The White Paper of **CLEBUS**

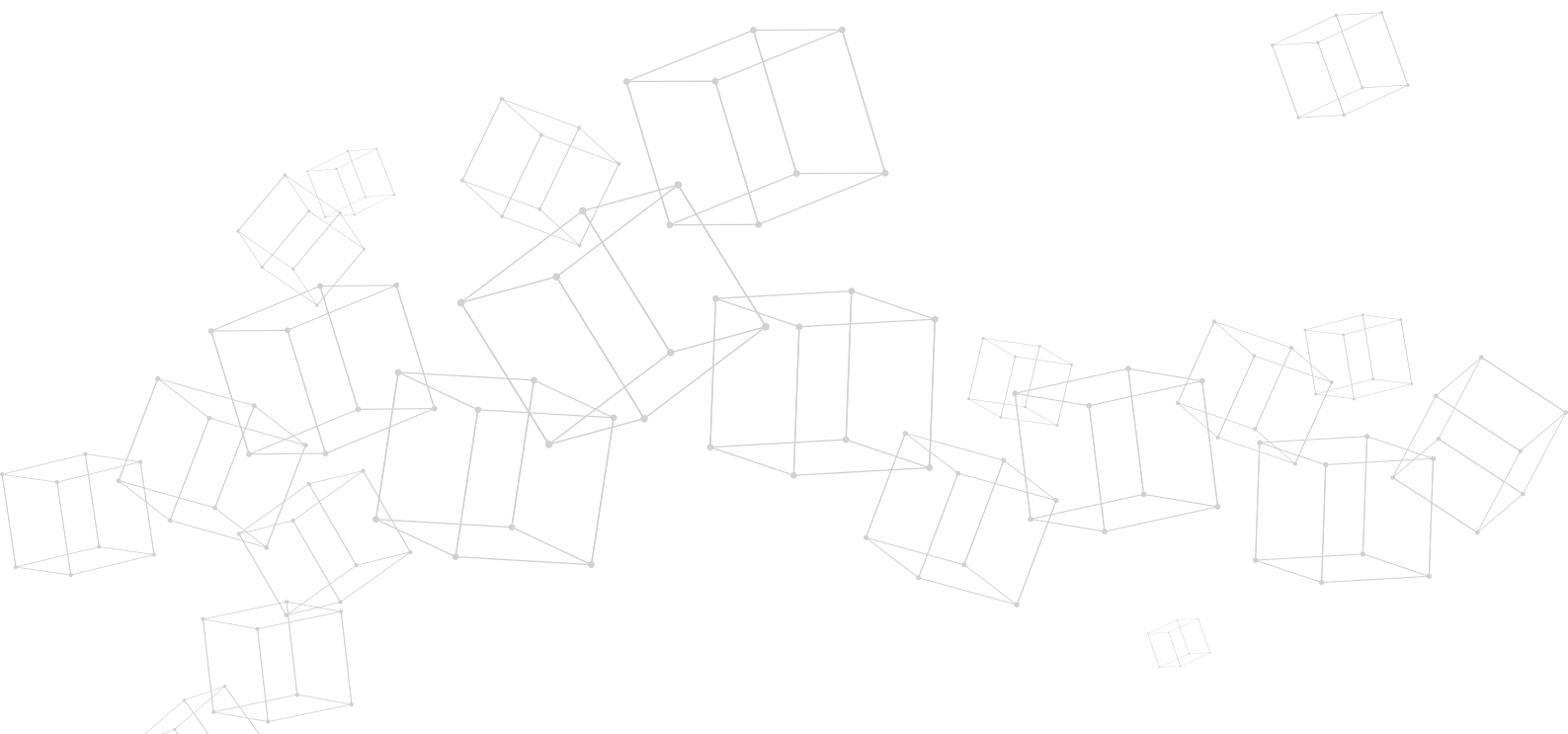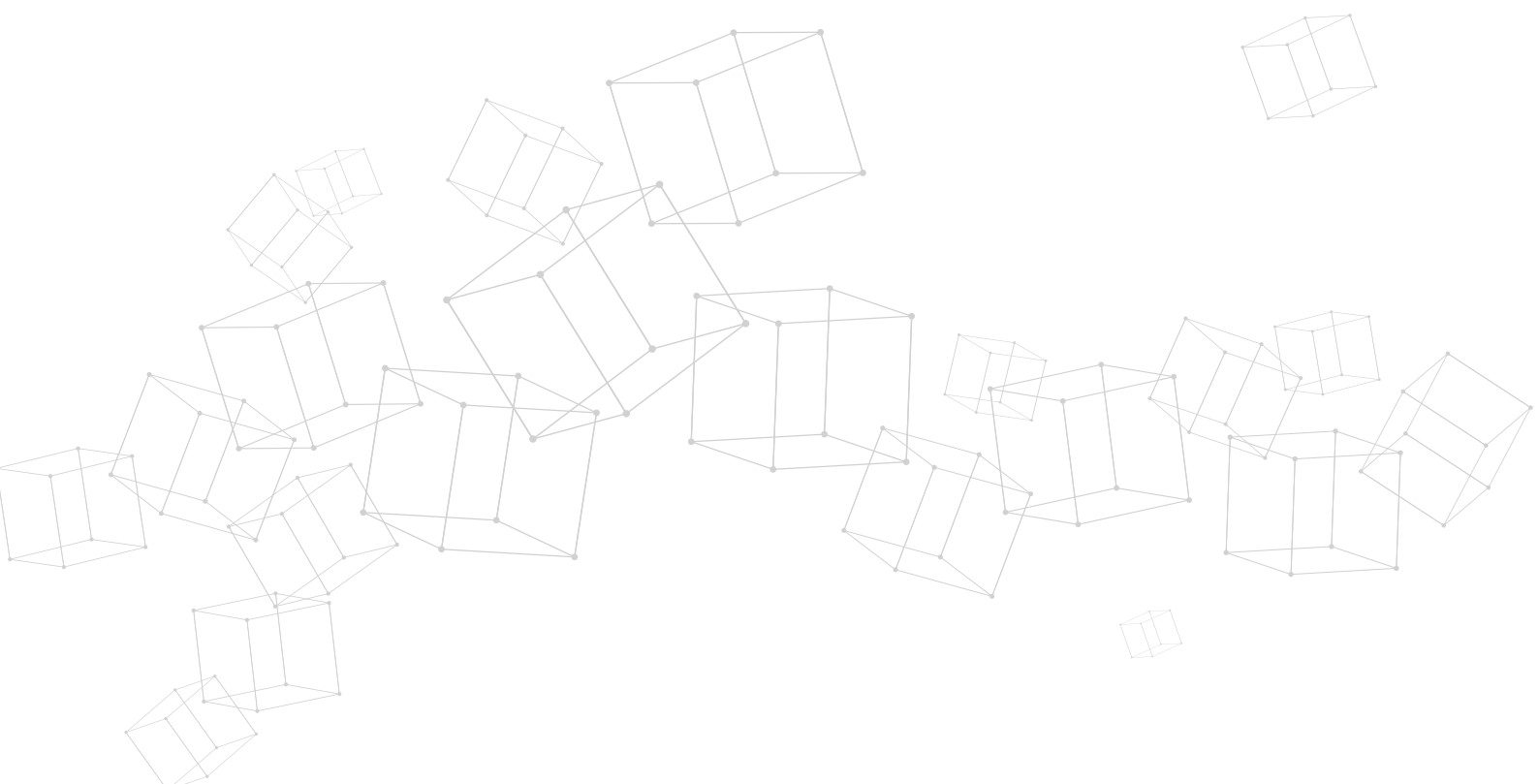**VER 2.0**

Table of contents

1. Abstract

CLEBUS™ is a combination of CLÉ and Universe, where CLÉ means Key in French.
To claim ownership of cryptocurrency, you need an account number and a password (private key) for the account. Since your account number is publicly available, your private key is your only online asset. As an online platform that pursues "Life to Earn", CLEBUS serves as a stage for users to multiply their online assets.

With the vision of "contributing to humanity by providing a sustainable hyper-connected ecosystem," the CLEBUS ecosystem aims to build a sustainable WEB3 ecosystem through the WEB2 → WEB3 transition and the identification of digital beings using NFTs based on blockchain technology. In particular, various chatbots created through generative AI platforms such as Open AI's GPT are verified, certified, and guaranteed through CLEBUS's own NFTs. Through CLEBUS, anyone in the world can certify their creations, products, services, and various resources and assets as NFTs to be commoditized and traded to generate revenue, and global users who use it can also participate, consume, and enjoy life as prosumers(producer and consumer).

