CESS

Cumulus Encrypted Storage System

An Infrastructure of Decentralized Cloud Data Network

https://cess.cloud

Abstract

Cumulus Encrypted Storage system (CESS) will demonstrate a strong presence in the marketplace and addresses the deficiencies of centralized technology in use today. CESS has created the infrastructure to scale with the need of a joint community and to safeguard the data. With data privacy being the most sought-after concern, CESS incorporates privacy as the utmost important consideration in designing the infrastructure. Unquestionably, performance and scalability are in the same think tank. There are three interoperable key characteristics of CESS: the Decentralized Cloud Data Network Infrastructure, the Decentralized Cloud Storage System, and the Decentralized Data Sharing Platform. They work together to solve the limitations of data security and storage capacity that have plagued mankind.

The Decentralized Cloud Data Network Infrastructure is a framework based on Blockchain, positioning its approach to distributing data without intermediary governance within the decentralized peer network. The Blockchain technology deployed is to distribute tokens and employs idle resources to yield data protection and privilege. The scheme of data network requires the verification of data entitlement which defines data ownership; it reinforces CESS cloud data network that encompasses cross-platform data, cross-collaboration, and cross-format, and thus inheriting tracking and supervision of data circulation.

The Decentralized Cloud Storage System has an account system, smart contract, and trusted decentralized cloud data network that can build an extensive distributed storage network. In conformity to application needs, it can launch a variety of transaction curation and consensus mechanisms, and create specific solutions for the development of CESS storage ecology that is well suited for commercial cloud storage need.

The CESS storage ecology is the online data sharing protocol that encapsulates data interoperability serving the Decentralized Online Data Sharing Platform for developers, creators, and consumers to build and evolve together. Examples are literary works, paintings, music, videos, and media. Originators on the internet can store NFT data on the Cumulus Encrypted Storage System as exclusive tokens. The tokens encourage a fan-based economy to share, trade, circulate and own NFT assets on the Decentralized Cloud Data Network. The community involved will generate a token economy, driving a new business model on CESS which has an unlimited "scalability" in future applications with data privacy, data security, data stability, data rights confirmation, and data rights protection.

CESS embraces evolving technologies. Decentralized data distribution is the future of the digitized world. With Blockchain paving the way to the next generation of the Internet namely Web 3.0, and with CESS, it is a powerful driving force for the development of Web 3.0.

Contents

1.Project Overview

With rapid advances of new computing technologies such as big data and machine learning, the value of humanity's digital assets, the so-called "Digital Gold", are being discovered. Explosively growing amount of data in cyberspace calls for new technologies of secure data storage and efficient data sharing. The challenges are to achieve secure storage, efficient sharing, and trading with data owner's rights protection, but current solutions are complex and worrisome.

Cumulus Encrypted Storage System (CESS) is dedicated to develop a new global decentralized cloud storage online data sharing platform – a network infrastructure that is transparent, efficient, and equal opportunity to all members of the global community. The CESS data sharing protocol enables: a) data interoperability in manner of cross-platform, cross-collaboration, and cross-format, b) tracing and monitoring data trading market, and c) fair and transparent data profit rewarding. CESS will adopt a phased approach to implement the above goals.

1.1 CESS, a Blockchain Based Decentralized Distributed Cloud Storage

Cloud data technology makes it possible for users to access data anytime and anywhere. However, conventional centralized cloud storage systems have drawbacks of low data security (e.g., data loss, data breaches and tampering), low auditability, no data rights protection, isolated data islands, etc. A new secure data storage solution is needed to overcome these significant headwinds.

The goal of **CESS project phase I** is to build a decentralized distributed cloud data storage based on blockchain technology, which provides users with cloud storage capability and user experience, but without the disadvantages of over-centralized systems.

CESS encourages excess or under-utilized resources as nodes to join CESS's unrestricted expandable network via the token economy incentive method. Each node joins the CESS peer-to-peer network by contributing data storage resources, computational resources, or network bandwidth. Built on our state-of-the-art virtualization and cloud computing technologies, CESS organizes and manages the participating resources providing clients with secure, high performance, and boundless cloud data storage services. Furthermore, the CESS protocol enables interconnection of network nodes, to build a large decentralized cloud storage system that supports up to 100PB storage scale to meet the demand of enterprise level data storage.

In Cumulus Encrypted Storage System (CESS), data files are encrypted and sliced into small data segments and are distributed to storage nodes. CESS storage proof scheme, Proof of Data Reduplication and Recovery (PoDR²), guarantees that system always holds multiple copies of user data files for retrieval. A missing data segment will not impact the integrity of a user data file.

