THE ORIGINAL OF DIGITAL CONTENTS AND MEHTOD THEREOF, No : 10-20120092272)

컨텐츠 프로바이더를 위한 디지털 원본 컨텐츠 배포 시스템 및 방법
(SYSTEM FOR SYNDICATING THE ORIGINAL OF DIGITAL CONTENTS FOR PERSONAL USERS AND METHOD THEREOF, No : 10-20120092273)

일반 사용자를 위한 디지털 원본 컨텐츠 배포 시스템 및 방법
(SYSTEM FOR SYNDICATING THE ORIGINAL OF DIGITAL CONTENTS FOR CONTENTS PROVIDER AND METHOD THEREOF, No : 10-20120092274)

MULTIMODAL

멀티모달 검색방법, 멀티모달 검색 장치 및 기록매체
(Multimodal searching method, multimodal searching device, and recording medium, No : 10-20130093450)

BLOCKCHAIN

디지털 컨텐츠 원본 확인키를 이용한 블록체인 방식의 계약 단말 및 방법
(Contract apparatus and method of blockchain using digital contents original key)

위치 정보를 이용한 블록체인 방식의 계약 단말 및 방법
(Contract apparatus and method of blockchain using location information, No: 10-2018-0139033)

10. Terminology summary

IPFS(Inter Planetary File System)

It is a P2P distributed file system that connects all computing devices with the same file system.It distributes and stores data or files that can be disclosed.

DCOS(DIGITAL CONTENTS ORIGINAL SYSTEM)

It controls and supports the entire process of creating, registering, distributing, discarding, and settlement of digital content based on source patents (5 types) for the digital sharing economy. It functions such as checking the original/copy of digital content (electronic documents, videos, sound sources, photos, etc.) and supporting the content distribution system through digital content authentication that cannot be reproduced.

Multimodal

A multimodal search method, a device, and a recording medium are provided. It is a technology that increases user-centered work efficiency by establishing a ubiquitous computing environment without a special device by utilizing biometric recognition such as voice recognition, gesture recognition, device pen, behavior recognition, and touch recognition.

The multimodal search method may transmit a search request using user information, the sensing information, and the received user input information. Since the search is performed based on comprehensive information on the user and surrounding environment as well as user input for search, it provides more necessary and satisfactory search results to users.

DID(Decentralized Identifiers)

It is the only identifier in the world that is registered in a distributed ledger technology or other form of distributed network without a centralized registrar.
It is a W3C standard certification technology that supports distributed integrated certification.

Integrated e-wallet and security

It provides security according to its own security standards to safely and completely protect customer assets (coin, bank, card, health, etc.), which are transaction criteria as well as integrated electronic wallets. It supports section encryption and data encryption required for electronic wallets and related DApps.

BIGDATA

It is possible to collect, refine, store, and analyze data such as structured, unstructured, and semi-structured data generated on the platform, and utilize search services and analysis results.

The big data system can reduce manpower costs by applying work automation technology to all stages of construction. Based on structured data refinement technology, the transition from input-oriented to data-oriented is supported, and fast artificial intelligence service development support and standardization technology of internal work are applied.

Artificial Intelligence Technology (A.I)

Artificial intelligence platforms based on big data and cloud technologies are interactive artificial intelligence automatic response solutions. It can be applied to various fields, especially to insurance, securities, banks, cards, online, manufacturing and distribution, and government agencies.

When a customer makes an inquiry, the intention of the question can be identified through natural language processing, and accurate answers can be presented through machine learning, statistical approaches, rule-based or machine reading, and intents in stages.

In addition, it is designed to immediately apply various existing tasks according to the business logic base, so it is possible to support services according to the direction customers want.

11.claimers

This white paper is intended to provide a detailed description of the overall content and progress of the project.
This white paper is not intended to encourage investment, etc., but only for the purpose of providing information.

Please note that the Company shall not bear any other liability, such as compensation, for any damages or other financial damages that may be incurred by the Investor by referring to this White Paper.

This white paper is prepared and provided on a date and does not warrant that any content contained in the white paper is accurate or unaltered to a future date. The information prepared in this white paper is based on judgment at this time, and this white paper is not legally required to be revised or amended by the project team.
The Project Team will not, and will not be liable for, any statement or guarantee to anyone who reads this White Paper in connection with this White Paper.
This white paper is not intended for countries, regions, or residents who are prohibited from distributing, publishing, or using it.
This white paper is only available for this project and may not be distributed, reproduced, delivered or published in part or in whole to anyone else without the prior written consent of the project team for any purpose.