CLEBUS already provides its own NFT certification services in various sectors, including automotive (Mercedes Benz Korea's official dealer H), golf, beauty, art, music, defense, and global NGOs. Various partners such as Mercedes Benz and their existing customers, connected through NFT authentication, are also organically connecting with each other and creating synergies to evolve into an expanded ecosystem. In this way, CLEBUS is contributing to WEB2 → WEB3 and plans to provide an open marketplace where various AI chatbots from around the world can certify and trade NFTs. CLE is a token used in the CLEBUS ecosystem, which is used as a gas fee to prove identity, as a tool for distribution according to ecosystem participation, and as a means of direct trading and asset accumulation. CLEBUS operates ClebusX as a trading system for generating revenue through NFTs, and is promoting expansion to the Metaverse platform with the goal of "Life to Earn" online. In addition, all trading systems on CLEBUS are transacted securely through a unique wallet provided by CLEBUS.

In preparation for the quantum computer era, NFTs and wallets are currently generated by ECC (elliptic curve cryptography) algorithms, but in the future, they will be generated and traded using quantum-resistant cryptographic algorithms, which are stronger cryptographic algorithms that cannot be cracked by quantum computers. NFTs and wallets with quantum-resistant cryptography are defined as Quantum NFTs and Quantum wallets in CLEBUS World. Currently, we are using TRC-20 tokens, but we are planning to create a Mainnet to expand the CLEBUS ecosystem. We also want to prepare for the era of quantum computers by creating a Quantum Mainnet that uses quantum-resistant cryptography.

In order to ensure that the value of CLE Token increases over time, we are preparing the following 3 things.

First, burn 10% of ongoing profits
• We want to burn 10% of the revenue generated from production, consumption, trading, authentication, NFTs, fees, etc. on CLEBUS World.
Second, the continued expansion of coin utilization areas
• We will continue to develop and integrate various platforms such as luxury, business, shopping, gaming, social media, conference, sports, certification, etc. platforms such as luxury, business, shopping, social media, conferences, sports, certification, etc.
Third, the transition from tokens to coins
• By developing the Quantum Mainnet and issuing it as a coin, we will not be dependent on a specific Mainnet, and we will expand the CLEBUS world by increasing the number of partners by discovering and incubating global businesses, talents, and technologies. We intend to expand the CLEBUS world by increasing the number of partners on the CLEBUS Mainnet by discovering and incubating global businesses, talents, and technologies.

2. Introduction

2-1. Information Age Problems

The problem with information being created and shared online, as seen through Cleco's eyes, is that it's not always as simple as it seems.

1) Lack of credibility of information
Even if it is based on the same ChatGPT, it can produce different results depending on what additional information is learned, and since it is possible to design prompts that can be learned through natural language, it has become an era where anyone without programming knowledge can create their own application (app) or chatbot. From another perspective, this means that the same chatGPT can give different answers depending on who created the chatbot, so it becomes important not to utilize a chatbot, but which chatbot is used. Therefore, it is necessary to verify the chatbot to ensure quality service and prevent inappropriate app activity.

In order to generate and share revenue similar to Apple's App Store or Google's Play Store, OpenAI operates a GPT store that has a verification process for the services sold. However, these AI apps or chatbots are not created exclusively through ChatGPT, and the competition in generative AI technology is fierce, and it is becoming possible to produce compliant performance at a lower cost. Therefore, verification or assurance is necessary for users to use the service with confidence.

In addition, AI is deeply involved in many areas of human life, improving efficiency and productivity in various tasks and providing convenience in daily life, making it impossible for AI to be completely excluded from human society. However, while AI is becoming important to all areas of human society, there is also a growing concern about the problems caused by AI's misjudgment. The main reason for the negative view of AI is its black-box nature, which makes it impossible for humans to understand the rationale behind an AI's incorrect decisions. Therefore, there is a need for a way to validate AI outputs in a way that humans can understand.

2) Volatility of information and lack of reward
This volatile information is exhausting for information providers and makes it difficult to separate the important from the less important. We need new ways to store information that is meant to be remembered and retained, and we need new ways to reward valuable and useful information, which is losing ground as expendable information seeks more revenue from advertising and fame. Moreover, platform companies have monopolized the distribution and exposure of important information and are taking all the revenue from it, so a new way of rewarding valuable information must be created.

3) Lack of security of cryptocurrencies when using quantum computers
Since the prime factorization problem or discrete logarithm problem, which was the foundation of public key-based algorithms, can be solved in polynomial time using quantum computers by the Shor algorithm, and the technology for developing quantum computers continues to improve, it is no longer possible to guarantee the security of encryption algorithms that apply them. Therefore, new public key-based algorithms that do not use the difficulty of prime factorization or discrete logarithm problems are required, and cryptocurrencies such as Bitcoin and Ethereum use the ECC (elliptic curve cryptography) algorithm, which is based on the difficulty of discrete logarithm problems and is not guaranteed to be secure when using quantum computers. Therefore, preparations must be made for this.

2-2. Solution

1) Tokenization of information (NFTs) and the virtuous cycle of reward and punishment
Cle coins embed value in information such as ideas, breaking news, business items, and intellectual property through tokenization.

In the Clever World, ephemeral information is contentified, serviced, and shared, and the value is preserved by turning that content into a permanent, immutable NFT. Once issued, NFT tokens are safe and secure within the CLEBUS World. NFTs can tokenize almost anything, and because blockchain technology ensures digital ownership and enables irreversible proof of transactions, they are commonly used to tokenize game items, real-world assets, art, luxury goods, collectibles, and more. Tokenization of specific items or characters in online mobile games, tokenization of specific assets such as real estate in virtual spaces or communities, tokenization of rare collectibles such as artwork or limited editions, and valuation and trading of tokenized NFT assets are underway. Financial, entertainment, and gaming companies are racing to continue investing in this space in anticipation of the growth of the NFT market and the various NFT-related innovative services that will emerge in the future.

NFTs have been used to tokenize knowledge and information, but now we want to tokenize any asset. The original providers of information should be rewarded for the reliability, efficiency, and usefulness of the content they create. Any user can issue NFTs for the content they have provided and verified, and they will be given the right to ownership and value creation in the form of NFTs, which can be valued and earned through token transactions. The acquired Cle coins and NFT tokens can be traded at any time through the exchange and can be freely transferred, exchanged, and held.

2) Validation and assurance of AI outputs using NFT and XAI technologies
In the case of B2B services, the authenticity of the chatbot itself was not important because it was supplied directly by the chatbot developer. However, it is difficult to commercialize when the general public is worried about malicious behavior such as phishing and malware, so verification of authenticity becomes an important factor when expanding to B2C.

NFTs can become an identity proofing tool for digital-being. Since not all platforms have the same credibility as OpenAI, CLEBUS aims to use NFTs, blockchain technology, and web 3.0 technology to verify and ensure the authenticity of generative AI outputs created by chatbots.

In addition, explainable Artificial Intelligence (XAI) has emerged to solve the problem of verification of AI outputs, and XAI technology that can analyze and understand the black box nature of AI and provide explanations is becoming very important. Explainable Artificial Intelligence (XAI) is to provide an explanation for the reasons for the learning outcomes of AI so that humans can understand them. Among the various approaches to ensuring the reliability of AI, XAI is particularly important because it can identify the causes of misjudgments and malfunctions of AI by presenting the process along with the reasons for making judgments. At CLEBUS World, we plan to add XAI technology and use it for AI authentication or verification of digital beings.

3) Securing quantum computing with quantum-resistant cryptographic algorithms
To ensure the safety of quantum computing, CLEBUS World plans to transform NFTs, Wallet, and Mainnet into Quantum NFTs, Quantum Wallet, and Quantum Mainnet using CRYSTALS-KABER and CRYSTALS-DILLISIUM, which were first adopted as standardized by the National Institute of Standards and Technology (NIST), and SAT-based quantum-resistant cryptographic algorithms, which CLEBUS World has the right to implement.