CESS is a distributed ecosystem with user friendly ledgers, novel consensus mechanism, and reliable storage infrastructure. More so, CESS offers the advantages of low cost, privacy protection, security and robustness. With the implementation of CESS data confirmation and proxy re-encryption technology, CESS provides our clients with trustworthy, secure and reliable data rights protection.

The advance of cloud storage and blockchain technologies is revolutionary.

1.2 CESS, a Blockchain Based Decentralized Cloud Data Network Infrastructure

Today's internet world is dominated by super platforms. In 2016, a book named "Platform Revolution, How Networked Markets are Transforming the Economy" by American scholars, Sangeet Paul Choudary/ Marshall.W.Van Alstyne/ Geoffrey G.Parker, indicates that the essence of Web 2.0 is platform economy, and that platforms are eating the world. By obtaining and controlling data from both service suppliers and service users, the Web 2.0 giants gain the majority of market shares and profits. Data and their regulations become core assets of enterprises and are completely under their control. Ordinary users are excluded from participating in the digital economy.

A new global digital economy will be a decentralized, open and transparent network world. Users will have control of their own data and will be rewarded for their data values. The blockchain based decentralized distributed storage offers the advantages of data security and data rights protection, and will lay a solid foundation for a future data-driven and bottom-up business model.

CESS is committed to build a decentralized cloud data network infrastructure and has proposed an innovative **R²S** consensus mechanism, namely, **Random Rotational Selection** consensus mechanism, to achieve low gas fees and rapid transaction processing throughput (10,000TPS), and to provide a fair, transparent, equal opportunity data sharing market to all participants, not manipulated by giant nodes. This is the goal of **CESS project phase II**.

1.3 CESS, a Decentralized Cloud Storage Online Data Sharing Platform

In future applications, CESS decentralized cloud storage online data sharing protocol will enable data interoperability in manner of cross-platform, cross-collaboration, and cross-format, that is, a platform for developers, creators, and consumers to build and evolve together. The CESS **Multi-format Data Rights Confirmation Mechanism (MDRC)** provides data owners with data rights protection and it is capable to process multiple data types. Individuals' digital assets will be uploaded, shared, and traded in a protected market, and the values of the digital assets will be continuously explored.

CESS decentralized cloud storage network will become a strong driving force of Web 3.0, and a key component of Web 3.0 infrastructure. This is **the ultimate goal of our CESS projec**t.

2. CESS, a Blockchain Based Cloud Storage Solution

A blockchain based decentralized cloud storage offers more security, integrity and scalability than traditional centralized storage networks. In the CESS solution, all user data files are encrypted, replicated and sharded to ensure security and redundancy, and users are given unique private keys to access their private data. In addition, storage nodes only store segments of data files, greatly protecting network from data leakages.

CESS encourages excess or underutilized resources as nodes to join CESS's unrestricted expandable network via the token economy incentive method. Each node joins the CESS peer-to-peer network by contributing data storage resources, computational resources, or network bandwidth.

Storage miners are incentivized to contribute their unused storage and bandwidth to the network. Clients pay to store or retrieve shared data. All user transactions are recorded and secured by CESS blockchain, and the integrity of stored data are guaranteed by CESS storage proof schemes.

The following are the key technologies of CESS storage network, and they will be further detailed in later chapters:

A fair and effective incentive model. This is to attract more resources around the world to join and build the CESS network infrastructure.

A mathematically verifiable consensus mechanism. This is to guarantee the system reliability and to protect the network from malicious attacks.

A distributed data storage technology. This is to efficiently manage system storage resources, to maintain the integrity of user data, and to provide fast data access.

Currently there are several existing blockchain based distributed storage solutions in the market. We will discuss our unique incentive and consensus mechanisms in detail.

2.1 Incentive Model

The purpose of designing a CESS network incentive model is to encourage miners to provide honest and quality storage service, and therefore to maintain entire network stability. Our model mathematically quantifies contributions of network participating nodes, and fairly allocates rewards. It is also very important to make an overall CESS token allocation plan among initial contributors, miners, and CESS partners. Both miner incentive model and CESS token allocation plans are detailed in Chapter 7.

2.2 CESS Consensus Mechanism

Various consensus algorithms exist today and most common ones are Proof of Work (PoW) represented by BTC and ETH (ETH is on its way to switching to PoS), Proof of Stake (PoS) represented by Cosmos, and Delegated Proof of Capacity (DPoS) represented by EoS. While most algorithms are proven to be reliable and robust, significant challenges still remain such as low Transaction Per Second (TPS) rate, expensive transaction fees, lack of average miner incentives, and security issues.

