ETERNAL LIFE COIN

Decentralized Web3 Healthcare Project with

Global Healthcare Providers and Cosmos3

2024 Whitepaper

ELC Organization

Web3 DeFi

Participation Ver_1.0.0

Table of Contents

1. Introduction

1.1 Project Vision

The modern healthcare industry faces many challenges in terms of patient data management, transparency in medical device distribution, and privacy protection. Eternal Life Coin (ELC) aims to solve these problems in the healthcare industry through blockchain technology, decentralization, and the power of DAO organizations. Our vision is to revolutionize the global healthcare data and medical device distribution ecosystem to create a safe and reliable healthcare environment.

ELC aims to return ownership of healthcare data to patients, empower users and patients to secure their own rights to healthcare, ensure transparency in medical device distribution, and increase accessibility and reliability of healthcare information.

1.2 Meme Coin

Meme coins are cryptocurrencies based on popular memes or humorous characteristics on the Internet. They are developed with concepts that are not overly goal-oriented, and are promoted by popular character images. Dogecoin, Shiba Inu, and Bonk are representative meme coins.
ELC also actively pursues the characteristics of meme coins. Recently, rapidly developing AI and biotechnology have created new trends in Internet public opinion, and expectations and discussions about the so-called 'singularity' are spreading. In particular, the playful

expectations and humor of pursuing eternal life are becoming increasingly powerful memes in Internet communities.
ELC does not want this trend to remain as a meme, but rather sublimates it into a meme and develops it into a achievable goal in the near future. ELC aims to establish itself as a unique project that draws public sympathy through the future-oriented and fascinating idea of eternal life, while maintaining the humorous charm of a meme coin and containing a long-term vision.

1.3 ELC's Goals and Mission

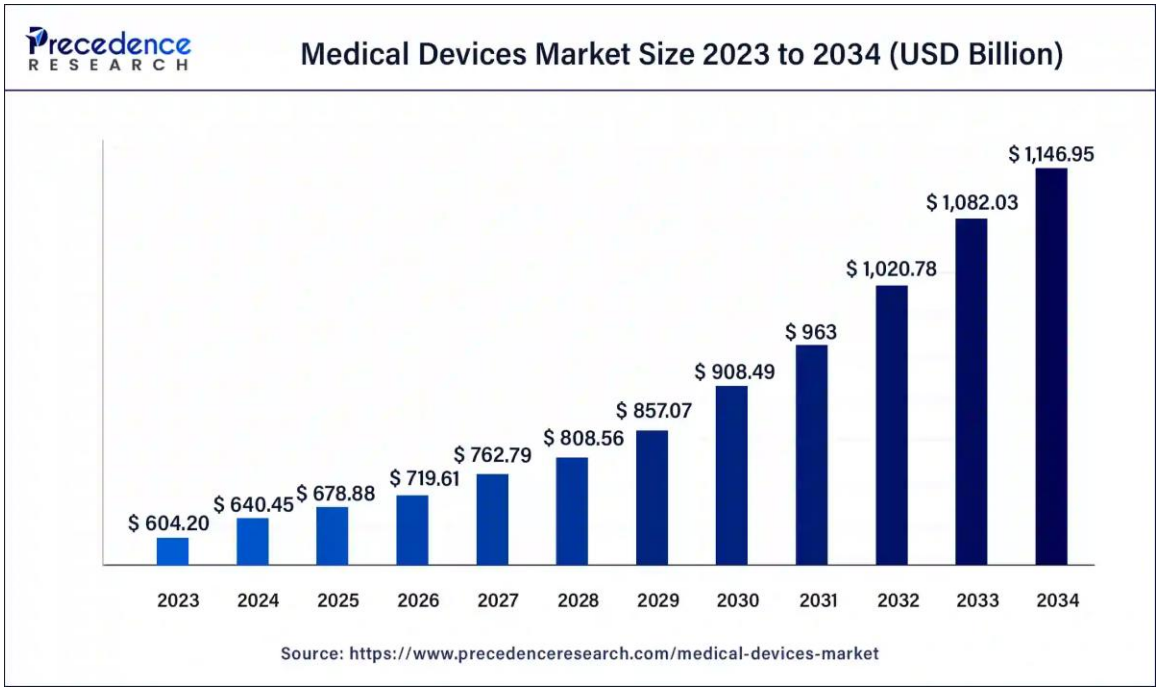
ELC has the following main goals:
- Securing healthcare data sovereignty: Supporting individuals to fully control their healthcare data and safely share it with healthcare institutions or researchers when necessary. To this end, DAOs are actively utilized for various healthcare information and commercial healthcare services, significantly transferring the price and service sovereignty of the healthcare market, which is centered around service providers, to the consumer federation system.
- Implementing community-centered governance: Through DAO (Decentralized Autonomous Organization), all participants can contribute to the direction of the project and the decision-making process.
Enhancing transparency in medical device distribution: Data from the entire process of medical device production, distribution, and use is recorded and verified through a blockchain-based tracking system.
During the manufacturing stage, medical devices are given a unique identification code, which is stored on the blockchain. This allows the authenticity of the product to be confirmed.
By recording status information such as temperature and location during the storage, transportation, and distribution of medical devices in real time, quality maintenance and safety are ensured, and the immutability of blockchain is utilized to record the distribution process of medical devices and block counterfeit and illegal inflow products. Blockchain transparently manages the supply of medical devices and materials for commercial procedures, and provides a trustworthy environment for practitioners and consumers. This promotes the use of quality-assured medical devices and increases the safety of treatment services.
- Secure storage of medical information: Using decentralized technology, medical information is safely stored and the risk of hacking and leakage is minimized.
Medical information is stored on decentralized networks (IPFS, Arweave, etc.) instead of centralized servers. This technology eliminates single points of failure by distributing data across multiple nodes. This minimizes the possibility of data loss, increases network stability, and ensures data availability.
Medical information is encrypted using advanced encryption algorithms (AES, RSA) before storage. This prevents unauthorized users from decrypting the information, and protects

the data while it is being transmitted or stored. Patients control access to their own data, and can optionally share it with healthcare providers or researchers when necessary.
By utilizing the transparency and immutability of blockchain, all access records of medical information can be tracked. Information about who, when, and what data was viewed or modified is stored on the blockchain, ensuring transparency in data utilization. This is useful for detecting hacking attempts or identifying the root cause of data leaks, and can prevent data security incidents in advance.