2-3. Meaning of CLEBUS

CLEBUS™ is a combination of CLÉ and Universe, where CLÉ means Key in French. To claim ownership of cryptocurrency, you need an account (account) and a password (private key) for the account. Since your account number is publicly available, your private key is your only online asset, hence Key is your online asset. CLEBUS is an online platform that pursues Life to Earn and serves as a stage for users to multiply their online assets. We are building the CLEBUS World so that all assets in the CLEBUS World can be traded using CLEBUS coins (CLE), and users with CLE can freely utilize all resources in the CLEBUS World to grow their assets.

2-4. The role of CLEBUS

CLEBUS already offers its own NFT certification services in a variety of sectors, including luxury automotive, golf, beauty, art, music, defense, and global NGOs. The various partners connected through NFT certification and their existing customers are also organically connecting with each other and creating synergies to evolve into an expanded ecosystem. In this way, CLEBUS is contributing to WEB2 → WEB3, and plans to provide an open market where various AI chatbots from around the world can certify and trade NFTs. CLE is a token used in the CLEBUS ecosystem, which is used as a gas fee to prove identity, as a tool for distribution according to ecosystem participation, and as a means of direct trading and asset accumulation.

The features of CLEBUS are summarized as follows.
1) Transition from WEB2 → WEB3)
2) Identifier of digital beings utilizing blockchain technology-based NFTs
3) Verification, authentication, and guarantee of various chatbots created through generative AI platforms such as OpenAI's GPT through CLEBUS's own NFTs

2-5. Goals of CLEBUS

With the vision of "contributing to humanity by providing a sustainable hyper-connected ecosystem", we are trying to build a sustainable WEB3 ecosystem through WEB2 → WEB3 transition and identification of digital beings using NFTs based on blockchain technology.

In particular, various chatbots created through generative AI platforms, such as Open AI's GPT, are verified, certified, and guaranteed through CLEBUS's own NFTs.

Through CLEBUS, anyone in the world can certify their creations, products, services, and various resources and assets as NFTs to be commoditized and traded to generate revenue, and we intend to provide an ecosystem where global users who use it can also participate and consume as prosumers (producers and consumers) and enjoy Life To Earn.

We also want to prepare for the era of quantum computers by applying quantum-resistant cryptographic algorithms to convert NFTs, wallets, and Mainnet into Quantum NFTs, Quantum wallets, and Quantum Mainnet.

3. CLEBUS World

3-1. CLEBUS™

The CLEBUS ecosystem aims to facilitate the transition from Web 2 to Web 3 by providing a sustainable, interconnected ecosystem, using blockchain and NFTs to implement digital identity authentication and validate and guarantee generative AI such as chatbots with proprietary NFTs. Through CLEBUS, users can monetize their creations or services by authenticating and trading them as NFTs, and anyone in the world can participate in the ecosystem as a producer and consumer. CLEBUS also provides NFT authentication services in various fields such as automotive, golf, and beauty, and uses the CLE token to support identity authentication, trading, asset accumulation, and more within the ecosystem.

3-2. AI + Certification

We plan to develop an algorithm that can detect deep fakes by learning to extract facial features from real and fake images in a neural network composed of a combination of convolutional layers (CNN) and pooling layers, and embed it in the CLEBUS World. CNN is expected to continue to be actively utilized in artificial intelligence deep fake detection because it can improve deep fake detection performance step by step with other types of deep learning models such as recurrent neural networks (RNN) and long short-term memory (LSTM), and because it is currently showing excellent performance in music recognition and natural language processing in addition to image processing. The fields that use CNN are summarized below.
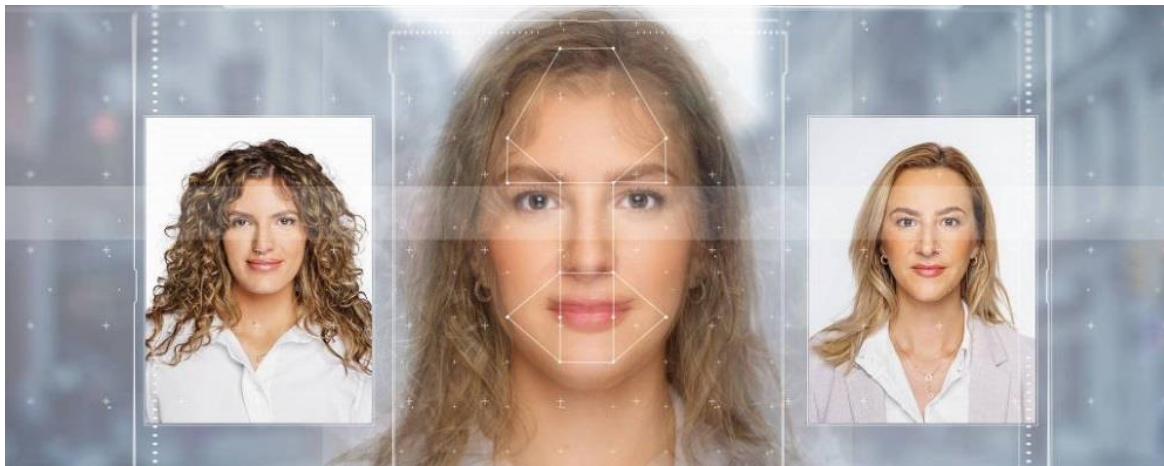
Digital AI content and services whose authenticity is difficult to verify can be protected from user harm with NFTs. CLEBUS ensures the originality and quality of AI services and prevents the side effects of deepfake technology. The above technology can be used in the following areas

-AI financial services certificates
-Ensuring content originality
-Preventing misrepresentation using deepfake technology

3-3. CLEBUS NFT

Lifestyle NFTs are the first blockchain life service on CLEBUS. NFTs can be used to immortalize important events and can be gifted, distributed, or sold to those who need them.

CLEBUS NFTs are TRC 721 compliant, offering low fees, fast transfer speeds, and high scalability.

Limited availability NFT	Event type NFT	Right NFT
NFTs can be used to issue new car vouchers, memberships, event tickets, etc. and sell or VIP services.	Promotional items or new product launches can be distributed and given away as NFTs.	NFTs are used as a proof of ownership, intellectual property rights, copyrights, etc. of works to guarantee the rights of the owner and transfer the rights to the buyer.

3-6. CLEBUS META

With the goal of Life to Earn, CLEBUS World aims to create a Metaverse platform in the following four areas to provide a base for users to share with each other and increase their crypto assets.

First, B2E (Business to Earn)
• Businesses and individuals can join the CLEBUS platform and utilize the CLEBUS community to pursue various businesses.

Second, C2E (Convention to Earn)
• C2E provides a platform for MICE within the CLEBUS platform

Third, P2E (Play to Earn)
• The CLEBUS platform can discover and store various games to generate revenue through games.

Fourth, S2E (Social life to Earn)
• The CLEBUS platform supports SNS and helps you earn money through second-hand transactions and meetings.

4. Technology in the CLEBUS World

4-1. CLEBUS Blockchain

Bitcoin, best known for its blockchain technology, is based on the Proof of Work (POW) consensus algorithm, which uses a hash operation to change the value of a nonce, creating a block when a number less than the hash value is found.

Bitcoin's networked method, known as mining, is computed using GPUs that are capable of many operations. This method of mining is becoming increasingly problematic due to its resource consumption and environmental issues. It also requires a large initial capital investment, and mining profits gradually decrease as Bitcoin's mining halving period passes.

The Bitcoin blockchain platform using the Mainnet supports only simple deposit and withdrawal functions, so it is not easy to introduce it to various services. By compensating for these technological and service shortcomings, Tron was born with smart contracts that can be used in various services, and Tron complements the existing algorithm and activates DAPPs at the same time. Tron has the following features

1) Platforms with built-in digital assets and payment methods
2) A network environment where users are sovereign over their data and applications do not steal their unique data.
3) Online services that allow anyone to access an open financial system
4) A blockchain platform with a neutral and open infrastructure that is not controlled by a specific company or individual.

The digital asset Troncoin (TRX) has many of the same features as Bitcoin. It's fully digitized and can be sent instantly to anyone, anywhere. And like Bitcoin, the supply of TRX is not controlled by any government or company, meaning it's decentralized.

People around the world are using this decentralization to make payments, store value, or use it as collateral. But unlike other blockchains, TRON can do more. Because TRON is programmable, developers can use it to build new kinds of applications.