CESS proposes a new consensus mechanism, namely the Random Rotational Selection(R^2S) consensus mechanism, that aims to optimize and solve some of these issues. The goal is to provide a data sharing platform with a novel consensus mechanism that has low gas fees, high transaction speed (10,000 TPS), and fair incentives to all participating consensus miners. Section 4.2.4 describes our approach.

2.3 Data Storage Workflow

When a client requests to store a data file, the CESS platform pre-processes the data file to obtain and store its meta-data and data fingerprints. The pre-process software also performs data file replication and fault tolerant erasure coding. The meta-data includes info of data owner, data keywords, and etc. The data fingerprints are for subsequent data rights confirmation.

Figure 1 illustrates the CESS data storage workflow.

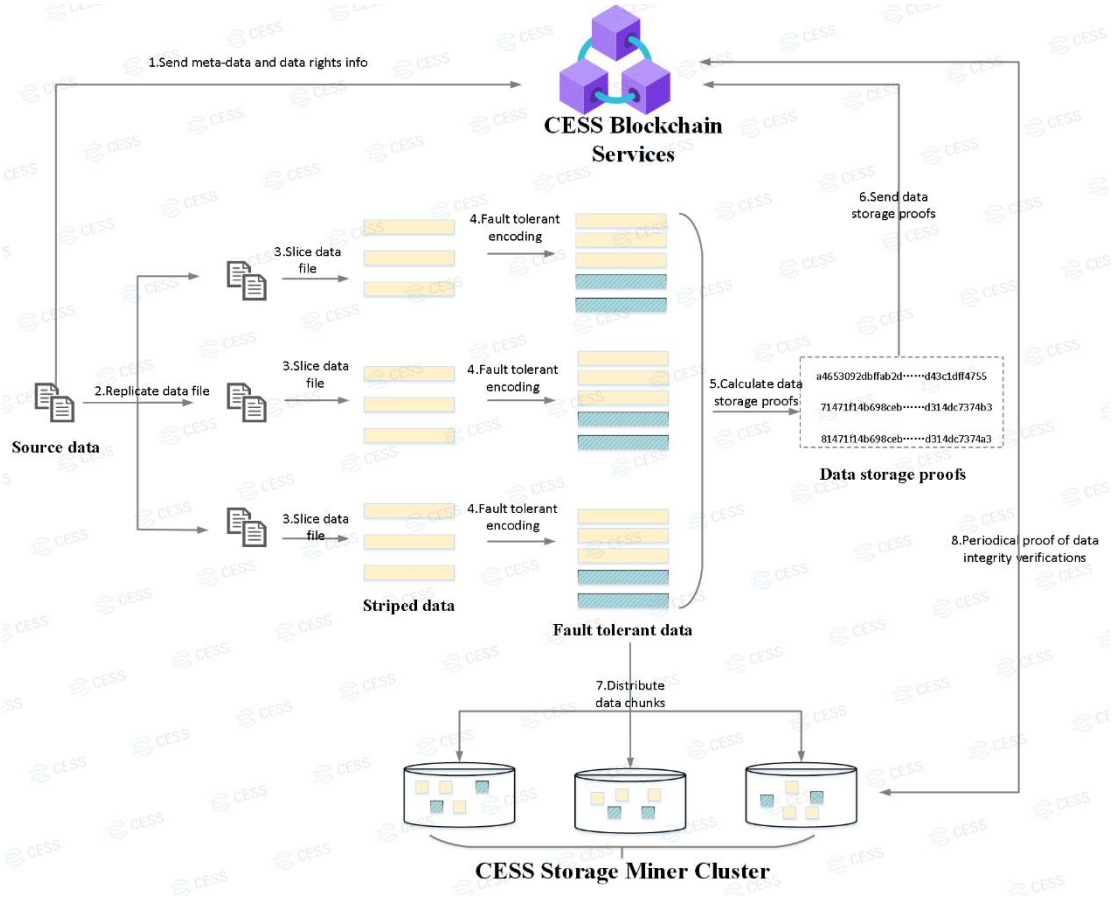

Figure 1 Data Storage Workflow

Step 1. User data files are uploaded and pre-processed by CESS client software. Meta-data and data fingerprints are generated and submitted to CESS chain.

Step 2. Each data file is replicated, by default, to three identical copies.

Step 3. Each copy is sliced into small data segments.