2. Market Analysis and Background

2.1 Current Status of Medical Device Distribution Market

The global medical devices market is growing steadily at a CAGR of 5-7%. However, there are problems in the medical device distribution process such as lack of transparency, inflow of counterfeit products, and inefficient tracking systems. These problems pose a serious threat to medical device quality and patient safety.



[Medical Devices Market Size 2023 to 2034 (USD Billion)]

2.2 Healthcare Data Management Challenges

Medical data is an essential asset for understanding the health status of patients, determining treatment plans, and advancing medical research. However, medical data is currently mainly managed by centralized institutions such as hospitals and insurance companies, which causes various problems.

First, centralized systems are vulnerable to hacking and leakage because data is centrally stored in one place. Leaked medical data is likely to be traded on the black market or used for fraud and identity theft, which can cause serious damage to patients.
In addition, most of the control over medical data currently lies with centralized institutions, and patients have difficulty accessing or utilizing their own data. This prevents patients from effectively managing their health information and can lower the quality of medical services.
In addition, each medical institution has different data management systems and standards, making it difficult for patients to transfer and utilize data when visiting other hospitals or sharing medical records. This causes problems such as duplicate testing, delayed treatment, and decreased research efficiency.
Centralized medical data management methods have limitations in terms of security, accessibility, and interoperability, and decentralized approaches such as blockchain technology are needed to solve these problems.

2.3 The need for decentralization

Blockchain technology provides an innovative solution that can solve the problems of medical device distribution and medical data management.
First, blockchain records the entire process of medical devices from production to consumption, preventing counterfeiting and enhancing transparency in the distribution channel. Information authenticated with a unique identification code is stored during the manufacturing stage, and status data during transit is recorded in real time to ensure quality maintenance and safety. End consumers can check product information directly on the blockchain.
Second, patients can safely manage their medical data through blockchain and share it in encrypted form with medical institutions or researchers when necessary. Through decentralized storage technology (such as IPFS), data is stored in a distributed network without relying on a specific institution, and cannot be accessed without the patient's consent.
In addition, blockchain enhances security through immutability and strong encryption technology designed to prevent data from being altered. The distributed network structure eliminates the risk of hacking of central servers, and automates data access and authority management using smart contracts to minimize the possibility of leakage.
Blockchain contributes to increasing trust and efficiency in the medical industry through transparency, enhanced ownership, and security.

3. ELC Project Overview

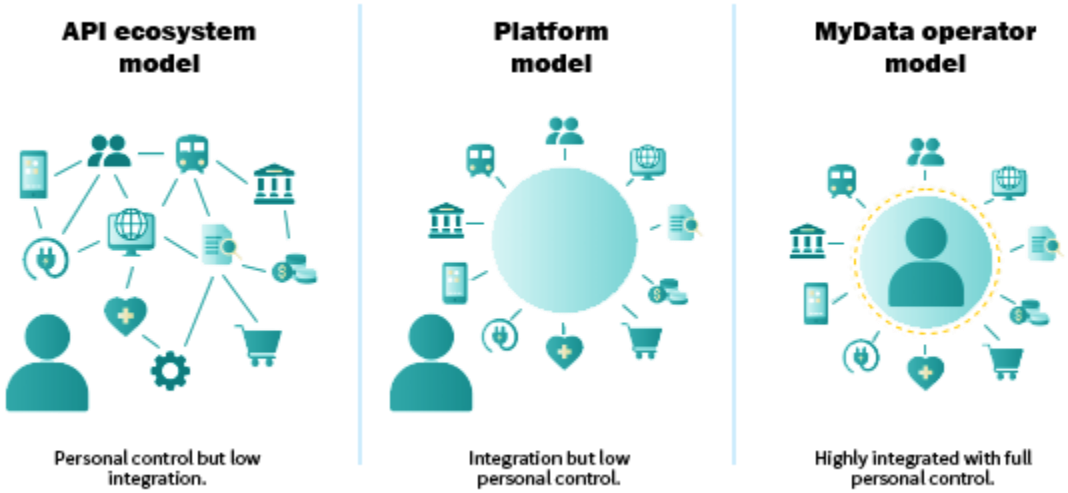
3.1 Definition of Eternal Life Coin

Eternal Life Coin (ELC) is a blockchain-based healthcare project designed to increase transparency in medical data management and medical device distribution. Built on

Binance Smart Chain (BSC), ELC will bring real change to the healthcare industry by utilizing fast processing speeds and low transaction costs.

3.2 Project Key Features and Features

- Medical data decentralization: Patients' medical data can be safely stored through blockchain and IPFS, and can be shared in an encrypted manner when necessary.
- Medical device distribution tracking: The production, distribution, and use processes of medical devices can be recorded and tracked through smart contracts.
- Transparent governance: The community participates in project operation through a DAO-based voting system.
- BSC network utilization: Provides fast transaction processing, low fees, and high scalability.



3.3 Integration with Web3

ELC provides a user-centric healthcare data management environment through Web3 technology. Users can access their data through a blockchain wallet and share data only when necessary.