4-2. CLEBUS network layer
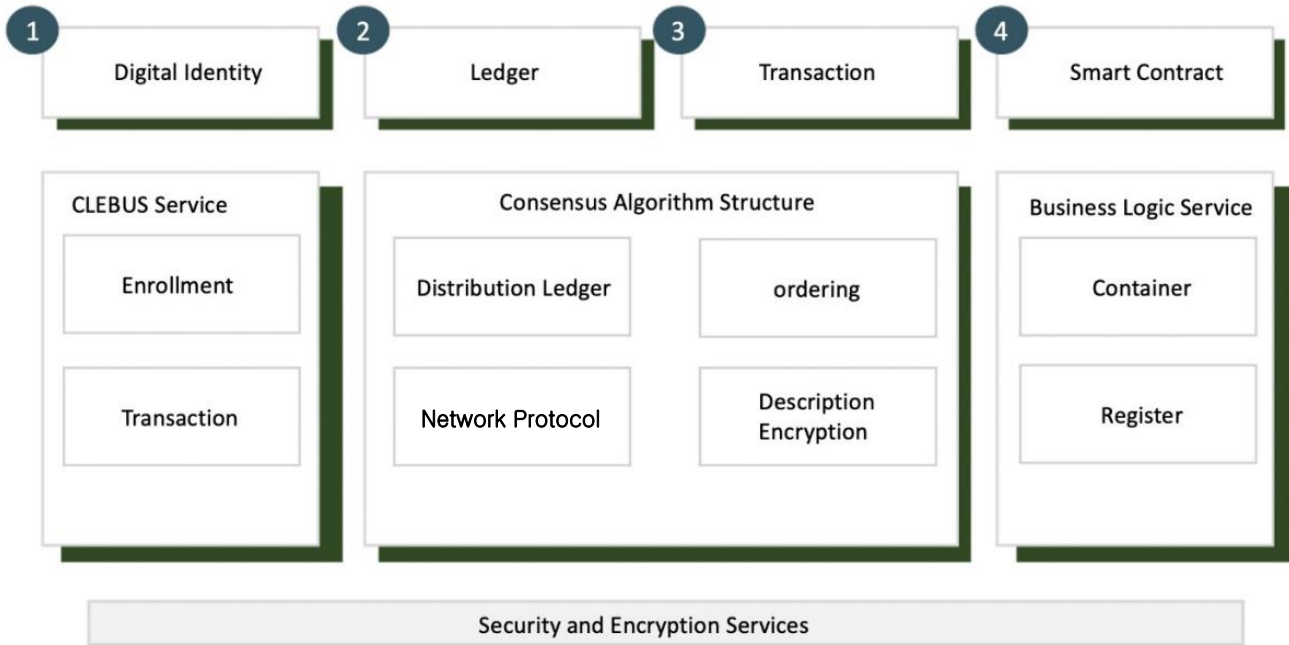
① Identity verification layer for securing CLEBUS data. DID authentication of users is mandatory for transactions in CLEBUS. Participants store relevant data in the distributed ledger for recording, modifying, and deleting, and provide functions for issuing related certificates.

② A blockchain data ledger. The CLEBUS distributed ledger is an integrated application structure of the TRON chain, which is a database that manages data for storage as a basic component of the blockchain. The structure of Ledger consists of functions to manage and process it.

③ Component and transaction information layer. As a layer that manages transactions generated from blockchain service processing, there is a distributed ledger service that processes 'Endorsement Validation' in batches to process transactions and generates blocks to branch to all nodes participating in the blockchain network.

④ Smart Contract component layer. Smart contracts are an important feature of the blockchain, implementing logic to utilize the blockchain for services organized in a consortium. Smart contracts are basically supported in various languages so that logic can be developed.
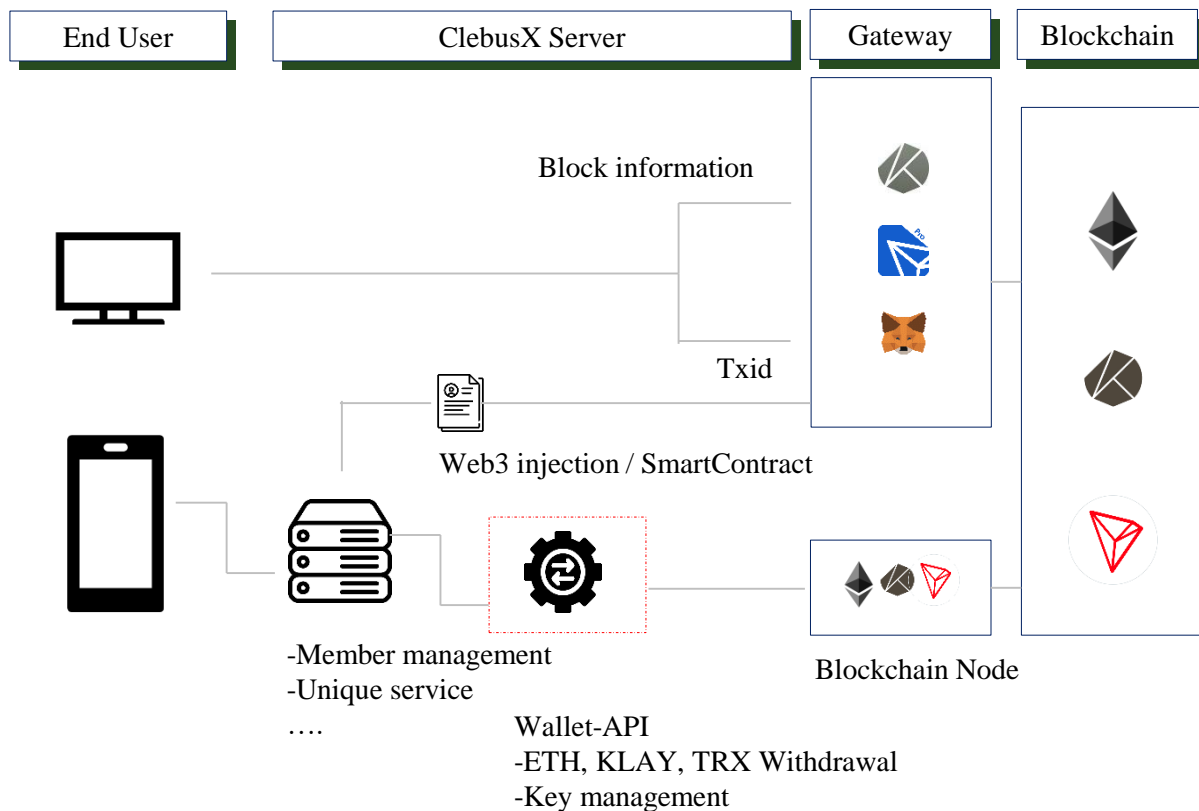
4-3. Clebus-X system

The key points of ClebusX's system to support peer-to-peer trading and NFT marketplaces include

1) Deposit and withdrawal support and asset custody for hybrid systems
2) System security
3) NFT-related technologies

In ClebusX's system, the deposit of virtual assets is done through the integration of personal wallets (Dapps) such as MetaMask, Kaikas, and Tronlink. Through Web3 injection, the assets held in the personal wallet are transferred to the wallet of the ClebusX system. The crypto assets deposited through the wallet are moved to the storage wallet where the main system manages the keys. The transferred virtual assets are used as a medium for exchange and trading. The main system includes a P2P trading engine, SWAP, Staking, and other unique service engines.

When withdrawing, the assets in the custodial wallet are withdrawn to the respective personal wallet (Dapp) or to the desired input address.

ClebusX's system allows NFTs to be published. The original source of the published content is stored in the IPFS (Inter Planetary File System) decentralized filesystem. NFTs are issued through ClebusX's internal management wallet, and the assets in the exchange wallet of the copyright holder who requested the issuance are deducted for gas. The issued NFT edition is created in the copyright holder's Collection, and the right to sell it belongs to the copyright holder.

In addition, the ClebusX NFT market can be used. However, the issuer's information recorded on the blockchain is provided by ClebusX. The management system for this will be updated in the future so that NFTs can be issued by accessing the copyright holder's personal wallet on the on-chain.

System security is divided into firewall policies and network security. Firewalls are the most basic and essential element of systems and networks. A proper firewall policy not only adds a layer of security to your system and production network, but can also block much of the illegal access. It also provides a deeper system configuration for security and access, leveraging virtual private networks (VPNs) to authenticate and level internal access.

While software firewalls exist in various forms on the market, ClebusX's entire platform is based on the OS's own firewall. Hardware firewalls provide the flexibility to operate firewall ports on switch equipment installed in the system and network, and introduce additional operating system features such as access control lists (ACLs) to improve the ease of platform management.