Step 4. Apply fault tolerant erasure coding (3,2), so that even if two data segment copies are destroyed, they can be recovered via fault tolerant method.

Step 5-6. Generate auxiliary data needed for CESS proof schemes, namely, Proof of Data Reduplication and Recovery (PoDR²), Proof of Replication and Proof of SpaceTime.

Step 7. Randomly and evenly distribute and store data segments to miners' storage nodes.

Step 8. Periodically validate data segments stored on all nodes, using CESS proof mechanism PoDR², to ensure data reliability and completeness.

2.4 CESS Client-Platform Interactions

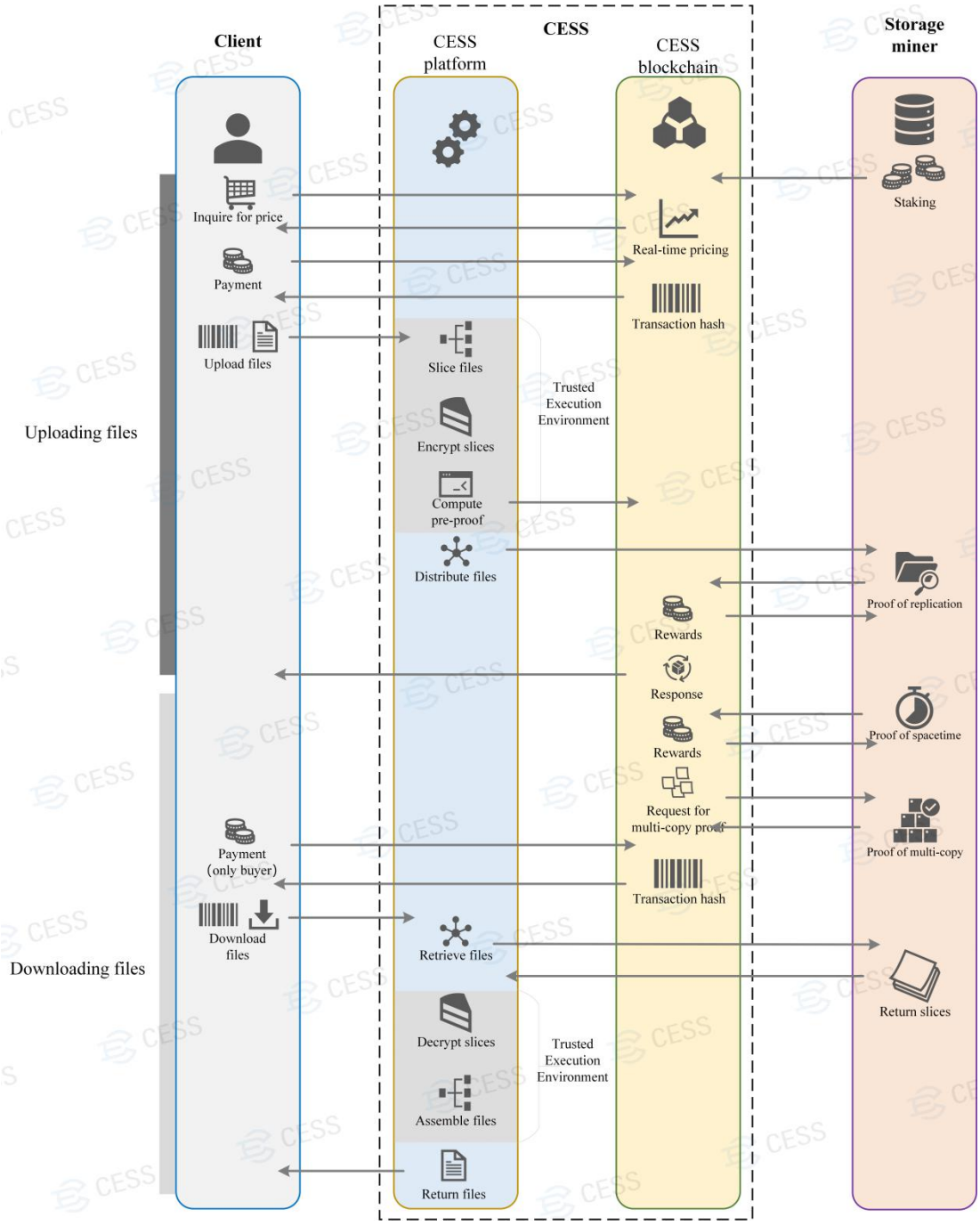

Figure 2 Client-Platform Interaction

A typical CESS data client and platform interaction flow is as follows: first, a data storage client interrogates CESS chain to get current storage price. The client then places an order for his/her data file via on-chain smart contract. Once the payment is made and order is approved, the client then uploads the data file using API provided by CESS platform. The data file is not directly uploaded to storage nodes, instead it is uploaded to a CESS storage scheduling node. The scheduling nodes are the ones with secure hardware environment (Trusted Execution Environment

or TEE) and the data file will be pre-processed, encrypted, and sharded (as described in section 2.3). Finally, the scheduling node distributes data segments to storage nodes to store.