4. Technology Architecture

4.1 Smart Contract Data Design

- Medical Device Tracking Smart Contract: Automatically records and verifies medical device production, distribution, and usage data
- Data Access Smart Contract: Patients control access to medical data

ELC's modeling language is used to define the domain model of the network. Below are some examples of .CTO files on how the models are defined and stored on the chain. These

can be modified according to various regulations and requirements to make the Medicalchain platform HIPPA and GDPR compliant.

Participants

Patient

Variable Type	Variable	Description
String	ID	A unique string (128-bit UUID)
Asset	PersonalDetails	Structure defined in asset
String(Array)	authorised	Array of all participants ID's that have been authorised to read HER
Asset	MedicalRecord	Structure defined in asset

Practitioner

Variable Type	Variable	Description
String	ID	A unique string (128-bit UUID)
Asset	PublicProfile	Structure defined in asset
String(Array)	Patient	Array of all participants ID's that have been authorised to read HER
Asset	MedicalRecord	Structure defined in asset

Personal Details
Relationship: Patient (Participant)

Variable Type	Variable	Description
String	ID	Unique ID for asset
Asset	FirstName	User's given name
String	Last Name	User's last name
Asset	EmailAddress	User's email used to sign up
Int	Dob	Unix timestamp of DOB
concept	Address	Defined in Concepts section
Super-Type	Owner	Extends Patient (Participant) asset

Practitioner's public profile
Relationship: Practitioner (Participant)

Variable Type	Variable	Description
String	ID	Unique ID for asset
Asset	FirstName	User's given name

String	Last Name	User's last name
Asset	EmailAddress	User's email used to sign up
Int	Dob	Unix timestamp of DOB
concept	Address	Defined in Concepts section
Super-Type	Identification ID	The assigned number the Practitioner was given when registered with practice
Array	Qualification	Qualifications Practitioner holds
String	Image Url	Pointer to Practitioners image
Super-Type	Owner	Extends Practitioner (Participant) asset

Medical Record

Variable Type	Variable	Description
String	ID	A unique string (128-bit UUID)
Super-Type	Owner	Extends Practitioner (Participant) asset
Super-Type	Author	Extends Practitioner (Participant) asset
Array	Permissions	Array of Participant IDS
String	File Hash	SHA-256 hash of the latest version of the file
Float	Version	Int increments every time a file is updated
String	Pointer	This points to where the file is in storage outside of the blockchain

Concepts

Address

Variable Type	Variable	Description
String	Number	Number/name of building
String	Street	A unique string (128-it UUID)
String	City	Extends Patient (Participant) asset
String	Country	Extends Practitioner (Participant) asset
String	Postal/zip code	Area code

4.2 Define authority

ELC Fabric includes an Access Control Language (ACL) that defines access to the .CTO domain model elements above. By defining ACL rules, you can control what resources

participants in the network's domain model can access. Some examples of such access rules include:


```
{
  "practitionerID": "PR12345678",
  "fullName": "Dr. John Doe",
  "specialization": "Cardiology",
  "description": "Experienced cardiologist with expertise in interventional cardiology.",
  "contact": "johndoe@hospital.com, +1-123-456-7890",
  "clinic": "Heart Care Clinic, 123 Main Street, New York, NY, USA",
  "qualifications": ["MD, Harvard Medical School", "Board Certified Cardiologist"],
  "profileLastUpdated": "2023-12-22"
}
```

```
{
  "practitionerID": "PR12345678",
  "patientID": "PAT98765432",
  "authorized": true,
  "authorizationDate": "2023-12-22",
  "authorizedBy": "Patient Consent",
  "accessScope": ["Medical History", "Prescriptions", "Lab Results"],
  "expiryDate": "2024-12-22"
}
```

```
{
  "transactionID": "TX12345678",
  "practitionerID": "PR12345678",
  "patientID": "PAT98765432",
  "authorized": true,
  "updateFields": ["Allergies", "Medications"],
  "updateDate": "2023-12-22",
  "authorizedBy": "Patient Consent"
}
```


ELC also provides APIs that allow third parties to obtain and interact with EHRs with the user's permission. All endpoints available in the UI are available to developers. We aim to foster a robust application and service ecosystem.

4.3 Building a decentralized application network

Web3 and blockchain technology are known as the foundation of a user-owned internet – a decentralized world where individuals have control over their data, identity, and online transactions. However, despite the promise of giving power back to users, widespread adoption of Web3 solutions for real-world use cases remains elusive.

The current landscape of Web3 is dominated by blockchain networks, particularly at the Layer-1 and Layer-2 levels, and focuses primarily on the distributed ledger technology that underpins these systems. While this has led to impressive innovations in areas such as decentralized finance (DeFi) and non-fungible tokens (NFTs), broader enterprise and consumer applications have struggled to fully transition to blockchain-based solutions. A key reason is the ongoing challenges of the three blockchain challenges that have yet to be fully solved: security, decentralization, and scalability.

Blockchain protocols are inherently slow by design due to the consensus mechanisms that ensure security and decentralization. This sluggishness, combined with the high costs associated with transaction fees, makes blockchain networks prohibitively expensive for everyday use. Moreover, the public nature of most blockchain networks raises privacy and confidentiality concerns, especially for enterprise applications that require strict data protection and compliance measures.

For Web3 to reach its full potential and be adopted into the real world, it must evolve beyond the current focus on distributed ledgers. A new generation of distributed application networks will need networks that are secure, decentralized, fast, cost-effective, and protect user privacy. These networks must be designed to scale seamlessly, handling millions of transactions per second at minimal cost, without compromising the core principles of decentralization and user ownership.

Robust p2p application protocols

Decentralized application networks require robust, application-specific protocols that can support a wide range of applications and use cases, while ensuring that power and control are managed by the protocol and distributed among users.

New primitives
Traditional client-server applications rely on server-side services, with client apps exchanging data via request-response or publish-subscribe design patterns.