Internal security management with VPN, All system administrators and operators access servers and systems using unique VPN accounts assigned to them. This ensures that in the event of a security issue, you can see who accessed the system and from what path, and take immediate action.

Countering Web or Structured Query Language (SQL) Injection Attacks ClebusX is divided into a blockchain-based distributed processing platform and a P2P, NFT trading platform. The basic attacks that are widely known against these structures are DB (datebase) Injection attacks using web and SQL. To defend against them, we have a program development, setting, and maintenance policy within a limited scope.
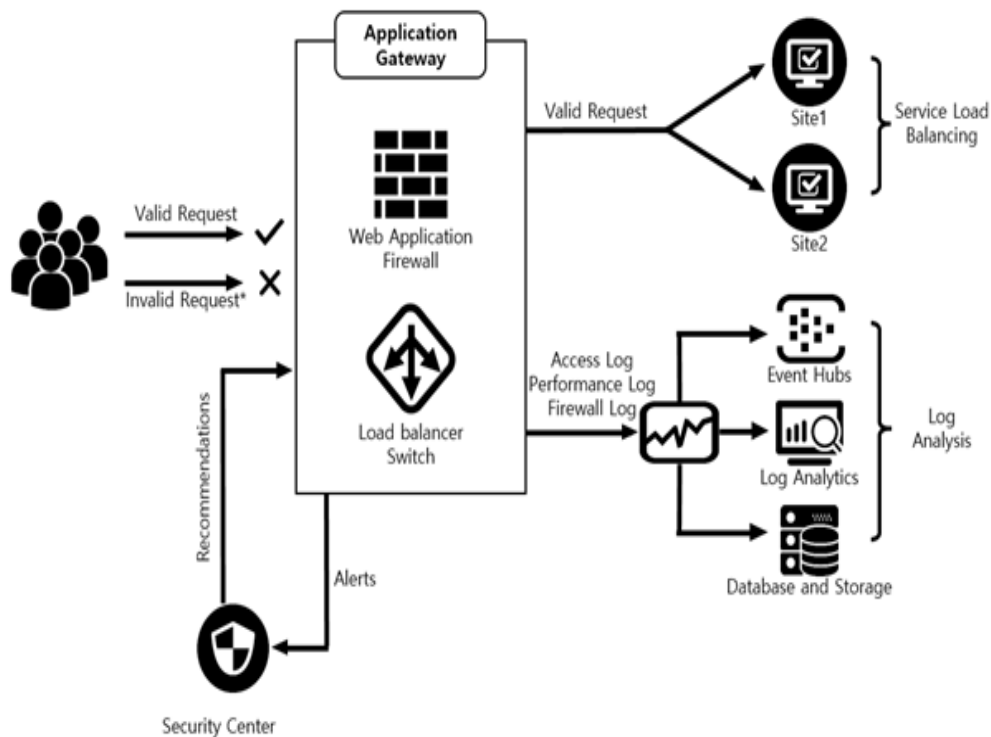
Invalid requests are usually blocked as soon as they are detected, while valid traffic (Valid Requests) is appropriately distributed and managed on internal web servers to serve users. In the event of an issue with ClebusX's control system (Application Gateway), the Security Center suggests issues for checking. Once the suggestions are delivered, internal security experts analyze the logs loaded into the control system and track events to detect security issues and respond according to policy.

5. Expansion

5-1. Switching from a personal wallet to a DEX wallet

When you register on the Clecoin.io site, an online wallet is created.

While online wallets are convenient to use, they are weak in terms of security. To overcome this shortcoming, we are planning to switch to a DEX-type wallet that can work with hardware wallets and support various Mainnets to exchange and manage coins and tokens without third-party intervention.

We aim to create a wallet for CLEBUS World that can store and exchange all cryptocurrencies used in CLEBUS World.

5-2. Token to Coin Conversion

Currently, CLE is created as a TRC-20-based token. While it has the advantage of providing various smart contracts and NFTs with low gas costs, we believe that it is necessary to have its own Mainnet for various online payments in the CLEBUS World that we want to pursue.
Therefore, we are planning to develop a new Mainnet for CLEBUS World.

At the time of updating this whitepaper, we are planning in two directions: forking an open-source Mainnet such as Bitcoin or Ethereum to create a new Mainnet, or designing our own protocol to create a completely new Mainnet.

6. Go to Quantum

6-1. The need for quantum-resistant cryptographic algorithms

Since the prime factorization problem or discrete logarithm problem, which was the foundation of domestic and foreign IT public key-based algorithms, can be solved in polynomial time using quantum computers by the Shor algorithm, and the technology for developing quantum computers continues to advance, the security of encryption algorithms applied to them cannot be guaranteed. Therefore, new public key-based algorithms that do not use the difficulty of prime factorization or discrete logarithm problems are required, and such cryptographic technology is called quantum-resistant cryptography or post-quantum cryptography (PQC).

Quantum-resistant cryptographic algorithms are being researched in five areas: hash-based, multivariable-based, code-based, isogeny-based, and lattice-based. Hash-based algorithms are one-way encryption and are mainly used for electronic signatures. Isogeny-based algorithms are slow to compute, and multivariable-based algorithms have a high decryption failure rate. Therefore, lattice-based or code-based algorithms are mainly used in the field of public key encryption (PKE).

Recently, the National Institute of Standards and Technology (NIST) is standardizing post-quantum cryptographic algorithms, and in the third round of PKE, three lattice-based algorithms (CRYSTALS KYBER, NTRU, and SABER) and one code-based algorithm (Classic McEliece) were finally selected.
Lattice-based cryptographic algorithms have the disadvantage that it is difficult to set variables and are vulnerable to side-channel attacks using additional information such as power, electromagnetic waves, time difference, and error injection generated during encryption and decryption, and in the case of code-based algorithms, the Information Set Decoding (ISD) technique has been steadily researched as a way to recover the original data without finding the private key.

In addition to the quantum-resistant cryptographic algorithms described above, most public-key-based cryptographic algorithms currently in use or being researched have a trapdoor one-way function, which is a relationship expressed as a formula between the public and private keys, and attacks are constantly attempting to find vulnerabilities in the algorithm based on the relationship to obtain the private key or original data, or to make decryption impossible.

To date, most cryptocurrencies, including Bitcoin and Ethereum, use the ECC (elliptic curve cryptography) algorithm. However, the ECC algorithm is based on the difficulty of discrete algebra problems, so it is necessary to prepare before quantum computers with thousands of qubits are built. Recently, Ethereum developers have also begun working to prepare for quantum computers.

Public-key cryptographic algorithms are built on NP-hard problems, or problems that are predicted to be NP-hard. Not only is SAT the first proven NP-complete (NP-hard & $\in$ NP) problem, but if the CNFs that make up SAT can be used as public keys, there is no arithmetic relationship between the private and public keys, making it immune to various algebraic attacks that attempt to find the private key from the public key.

Recently, new quantum-resistant algorithms using SAT have been researched, and we have the right to practice patents related to SAT-based quantum-resistant cryptographic algorithms under a license agreement. Using SAT-based algorithms and CRYSTALS-KABER and CRYSTALS-DILITHIUM, which were first adopted by NIST as standardization targets, we intend to transform NFT, Wallet, and Mainnet into Quantum NFT, Quantum Wallet, and Quantum Mainnet.

6-2. Quantum NFT

CLEBUS World has already developed and operates a system that enables NFTs to be issued and traded through ClebusX.

All current NFT issuance systems, including ClebusX, store data in a specific area of the server called a URL and store the URL on the blockchain to permanently record the ownership of the URL. Every time a transaction is made, the transaction history changes and the owner of the URL changes.

However, because the data source is still stored in the URL, anyone can access the URL, download the data, and copy it.

This can be described as insecure ownership, because the URL is unique, but the asset it contains can be copied in multiple copies once it leaves the URL. That's why we want to adopt a structure where the source of the data is encrypted and the data that is visible to the public for transactions is dithered or text-marked.

We plan to implement Quantum NFTs using a quantum-resistant algorithm as the cryptographic algorithm.