CESS storage miners do not make deal directly with clients, and they get rewarded from CESS system by providing storage space. Miners' storage resources are uniformly managed by CESS system, which fairly distributes data files. Miners have the responsibility to maintain the integrity of clients' data. Any malicious behavior will be punished (CESS token deduction).

2.5 On-chain Data Rights Confirmation

CESS is committed to create a strong data-rights-protected marketplace for data originators. Without proper data rights protection enforcements, a data exchange market will become the best candidate for cyber piracy and it will not be able to provide high quality contents to end users. With this in mind, CESS has designed a unique on-chain Multi-format Data Rights Confirmation Mechanism (MDRC), which extracts data fingerprint from each data file as data certificate ID, and checks similarities based on certificate IDs to prevent data rights violations. CESS MDRC mechanism confirms data owners' rights, and provides a strong evidence for copyright protection disputes.

CESS data fingerprints extraction algorithm is designed to process different data types that require very different extraction methods. It can handle text, photos, audio, video, and other data formats.

Section 5.1 discusses the details of MDRC mechanism.

3.Application scenarios

3.1 Distributed Network Drive

CESS offers Distributed Network Drive/disks service to end users. Compared to traditional Network Drive service providers, the CESS network disk service has significant advantages on security, ownership protection, cost, and capacity.

CESS disks do not require cloud servers, effectively avoiding dependency on the backbone and centralized servers. Instead, user data are stored in multiple storage nodes. Data uploading/downloading is no longer restricted by network disk service providers, and data transfer speed is greatly improved. By adopting blockchain-based cryptographic algorithms to encrypt stored data, CESS ensures the privacy of user data, without worrying about data loss or central server outages. The disks' capacity can be dynamically expanded according to actual needs, breaking the storage size limitation of traditional network drive service.

3.2 NFT Storage and Trading Platform

Recently in the crypto-universe, NFTs have attracted significant enthusiasm from artists, auction houses, art collectors, celebrities, as well as strategic investors and societal elites who wish to capture the upside of the novel investment vehicle and/or hedge against inflation. Decentralized and secured storage of NFT provenance and trading data underpins consumer confidence on the respective NFT trading platform and NFTs traded on the platform. CESS answers the call for such a decentralized and secured data storage system.

NFT developers and/or owners only need to upload NFT files and CESS will verify and confirm owners' data rights using the Multi-format Data Rights Confirmation Mechanism (MDRC), and then distribute the data files to storage nodes. Characteristic structural features, subject and semantic features are automatically mirrored in the vector space of CESS, to enable proper indexing and mapping, which in turn facilitates both the public visits and private safe retrieval of the NFTs. For example, if an American artist creates an NFT artwork and sells it to a UK buyer online through CESS, the copyright transfer and time-stamping of the transaction will be executed transparently and remain permanently trackable, as intrinsically guaranteed by CESS blockchain technology. The new owner of the NFT (i.e., the UK buyer) will be automatically and uniquely issued an encrypted code (i.e., private key) upon the completion of online transaction. The old private key held by the American artist will automatically become obsolete simultaneously.

In future applications, the CESS storage ecology will be the interactive platform serving the Decentralized Data Sharing applications for developers, creators, and consumers to build and evolve together. Examples are literary works, paintings, music, videos, photos, and more. Originators on the internet can store NFT data on the Cumulus Encrypted Storage System as

exclusive tokens; data will be protected by CESS MDRC, namely Multi-Format Data Right Confirmation; MDRC confirms data right for the initial submission by the creator, therefore, achieving NFT data asset protection. Meanwhile, the copyright confirmation and transfer are in real-time and transparent. The protected tokens encourage a fan-based economy to share, trade, circulate and own NFT assets on the Decentralized Cloud Data Network. The community involved will generate a token economy, driving a new business model on CESS.