However, distributed application networks require a new class of computing objects or primitives that can operate securely and in sync across peers in a distributed network. A new user experience
Many users are accustomed to signing up to centralized services. Transitioning them to Web3 requires an innovative approach that allows them to connect their wallets, maintain

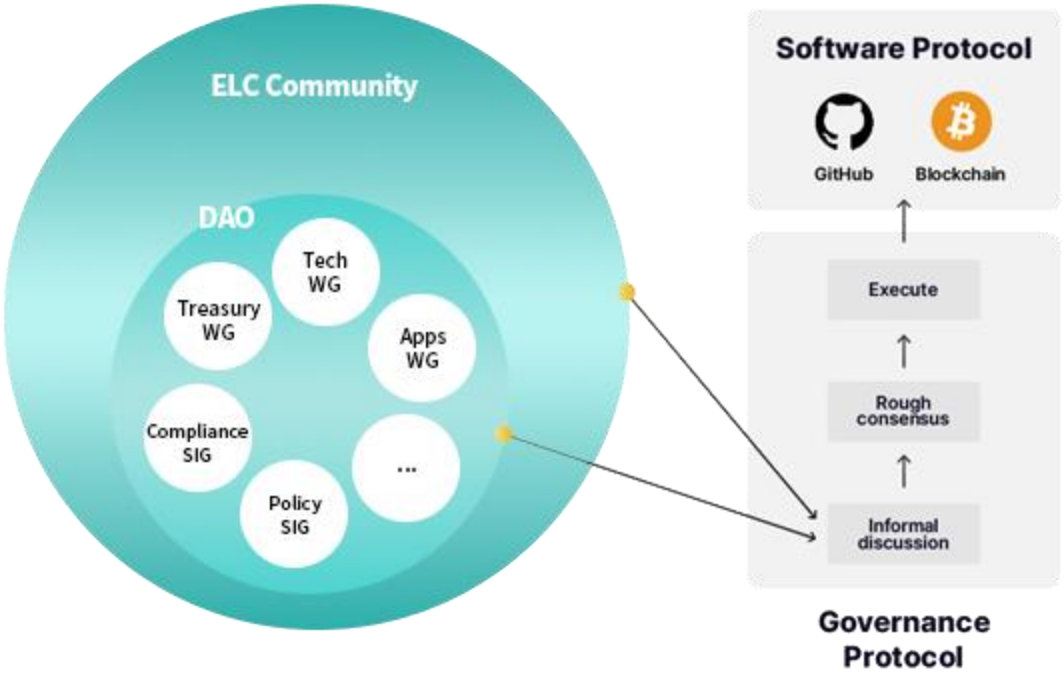
self-storage of their data, and leverage zero-knowledge identities. This experience must be complemented by a familiar user interface and seamless access to decentralized applications (dApps).

4.4 DID Self-Sovereign Identity Identifier Based

DID is a unique ID (identity identifier) that can be freely used anywhere on the Internet, created based on mathematics and cryptography without the help of a third party. It is like assigning a unique number to every atom in the universe, randomly selecting one of them, and assigning a password (private key) that can control the ID generated from that unique number and the information connected to it. Personal accounts and the information connected to that account are recorded on the blockchain, and the authority to view and control them is given only to users who own the private key. Through this, we can freely create and manage our own identity, free from the help or control of the government or corporations. This method can be used especially well in the medical field, which requires a high level of personal information protection, and since the records of identity and the authority to control them can be safely kept as long as all computers and the Internet connected to the blockchain do not disappear, it can realize the self-sovereign identity required for the vision of ELC.

4.5 DAO-based governance structure

ELC is designed to operate in a community-centered manner through a DAO (Decentralized Autonomous Organization), and participants can directly contribute to the development of the project. All ELC token holders can submit proposals and participate in voting to determine the direction of the project.



Eligibility for Governance Participation

Anyone can participate in basic governance without qualification restrictions. You can propose policy opinions in the forum or participate in improving open source code, and the IETF's Rough consensus will be adopted as the consensus method. However, some rights that require clear roles, such as policy adoption, DAO financial management, and code modification rights, will be granted to specific members elected by consensus of DAO members. This authority is managed through a Verifiable Credential (VC) that can prove that the wallet owner is a specific stakeholder, and the opinions of specific stakeholders can be reflected more heavily.

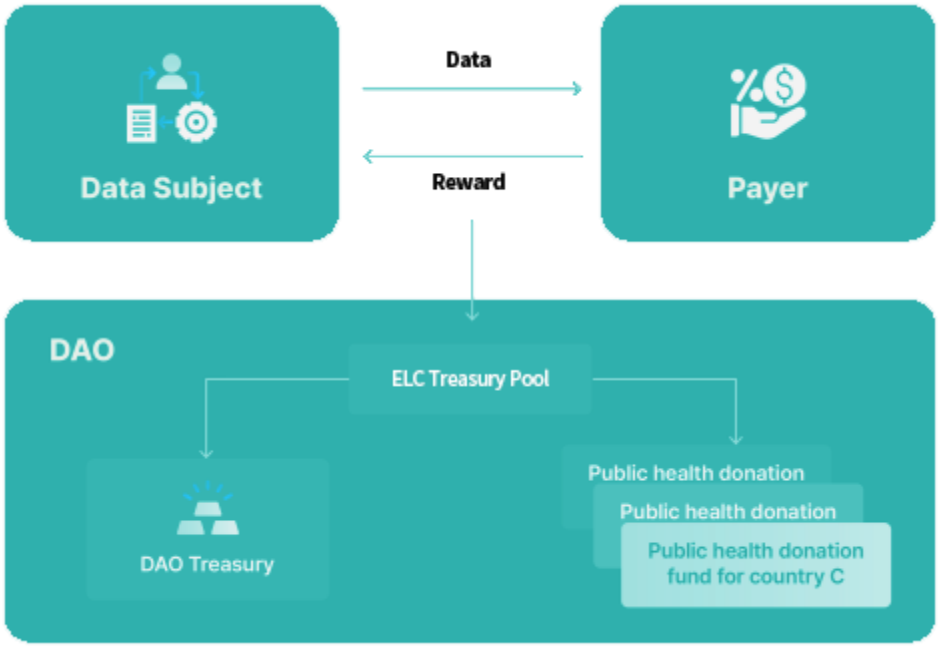
To prevent concentration and abuse of authority, authority is granted to multiple members with dispersed interests, and decisions are made only after sufficient agreement is reached among them. Authority is proven by VC through DID, and the expiration date is set according to the policy and automatically expires if not renewed.