The block diagram below shows how the encrypted original is restored to the previous owner's private key when it changes hands, and re-encrypted and stored with the new owner's public key.
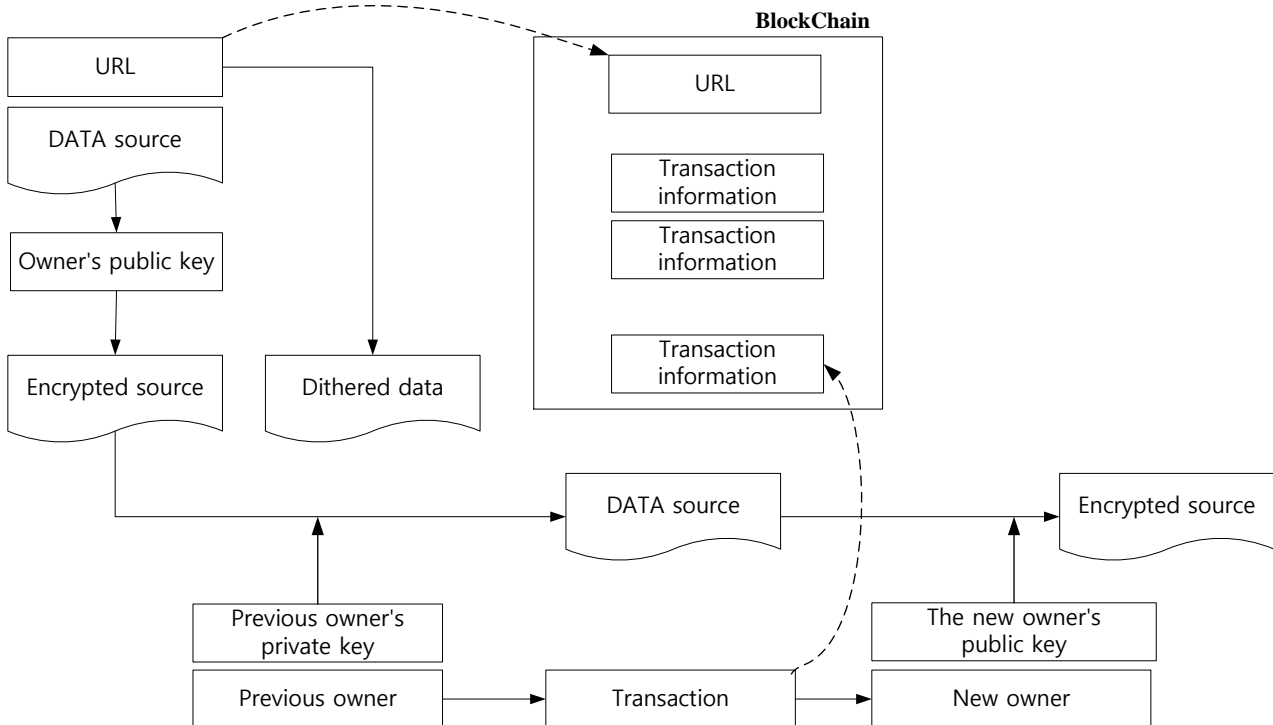
6-3. Quantum Wallet

To extend a wallet to a DEX wallet, we need a system to exchange coins through the wallet.

Since the account of the wallet containing the coins is public, the password of the account becomes the coin asset we own. In order to prevent the password from being stored in memory as raw data at any point during the process of handing over this asset to the other party, we want to encrypt the password with a quantum-resistant cryptographic algorithm.

We plan to use a quantum-resistant cryptographic algorithm as the encryption algorithm.

We have encryption and decryption technology using CRYSTALS-KABER, which was recently selected as the first NIST standardization target, and we also have the right to implement SAT-based cryptographic algorithm implementation technology, which is the mother of NP-Problem.

Cryptographic algorithms are divided into PKE (Public Key Encryption) and DS (Digital Signature).

So far, cryptocurrencies only use DS, which means that when a coin is signed by the holder, the nodes check the authenticity of the signature, and if they determine that it is a valid transaction, they send it to their peer nodes, and the nodes put the transaction in the MemPool (Memory Pool).

When implementing a wallet with DEX functionality, we need not only a signature algorithm but also a cryptographic (PKE) algorithm to encrypt passwords.

We plan to use SAT and CRYSTALS-KYBER as quantum-resistant encryption algorithms and CRYSTALS-DILITHIUM as a signature algorithm.

Some coins have been created that use FALCON-512 as a quantum-resistant signature algorithm, but we want to use the CRYSTALS-DILITHIUM signature algorithm instead. We want to use the CRYSTALS-DILITHIUM signature algorithm rather than FALCON-512 as the signature algorithm because it is easier to manage the code than the FALCON signature method because it partially uses CRYSTALS-KABER as a quantum-resistant cryptographic algorithm.

Also, since CRYSTALS-KABER is currently the only PKE selected by NIST, both FALCON and CRYSTALS-DILITHIUM are currently standardized, but I predict that in the future, CRYSTALS-DILITHIUM will be used more, as in my implementation.

6-4. Quantum MainNet

Bitcoin has four drawbacks, as described below.

The first is that the size of the ledger is constantly increasing by storing all transactions continuously, making it impermanent.

The second is that the number of nodes is reduced by storing the entire ledger instead of dividing it among all the nodes, which defeats the purpose of decentralization and leads to centralization.

The third is that it consumes a lot of computing power by performing iterative operations to find a nonce with a hash value within a certain number to create a block that stores transactions.

Finally, the use of elliptic curve cryptography makes it resistant to quantum computers.

To solve the first problem with Bitcoin, we have a long-term plan to move away from the traditional method of creating blocks of transactions and cascading hash values, and instead create blocks from a chain of accounts, where each account constitutes a chain, and each block is created from a chain of accounts.

In addition, just like deleting old transactions from a bank account, a balance is recorded so that old chains can be deleted when the length of the chain grows beyond a certain value, so that the size of the block does not increase beyond a certain number even if transactions continue to occur.

To solve the second problem, we have a long-term plan to introduce a sharding technique where nodes divide the ledger into new connections between new nodes, instead of the existing method where all nodes store the same blockchain. Therefore, the proposed algorithm assigns shard numbers to all blocks so that a node stores only one shard.

To solve the third problem, we want to abandon the race to find a nonce value that makes all nodes have a hash value below a certain number and adopt a method where only one node updates the block like a centralized system, but the node that updates is randomly selected to make it impossible to tamper or collude.

To solve the fourth problem, we want to use a quantum-resistant algorithm. The elliptic curve cryptography (ECC) algorithm used by Bitcoin and Ethereum is based on the difficulty of solving discrete algebraic problems.
However, since the Shore algorithm, published in 1994, proved that discrete algebraic problems can be solved by quantum computers in polynomial time, it becomes unusable at some point when the number of qubits processed by quantum computers increases.

To solve this problem, we plan to use the CRISTALS-DILLISIUM signature algorithm and CRYSTAL-KABER encryption algorithm, which were first adopted as standardized by NIST as quantum-resistant algorithms that cannot be solved in polynomial time even by quantum computers.
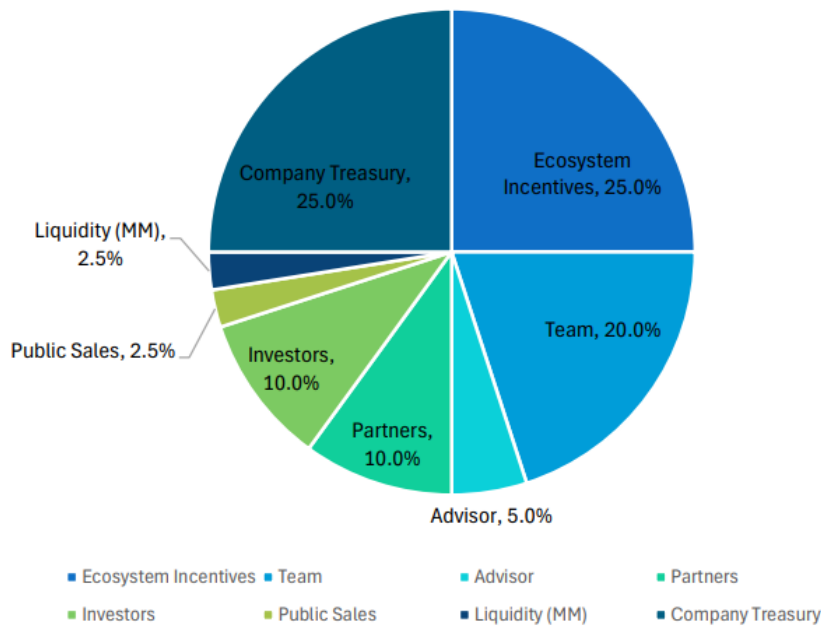
7. CLE

7-1. CLE 분포

Token Name	CLE COIN TOKEN (CLE)
Algorithm	TRC-20
Decinals	6
Total Token Supply	10,000,000,000 CLE

Currently, we have issued 10 billion TRC-20 tokens and aim to distribute the issued CLE tokens as shown in the chart below.