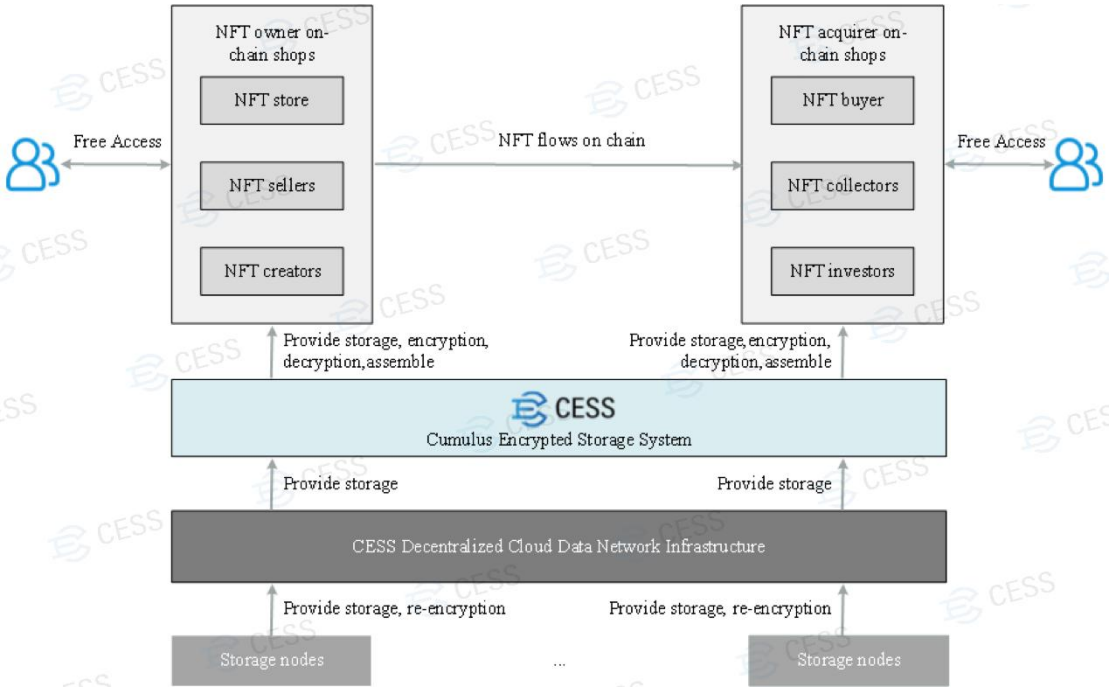

Figure 3 NFT Storage and Trading Architecture

3.3 Distributed Enterprise Storage Service

As a decentralized cloud storage system with a tremendous amount of storage resource pool, CESS perfectly meets the demand of enterprise data storage services.

The CESS storage network is built on blockchain technology and multiple storage proof mechanisms, including our innovative Proof of Data Reduplication and Recovery (PoDR²). The system makes full use of underutilized bandwidth and unused storage resources to provide a more powerful and more efficient storage service than traditional cloud storage at a low cost. CESS validates and protects owners' data rights, and provides an open yet secure marketplace for data sharing.

Specifically, CESS brings the following changes to the data storage industry:

Evolution of Data Production Chain:

Our distributed storage can make the data production process non-linear and network oriented, that is, all production elements can be network configured. Data production becomes fully synergized, generating products in a manner of human-machine-human collaboration (so called “crowd-production”).

Evolution of Data Flow Chain:

CESS makes it possible to eliminate traditional intermediary data transaction channels. This elimination enables all kinds of users to access data products anytime and anywhere. New data flow chain modes for data products and services, such as non-linear circulation, will occur. Traditional monopoly data channels and platforms will be replaced. Smart contracts between producers, products, and users make it possible for trustworthy dissemination between products and service points. Transaction costs will be greatly reduced.

Evolution of Data Consumption Chain:

Instead of giant corporations or data centers dominating the data arena, the sovereignty of data is now changed. The rightful owners of data now can store, integrate, optimize, match, and participate in managing their digital assets.

3.4 Data Rights Protection

From clients' point of view, CESS is a decentralized and user-managed data content sharing platform. Our mission is to give data ownership back to users, to encourage users to explore the values of their digital assets, and at the same time protect users’ rights. With this in mind, CESS has implemented an on-chain smart contract based data sharing platform that is self-executable, fair and transparent. It also covers the entire life cycle of data rights confirmation, data rights tracking, and data rights protection.

CESS offers two types of smart contracts to users with different profit models. When users upload data files, they get to choose model values. CESS generates data file attributes based on user inputs. The data attributes include profit model type, whitelist, blacklist, and so on. Data attributes are published together with user data. Whenever a data file is retrieved, its smart contract is executed according to the program set by the data file owner. Based on data file attributes, the system checks if data buyers have permission to retrieve the files. If permission checks are passed, the system will issue charges to buyers based on data file profit models, and then start data downloading.