Role of DAO

ELC DAO aims to develop software and policies through open source and voluntary cooperation, but systematic organizational support is required for major elements such as ELW SDK development and policy drafting. DAO aims to maintain a decentralized structure while supplementing technical and legal limitations by participating with members with specific roles and responsibilities, and ultimately transfer all financial and development authority to DAO.

DAO Treasury Management

DAO operates the treasury through fees generated from data transactions and tokens provided by the DAO Foundation. In addition to automated incentive distribution using smart contracts, elected managers perform tasks that cannot be automated such as contracts or transactions. Transactions of public health data are donated to public medical institutions through separate deductions, thereby strengthening public cooperation.



Data Issuer Verification Management
DAO verifies the information of data issuers and institutions, and registers the DID of the verified issuer in the registry. The Data Utilization SDK marks issuers included in the registry as 'verified', allowing the utilization organization to verify the reliability of the data without any additional procedures.

The DAO plays a key role in managing data reliably based on decentralization and transparency, and supporting the public health ecosystem.

4.6 ELW (Eternal Life Wallet) SDK

ELW(Eternal Life Wallet) SDK is an open source development kit that allows information subjects to develop a data wallet that manages their identity, data received from institutions, and assets acquired through data sharing rewards. The way personal data is stored in a data wallet is similar to storing card keys or receipts that can access the data rather than storing the original data itself. It is similar to storing not only cash or credit cards but also ID cards, membership cards, tickets, blood donation certificates, card keys, receipts, etc. in a wallet and using them whenever necessary. Just as losing a wallet means losing everything inside

it, the wallet owner has full control over it, and in other words, the wallet owner is also fully responsible for it. The same goes for data wallets.

In this chapter, we will introduce the core functions that ELW SDK plans to provide. Most of them are implemented based on open standards and open source, which is to focus on adding added value by focusing on the problems that ELC is trying to solve based on already sufficiently proven technologies rather than reinventing the wheel. This approach has the advantage of minimizing intentional/unintentional flaws that can occur in new software while still enjoying ongoing improvements and innovations in open standards. In addition, this approach allows users to access their assets and data in wallets developed based on the ELW SDK through various applications, thereby increasing the utility enjoyed by users.

Private Key Creation and Management

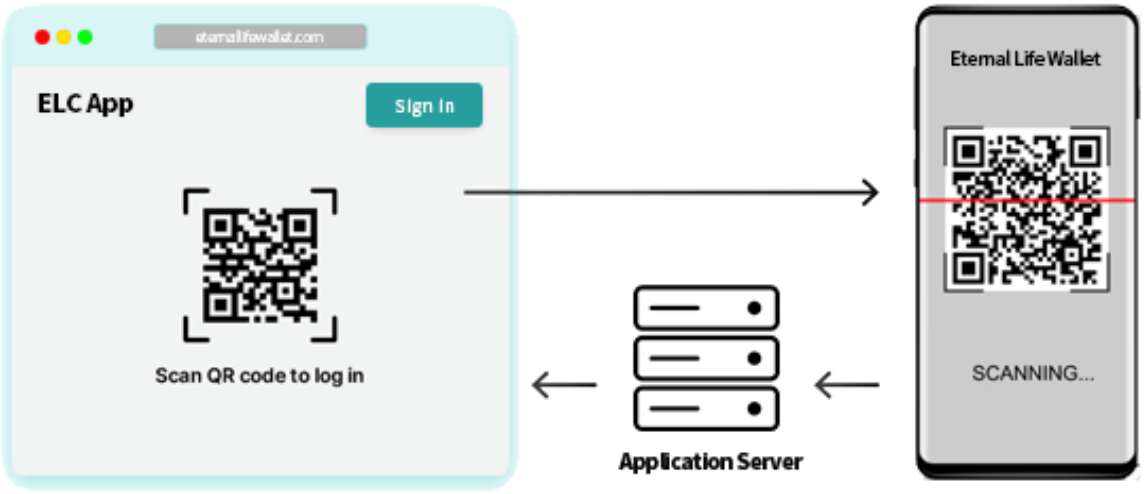
The most basic function of the ELW SDK is to safely generate and store private keys required to access and manage one's assets, data, and identity identifier DID. Since the ELW SDK is developed to be compatible with the BIP39 standard, it has the same security as most Bitcoin wallets' private keys and the mnemonic code generation method for recovering them. Therefore, the ELW SDK can also be used to basically implement Bitcoin wallet functions. For additional security in storing private keys, the device's TEE (Trusted Execution Environment) can also be utilized.

Connection, Authentication, Login

Once a user creates his or her own DID, he or she can connect P2P with institutions that access the data without an intermediary. Data and messages are encrypted end-to-end, making them inaccessible to anyone but the parties involved, minimizing the risk of personal information exposure.