(1) Partners : Provide to alliance partners.
(2) Investors : Provide to investment firms.
(3) Public Sales : Used to promote airdrops or CLEs.
(4) Liquidity : Used to secure liquidity.
(5) Company Treasury : It's held by the Foundation.
(6) Adivisors: CLEBUS PROJECT To be paid to the CLEBUS Foundation's Advisors participating in the CLEBUS Project.
(7) Team: Provide to CLEBUS PROJECT team members.
(8) Ecosystem Incentives : Use for distribution coordination and ecosystem.

7-2. Burn plan

We're looking to do three things to continue to increase the value of our CLEs.

1. burning or permanently locking up CLE coins equal to 10% of CLEBUS revenue each year until 2035.
2. Continuous expansion of CLE usage through global expansion.
3. Provide various benefits and rewards for CLE holders.

7-3. Personal wallet for CLE storage

By registering an account on the clecoin.io site, users can use the online wallet created by CLEBUS World for storing and managing CLE tokens. After registering an account, the user will receive a private wallet and a private key to access the wallet through an authentication process.

By utilizing this private wallet, users can perform various activities within the CLE wallet platform.

First, they can freely transfer CLE from their personal wallet to external or other people's wallets without any fees if they are not CLE Force Up. Since CLE utilizes the TRX blockchain, there are no fees for individual transactions, including deposits and withdrawals.

Second, you can purchase CLE through an external exchange, transfer it to your personal wallet, and then force up CLE.

Finally, CLE in your personal wallet can be transferred to external exchanges at any time, and you can earn CLE through attendance checks and various other events.

8. CLEBUS Roadmap

2021
- 3Q CLE issuance, e-wallet development

2022
- 1Q CLEBUS Homepage OPEN
- 1Q Listing on CLE Crypto Exchange (LBANK)
- 1Q KPGA Korean Tour "CLEBUS OPEN" Golf Tournament Signing Ceremony
- 2Q Mercedes-Benz Korea Authorized Dealer H provides NFT authentication service
- 3Q CLEBUS-X (P2P crypto exchange, NFT marketplace) Beta Opened
- 4Q Other luxury brand NFT services

2023
- 1Q CLEBUS-X (P2P crypto exchange, NFT market) Beta 2.0 is now live
- 2Q Mercedes-Benz Korea Authorized Dealer H Expands NFT Membership Service
- 3Q Global NGO to offer luxury beauty/fashion NFT certification service
- 4Q BOTHORI & SLEEPPO Car Body NFT Collection Planning and Development

2024
- 1Q Introducing smart NFT technology to control cars
- 1Q CLEBUS AI chatbot authentication sample version 1.0.1 released
- 2Q Announcing CLE White Paper 2.0
- 3Q CLE 2nd Cryptocurrency Exchange Listing Plan
- 3Q AI+ Certification Beta Open
- 4Q Quantum (NFT / DEX Wallet / Mainnet) Planning

2025~
- Ai, Digital Beings + NFT Certification Platform Planning/Development
- Planning and development of Quantum NFTs, Quantum DEX wallets, and Quantum Mainnet
- CLEBUS World Planning/Development
- Listed on multiple global exchanges
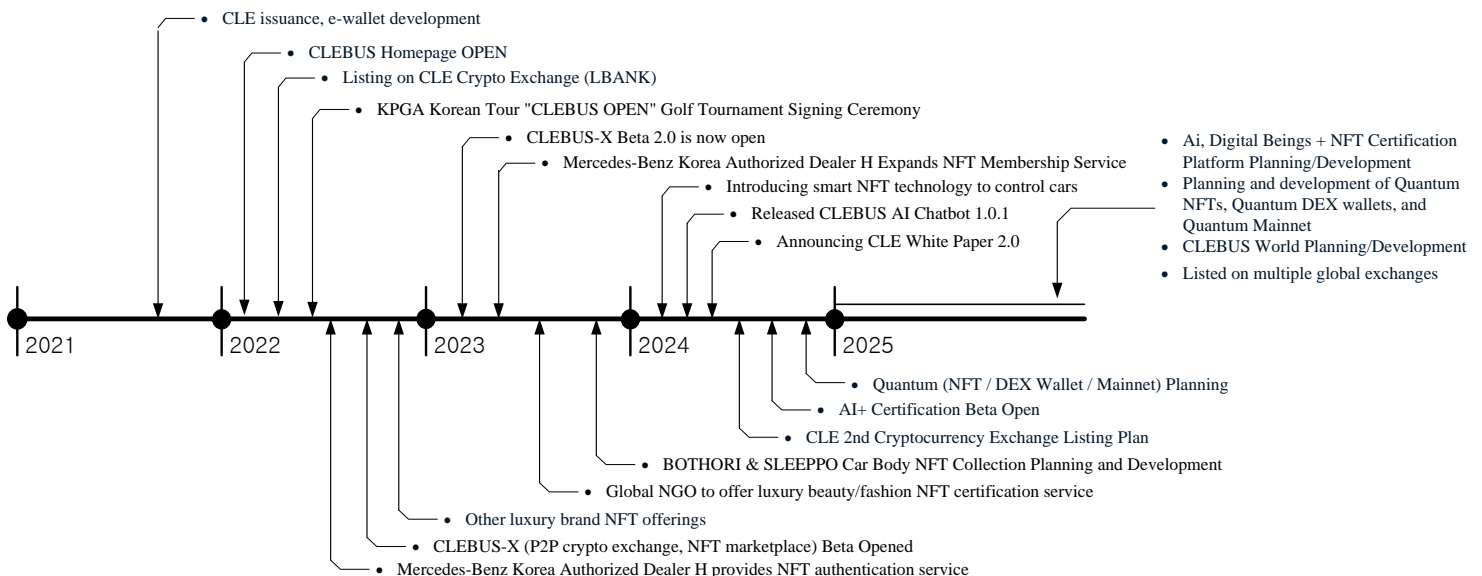
9. Legal notices

Please read everything in this Legal Notice and Disclaimer carefully. If you are in any doubt about your future actions, we recommend that you seek the opinion of a legal, financial, tax, or other professional.

1. Legal notices

① This white paper is distributed for general reference purposes only in connection with the CLEBUS project as of the time of writing and is subject to review and revision. Please note that this white paper reflects the latest information as of the date on the cover and is not final. After that date, the information contained herein, including CLEBUS token business operations and financial status, may change. This whitepaper may be updated from time to time.

② No one is obligated to enter into any contract or legally binding commitment in connection with the purchase or sale of CLEBUS TOKEN, and no funds should be solicited based on this white paper. The purchase and sale of CLEBUS TOKEN will be conducted through the CLEBUS Platform, the details of which will be announced separately from this Whitepaper.

③ This white paper should not be construed as an offer to sell or purchase tokens from the issuer/distributor/company of CLEBUS tokens under any circumstances, and neither the presentation of this document nor the document itself should be relied upon or formed the basis of any contract or investment decision.

④ The CLEBUS tokens are not intended to constitute securities, units of a business trust, or units of a collective investment scheme, each of which have the respective definitions set forth in the equivalent regulations of the jurisdiction in which they are incorporated. Accordingly, this white paper is not offered as a business plan, prospectus, offer or otherwise and should not be construed as an offer or solicitation of an investment in securities, units of a business trust, or units of a collective investment scheme in any jurisdiction.

⑤ The CLEBUS tokens should not be understood, interpreted, categorized or treated as an opportunity for purchasers to participate in the CLEBUS service or to receive any investment income/revenue/payment/profit or any part thereof.

⑥ This document may not be reproduced, distributed or otherwise disseminated, in whole or in part, in any jurisdiction where the token issuance method described in this whitepaper is regulated or prohibited.

⑦ If you wish to purchase CLEBUS tokens, you must not understand, interpret, categorize, or treat CLEBUS tokens as (1) any currency other than cryptocurrency; (2) bonds and stocks issued by any entity; (3) rights, options, or derivatives on such bonds and stocks; (4) rights under contracts for difference and other contracts that purport to be or are designed to guarantee a return on investment or avoid losses; or (5) units or derivatives of securities, including collective investment schemes and business trusts.