CESS data users can also set their data file attributes by themselves. On CESS platform, all data file retrieval records are recorded on blockchain and hence are backward traceable. The CESS data rights protection mechanism maintains a recording module to allow users to view their data file retrieval records, providing strong evidence for user data rights protection.

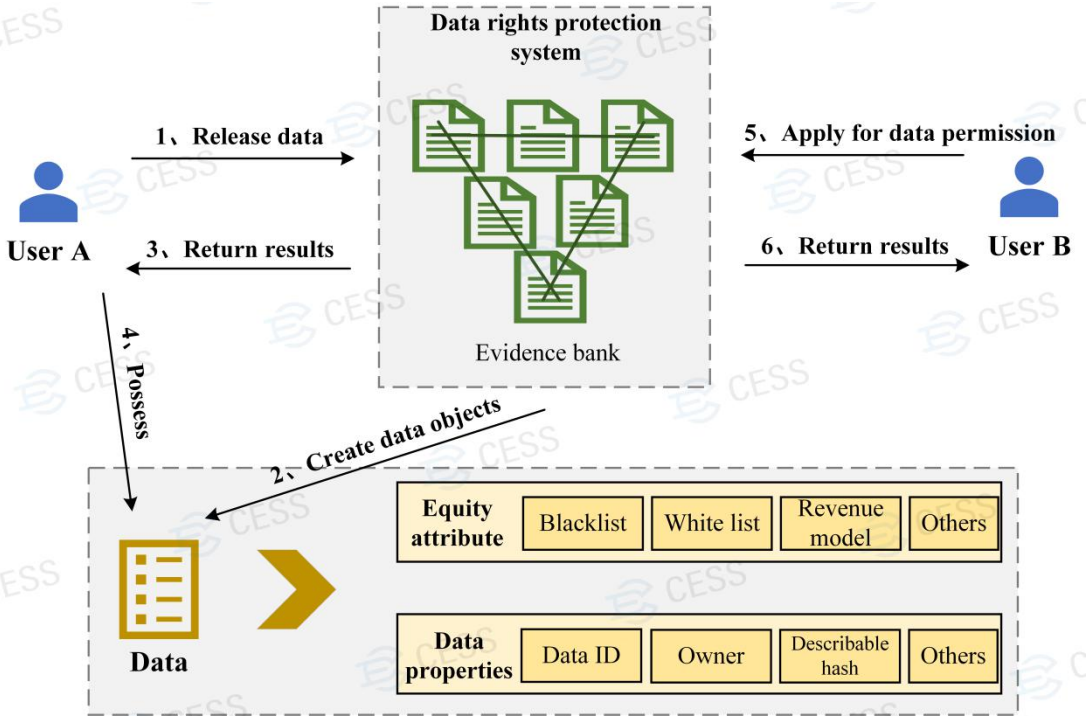

Figure4 Data Right Confirmation and Protection

4. Technical Implementations

4.1 Overall System Architecture

CESS is a decentralized, high speed, secure and scalable cloud data storage network. CESS proposes a novel Random Rotational Selection(R²S) consensus mechanism to achieve low gas fees and rapid transaction processing throughput (10,000TPS). CESS offers large-scale storage capacity, managing billions of data files with up to 100PB space, to meet enterprise level demands. At the same time, CESS provides data services including data rights confirmation and protection. Therefore, our platform not only provides expandable data storages for DAPPs, but also strong data owner rights protection.

As shown in the figure 5, CESS adopts a layered and loosely coupled system architecture, which is divided into blockchain service layer, distributed storage resource layer, distributed content delivery layer and application layer.