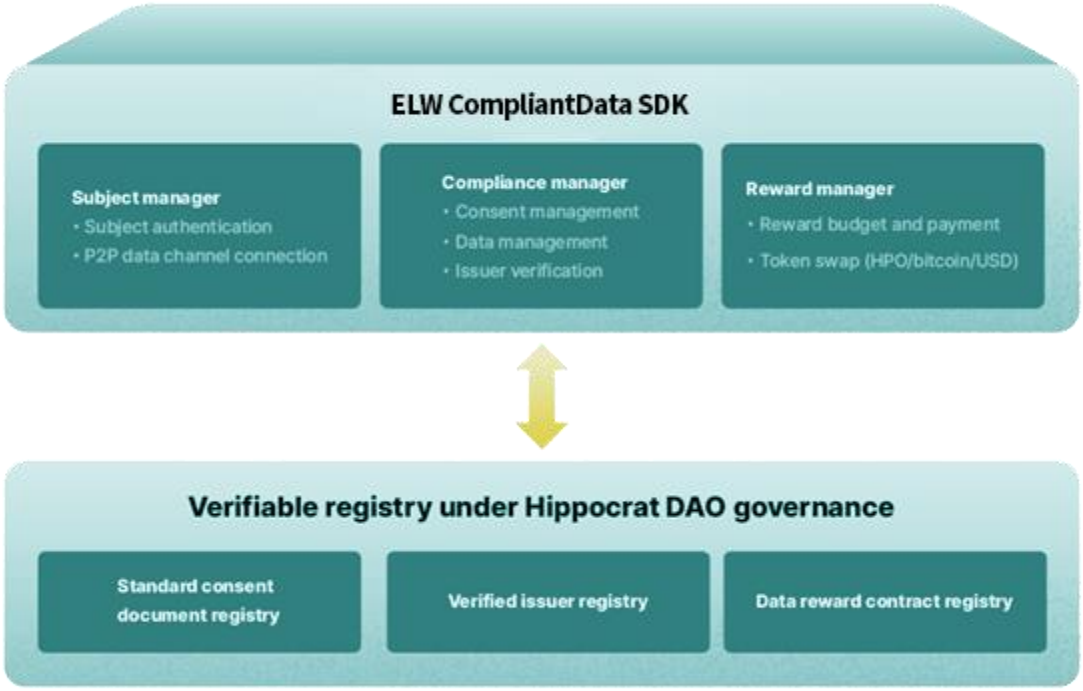
The initial connection is made by scanning a QR code or pressing a button on the institution's application or website, and the user confirms the target information and request authority and then approves. Once the connection is established, the trust relationship is maintained unless terminated.

For example, when a patient visits a hospital for the first time, they can share legal identification information such as their name and resident registration number via a QR code, and the hospital can verify this to complete patient registration. This allows for simple login, authentication, and data transmission/reception using only a QR code without creating an ID and password, and applying additional security such as a PIN or biometrics provides higher security through multi-factor authentication (MFA).



[You can easily log in, authenticate, and send and receive assets and data just by recognizing the QR code.]

Data Utilization



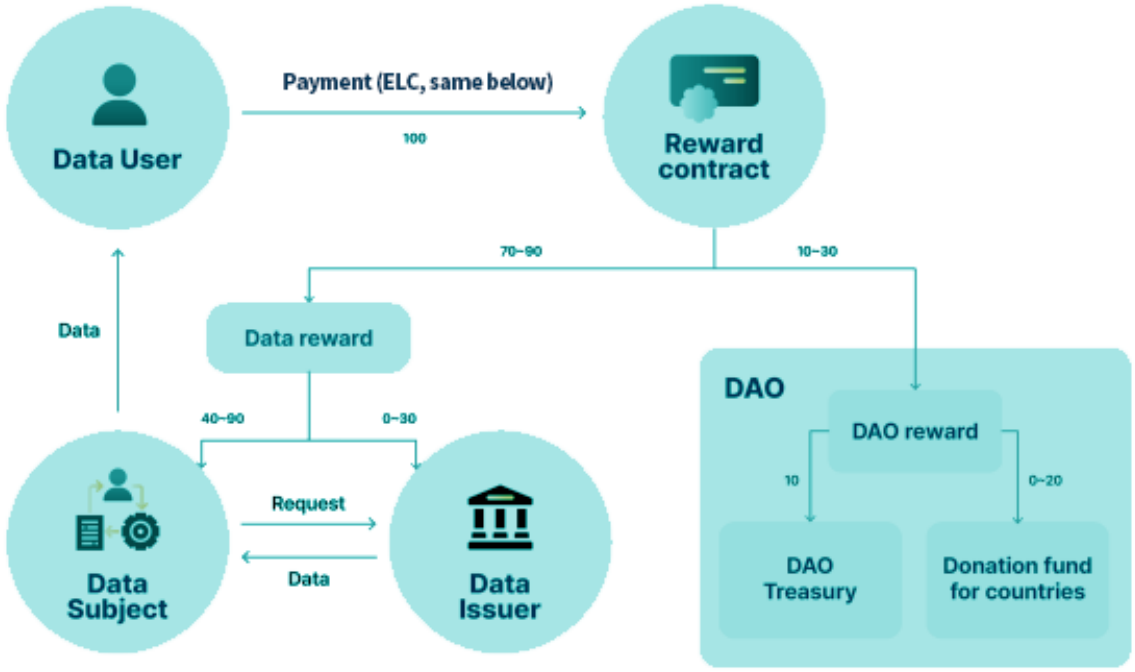
The above features will be first applied to the user service ELnote, and together with the data utilization SDK, actual patients will be able to use health management and community services through the data stored in their data wallets. The SDK can be freely integrated into other for-profit/non-profit products without separate contracts.

ELnote will provide a use case for patients to utilize the data wallet in the initial ELC ecosystem. ELnote provides reliable customized information, health management solutions, and community experiences based on data obtained with sufficient consent from patients with diseases that are difficult to access treatments such as rare diseases and incurable cancers. Furthermore, if patient-derived health data generated by patients during the service use process and clinical data submitted through the wallet are integrated and processed into a form that can be utilized by other data demand organizations such as pharmaceutical companies, high value-added data sales will become possible. This process is based on patient consent, and the generated revenue becomes a source of compensation distributed to patients and data issuing organizations, enabling sustainable data compensation and utilization.