2. Limitations on distribution and propagation

① The distribution or dissemination of this White Paper, in whole or in part, may be prohibited or restricted by law or regulatory requirements in any jurisdiction. If restrictions apply, you should inform yourself of any restrictions that may apply to your possession of this White Paper, seek legal advice, and comply with such restrictions, and the Foundation and its officers, employees, agents, affiliates, and others (hereinafter referred to as "Affiliates") operating the CLEBUS Project shall not be liable for any such restrictions.

② If you have access to or possession of this white paper as a result of its distribution and dissemination, you must not distribute, reproduce, or otherwise share this white paper or its contents with others for any purpose, or allow or cause such a situation to occur.

2. Exclusion of liability

① The CLEBUS Foundation and related services provided by the CLEBUS Foundation and its affiliates are provided on an "as is" and "as available" basis. The CLEBUS Foundation and its affiliates make no express or implied warranties or representations as to the accessibility, quality, suitability, accuracy, adequacy, or completeness of the CLEBUS Token and related services, and shall not be liable for any errors, delays, omissions, or actions taken in reliance thereon.

② The CLEBUS Foundation and its affiliates do not describe, guarantee, promise, or represent to any entity or person the authenticity, accuracy, or completeness of any information, including the information contained in this white paper, in any form.

③ CLEBUS Foundation and its affiliates shall not be liable in contract or tort for any indirect, special, incidental or consequential losses (including, without limitation, loss of investment returns/revenue/profits, loss of use or data) arising out of or in connection with your acceptance of or reliance on this white paper in whole or in part, and this applies to the fullest extent permitted by applicable laws and regulations.

4. Cautionary statements about forward-looking statements

① Certain statements in this whitepaper contain forward-looking statements about the future of the project, future events, prospects, etc. These statements are not statements of historical fact and are identified by words such as "intend," "estimate," "believe," "expect," "outlook," "project," "anticipate," and similar expressions. In addition to this white paper, other public materials, such as presentations, interviews and videos, may also contain such forward-looking statements. Forward-looking statements contained in this white paper include, but are not limited to, statements regarding the future results, performance, and achievements of CLEBUS Foundation and its affiliates.

② Forward-looking statements involve various risks and uncertainties. These statements are not guarantees of future performance and should not be unduly relied upon. If risks and uncertainties materialize, the actual performance and development of CLEBUS Foundation and its affiliates may differ from the expectations set forth in the forward-looking statements. Even if these circumstances change in the future, CLEBUS Foundation and its affiliates do not undertake any obligation to provide updates to forward-looking statements. If you act on any forward-looking statements contained in this white paper, CLEBUS Foundation's and its affiliates' websites and other materials, you do so at your own risk that the forward-looking statements do not materialize.

③ As of the date of this white paper, the CLEBUS Project is not complete or fully operational. Although the description is based on the premise that the CLEBUS Project will be complete and fully operational in the future, it should not be construed as a guarantee or promise that the CLEBUS Project will be complete and fully operational.

5. Potential risks

① We recommend that you read the following carefully and fully analyze and understand the relevant factors and risks before deciding to purchase and participate in CLEBUS tokens. Risks include, but are not limited to: (i) storage-related buyer negligence risks, such as loss of identifying information resulting in restricted access to CLEBUS Tokens and loss of essential private keys associated with digital wallets holding CLEBUS Tokens; and (ii) risk of fluctuations in the value of CLEBUS Tokens after issuance due to global market and economic conditions. The CLEBUS Foundation may not be able to fund the development of the CLEBUS Token ecosystem or use the CLEBUS Token in the intended direction due to this uncertainty in the value of the CLEBUS Token; and (iii) risks related to changes in the political, social, and economic environment, changes in the equity or cryptocurrency market environment, changes in the regulatory environment in the countries in which the CLEBUS Foundation and its affiliates operate, and changes in the ability of the CLEBUS Foundation and its affiliates to survive or compete in such environments. Certain jurisdictions may apply existing or new regulations related to blockchain technology that are unfavorable to the CLEBUS token, which may result in significant changes to the CLEBUS token ecosystem and the project, including the abolition/loss of the CLEBUS token.

② Risks related to changes in the future capital needs of the CLEBUS Foundation and its affiliates and the availability of capital and financing to meet them. Lack of funding may affect the development of the CLEBUS platform and the use and potential value of the CLEBUS token.

③ Various reasons, including unfavorable fluctuations in the value of the CLEBUS token, failure of business relationships, and claims of intellectual property rights by competitors during development and operation, may lead to the suspension, dismantling, or discontinuation of the CLEBUS project or launch plans, which may adversely affect the CLEBUS token ecosystem, the CLEBUS token, and the potential utilization of the CLEBUS token.

④ Risks related to the lack of interest from companies, individuals and other organizations in the CLEBUS project and services, and limited public interest in the creation and development of deployed applications. This lack of interest may limit financing or affect the development of the CLEBUS Project and the utilization and potential value of the CLEBUS Token.

⑤ The risk of making significant changes to the CLEBUS Token or to the key features and specifications of the CLEBUS Project and the CLEBUS Token ecosystem prior to launching or implementing the CLEBUS Project. While CLEBUS intends for the CLEBUS Token and CLEBUS features to be consistent with the content of this whitepaper, such changes may nevertheless be made. The risk of competition from other platforms that could potentially adversely affect the CLEBUS token and the CLEBUS platform (e.g., if competing projects are not commercially successful or have poor prospects).

⑥ The risk that third parties or other individuals intentionally or unintentionally plant harmful and malicious code in the CLEBUS Project to interfere with the CLEBUS Project infrastructure and the utilization of CLEBUS tokens. The blockchain used in the CLEBUS Project is also vulnerable to such attacks, which poses a risk to the operation of the CLEBUS Project and related services.

⑦ Force Majeure The occurrence of catastrophic events, such as natural disasters, may affect the business operations of the CLEBUS Foundation and its affiliates and other factors beyond their control. Events such as mining attacks, attacks by hackers or other individuals may result in the theft and loss of CLEBUS token sale proceeds, theft and loss of CLEBUS tokens, and impairment of the ability to develop the CLEBUS token ecosystem.

⑧ The CLEBUS token and other cryptocurrencies are new, unproven technologies and are constantly evolving. As technology evolves, advances in cryptographic technologies and methods, changes in consensus protocols and algorithms, etc. may pose risks to the CLEBUS Token, the sale of the CLEBUS Token, the CLEBUS Project, the CLEBUS Token ecosystem, and the utilization of the CLEBUS Token.

⑨ CLEBUS tokens do not grant any decision-making rights to any other entity with respect to the CLEBUS project, the CLEBUS ecosystem, etc. All decisions, including discontinuation of CLEBUS products and services, the CLEBUS token ecosystem, further creation and sale of CLEBUS tokens utilized in the CLEBUS token ecosystem, sale and liquidation of CLEBUS, etc. are made at the sole discretion of CLEBUS PLATFORM. (xiii) The tax and accounting treatment of CLEBUS tokens is uncertain and may vary from jurisdiction to jurisdiction. The tax treatment of your purchase of CLEBUS Tokens may be adversely affected and you are advised to seek independent tax advice in this regard. In addition to the risks described above, there are other risks that the CLEBUS Foundation and its affiliates cannot predict, and unforeseen combinations and variations of these risks may also emerge.

⑩ If any of the above risks and uncertainties develop into actual events, the business, financial condition, results of operations and prospects of CLEBUS Foundation and its affiliates could be materially and adversely affected. As a result, you may lose some or all of the value of your CLEBUS tokens.

6. No additional information and updates

No one is authorized to provide any information/statements about the CLEBUS Foundation and its affiliates, and their related businesses and operations, other than those contained in this white paper, and such information/statements, if provided, should not be relied upon as authorized by or on behalf of the CLEBUS Foundation or its affiliates.

7. No advisory

None of the information in this whitepaper constitutes business, legal, financial, or tax advice about the CLEBUS token, the CLEBUS Foundation, or its affiliates. You are encouraged to seek the opinion of your own legal, financial, tax, or other professional advisors regarding the CLEBUS token, the CLEBUS Foundation and its affiliates, and their related businesses and operations. The financial risks of purchasing CLEBUS tokens may apply indefinitely.