To implement this scenario, the conditions for data utilization and compensation must be included in the content that the patient agrees to. In particular, depending on the level of personal information disclosure, data can be divided into protected medical information, de-identified medical information, limited data sets or identifiable medical information, anonymous medical information, and pseudonymized medical information. In general, the higher the level of personal information and the more information is requested, the greater the compensation amount, but the higher the possibility that the patient will refuse to protect their personal information. Accordingly, data utilization organizations will try to secure only the data that is absolutely necessary to persuade the patient. In addition, since the data involves a lot of public resources in the process of generating it, the more pseudonymized or anonymous information it is, and the more it is used for scientific research purposes, the greater the proportion of compensation distributed for public purposes. This mechanism can contribute to improving the quality of public health care services.

4.7 Incentive Model

Stakeholder Roles and Incentives
ELC stakeholders are divided into users and governance participants, and each provides incentives according to their roles. Governance participants contribute to policy development and protocol development and receive rewards through DAO, while users utilize the protocol to solve problems or gain economic benefits. ELC complies with the regulations of major countries and designs a reliable incentive model through consensus with the community.



Governance Participant Incentives
Governance participants participate in policy proposals and agreements in the DAO for the development of the protocol, and receive compensation based on DAO income (data transaction fees, etc.). This compensation is provided in the form of a project-level contract or salary, and the size of the compensation may increase as the protocol develops. The compensation distribution rate is determined through discussion and agreement of the DAO.

Protocol User Incentives
-Information Subject: Has control over data transactions and utilization, and receives compensation in exchange for sharing data. Can enjoy economic compensation and services through transactions with data users.
Data Issuer: Provides data creation costs and expertise, and negotiates the compensation distribution rate with the information subject. The issuer can set the compensation to no more than half of the information subject's share, and the appropriate distribution rate is determined through a competitive market mechanism.
Data User: Obtains consent to data utilization by offering attractive services and compensation. Public interest and low-personality data are distributed as public resources, and can support research and health services in cooperation with governments and public institutions of each country.

ELC builds a sustainable ecosystem through an incentive model that aligns with the roles and motivations of stakeholders.

5. ELC Ecosystem

The ELC ecosystem is designed around securing healthcare data and ensuring transparency in the distribution of medical devices. The ecosystem consists of the following key players:

1. Patients: Key players who own healthcare data and control access and sharing of data. Patients can optionally share their data with research institutions and healthcare providers and receive compensation.

2. Medical device manufacturers: Build trust in the supply chain by recording product quality and certification information on the blockchain. Manufacturers can authenticate the source of products through smart contracts.

3. Distributors: Deliver medical devices to hospitals and healthcare providers and transparently manage all data during the distribution process. Prevent counterfeit products from entering the market through a smart contract-based tracking system.

4. Hospitals and healthcare providers: Obtain patient consent to utilize data and provide compensation for data sharing. Hospitals can also verify the safety and reliability of products through a medical device tracking system.

5. Research institutions and pharmaceutical companies: Analyze healthcare data to develop new drugs and conduct research. Only data with patient consent is accessible and data usage fees are paid to patients.

6. Regulators: Monitor the quality and safety of medical data and medical devices to ensure compliance. Leverage the immutability of blockchain to audit data and quickly resolve issues.

The ELC ecosystem aims to create a patient-centric healthcare environment where these participants work together. Transparency and security using blockchain technology play a key role in creating a trustworthy ecosystem for all participants.
The ELC ecosystem is designed around collaboration between medical device manufacturers, distributors, hospitals, patients, researchers, and regulators. Through the blockchain network, each participant exchanges trusted data in real time, while patients are guaranteed control over their own data.

6. Medical Device Distribution Data Tracking

ELC records all stages of medical device distribution on the blockchain to ensure transparency. Data recorded at each stage cannot be changed and can be verified by participants in real time. The main functions of the distribution data tracking system are as follows:

1. Product authentication: Medical devices are given a unique identification code during the manufacturing stage, which is stored on the blockchain. This allows you to verify whether the product is genuine.

2. Real-time status tracking: Status information such as temperature and location during the storage, transportation, and distribution of medical devices is recorded in real time to ensure quality maintenance and safety.

3. Anti-counterfeiting: The immutability of blockchain is utilized to record the distribution process of medical devices and block counterfeit and illegal products.

4. Supply chain management efficiency: Share data between manufacturers, distributors, and hospitals in real time to improve the efficiency of the supply chain.
ELC records and tracks the entire process of medical device distribution through smart contracts. This prevents the inflow of counterfeit products and increases the transparency of the supply chain. Smart contracts record all data from the production of medical devices to reaching the final consumer in real time, and participants can verify this.

7. Decentralized Medical Data Storage

ELC utilizes decentralized storage technology to manage healthcare data securely and efficiently. Key features include:

1. IPFS-based distributed storage: Healthcare data is stored on a distributed network using the InterPlanetary File System (IPFS). This ensures data integrity and availability, and eliminates a single point of failure.

2. Encryption and access control: All data is strongly encrypted before storage, and patients have complete control over data access. Healthcare providers and research institutions cannot access data without the patient's explicit consent.

3. Data backup and recovery: Decentralized data storage distributes data across multiple nodes, so there is almost no risk of data loss. Data can be quickly and safely recovered when needed.
Medical data contains sensitive information, so it is managed securely using decentralized storage technology (IPFS). Data is stored encrypted, and patients have control over data access. Decentralized storage reduces the risk of hacking and data leakage.

8. Governance Structure

ELC provides a transparent governance structure based on a Decentralized Autonomous Organization (DAO). Its main features are as follows:

1. Participatory decision-making: All ELC token holders can participate in the DAO's decision-making process. Token holders decide the direction of the project by voting on proposals.

2. Smart contract automation: The decision-making process is automated through smart contracts, and the results are recorded on the blockchain to ensure transparency and fairness.

3. Upgrades and improvements: The DAO is used to discuss and implement technical upgrades or ecosystem policy changes to the ELC platform. This ensures the sustainability of the ecosystem.

4. Decentralized authority structure: It is designed to exclude centralized decision-making and allow all participants to contribute to the development of the project with equal authority.
ELC realizes participant-centered governance through DAO. DAO members use ELC tokens to participate in voting and influence major decisions of the project. This process is executed through smart contracts to ensure fairness and transparency.

9. Roadmap

ELC's roadmap sets clear goals and schedules for each stage to ensure successful execution of the project:

- Q3 2024: Project design and team composition
- Blockchain architecture design

- Q4 2024: ELW alpha test
- Binance Smart Chain-based network construction
- Smart contract design DeFi development

- Q1 2025: ELW beta service
- Key partnerships including medical device manufacturers and hospitals
- DEX exchange listing

- Q2 2025: Shopping mall linkage platform beta service
- Community-based governance activation

- Q3 2025: Global shopping mall linkage ecosystem expansion

- Q4 2025: DAO-based global service and curation

10. Token Information & Allocation

ELC is built on the smart contract of Binance Smart Chain (BSC). BSC is one of the chains that emerged after Ethereum, and is attracting attention for its low transaction fees and fast processing speed. BSC is easy to develop and has high accessibility, which has the effect of shortening the overall development period, and it has the advantage of being able to utilize the blockchain ecosystem that already has a large number of users. These characteristics are efficient in terms of development and promotion when designing and distributing utility tokens, and they facilitate cost reduction and further development. In addition, BSC can easily perform token issuance and management through the BEP20 standard.

Among the token standards provided by Binance Smart Chain, ELC will utilize BEP-20 and NFT standards (e.g. BEP-721, BEP-1155). BEP-20 is the most commonly used token standard on BSC, and has the advantage of being easy to link with third-party wallets and bridge services. It guarantees compatibility for transactions on the BSC network, and supports smart contract functions, making it suitable for developing various applications. BEP-721 and BEP-1155 provide standards for creating and managing NFTs, supporting the ability to prove unique ownership of digital assets or efficiently handle large amounts of NFTs.

All users can stake AI-bot computing NFTs on CeFi and DeFi platforms by utilizing the token wallet and NFT collection functions provided by ELW. Staking refers to the act of locking cryptocurrency (token/coin) on a blockchain network and utilizing it for platform operation in exchange for rewards (e.g. interest). Thanks to BSC's low fees and fast processing speed, ELC users can experience efficiency and economy in staking and trading activities.

Most transactions that occur on ELW are subject to rewards or fees, which are calculated in proportion to the number of tokens that the user trades or stakes. This ecosystem actively utilizes the characteristics of BSC and the BEP standard to provide an efficient and scalable financial experience.

10.1 Token Information

ELC tokens are utility tokens used for data trading, distribution tracking, and governance activities within the healthcare ecosystem.

Name	Eternal Life Coin
Symbol	ELC
Network	BEP-20
Number of Issues	1,000,000,000
Issuance Method	PoS
decimal	18

10.2 Token Distribution

ELC	Quantity	Ratio	Note
Total	1,000,000,000	100.00%	
Private Sales	100,000,000	10.00%	
Research Infrastructure including Facilities	250,000,000	25.00%	
Ecosystem	150,000,000	15.00%	Liquidity provision
Reserve	100,000,000	10.00%	Reserve
Marketing and Partners	150,000,000	15.00%	Promotion fee pool. Affiliate, system integration
DAO & DeFi & Airdrop	250,000,000	25.00%	Dividend and DAO incentive liquidity provision pool

11. Security and Compliance

ELC is designed with security as a top priority. The network is secured through regular security audits and smart contract verification, and operates in compliance with global data protection regulations (e.g. GDPR and HIPAA).

12. Conclusion

Eternal Life Coin is an innovative project designed to solve fundamental problems in the healthcare industry. It aims to secure ownership of patient data, increase transparency in the distribution of medical devices, and build a healthcare ecosystem that all participants can trust by utilizing blockchain technology and decentralized networks.

13. Disclaimer

This white paper was written for the sole purpose of providing specific information about the ELC platform and team to those interested in the ELC project. This white paper is not intended to encourage readers to invest in the ELC team and project, and is completely unrelated to investment.

In addition, the ELC tokens in this white paper are not securities that are investment targets, and do not represent investment value. ELC tokens are used within their own ecosystem and do not have the nature of securities (security), so they do not have any rights as

shareholders, such as voting rights or dividend rights, regarding ELC services and the foundation, or any other rights equivalent thereto.

This white paper provides the business plan and opinions of the ELC team 'as is', and we inform you that the contents of this white paper may be changed as necessary during the business development process.
Therefore, when using or referencing this white paper, please make a decision on whether to participate in the project at your own discretion. The results of your decisions, regardless of whether they result in profit or loss, are entirely attributable to you, and you are also legally responsible. Please note that the ELC team does not assume legal responsibility for any decisions you make using or referencing this white paper, and that the ELC team does not assume any responsibility for any damages, losses, debts, or other financial damages that may arise to you as a result of decisions you make referring to this white paper.

The ELC team does not guarantee that the white paper was written based on legitimate rights and does not infringe the rights of any third party, that the white paper is commercially valuable or useful, that the white paper is suitable for achieving your specific purpose, or that the content of the white paper is free of errors. Of course, the scope of liability exemption is not limited to the examples above.