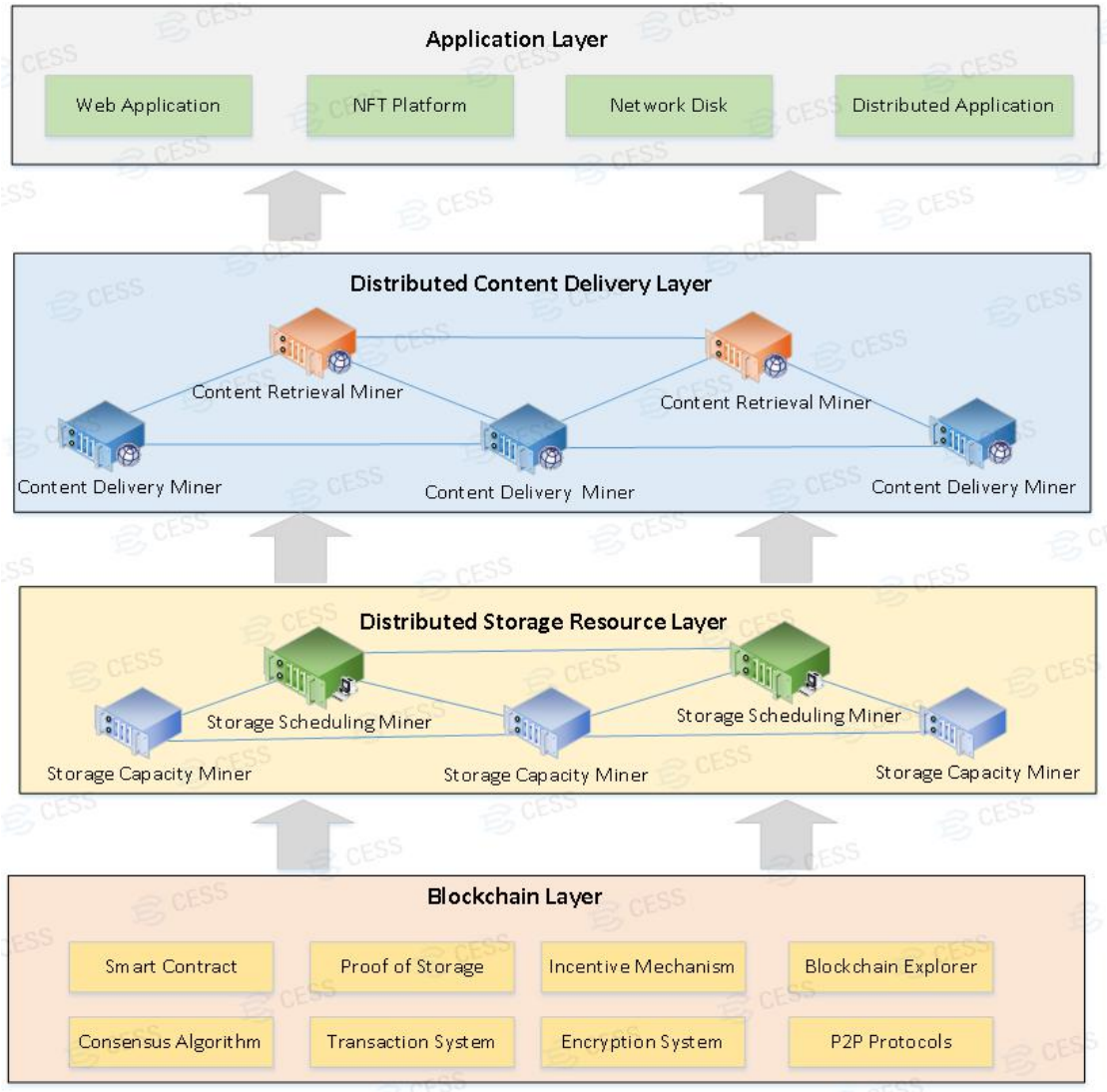

Figure 5 Layered System Architecture

Among them, a Blockchain service layer provides blockchain service of the entire CESS network, including encouraging unused storage resources and computational resources to join the CESS network to provide data storage, data rights confirmation and other services for the application layer. The Distributed storage resource layer uses virtualization technology to realize the integration and pooling of storage resources. The infrastructure consists of storage capacity miners and storage scheduling miners. The distributed content delivery layer uses content caching technology to achieve fast delivery of stored data, which is composed of data index miners and data delivery miners. The application layer provides API/SDK tools to support data storage service, blockchain service, network drive service, enterprise level SDK, AI applications, and etc.

High Performance Blockchain Service Layer: In addition to incentivize unused computing resources and storage resources to join the CESS storage network, it also provides efficient blockchain services. CESS proposes a novel Random Rotational Selection(R^2S) consensus mechanism, together with asynchronous Byzantine consensus algorithm to provide 10,000 TPS capability, as well as Turing's complete smart contract and cross-chain interoperability capability.

Distributed Storage Resource layer: This is the most critical hardware infrastructure layer of the entire CESS network. It manages storage resources contributed by miners around the world, for example, unused or under-utilized servers/desktops/laptops, to build a massive-scale data storage network. This part is composed of storage scheduling nodes/miners and storage capacity nodes/miners. Storage scheduling nodes store meta-data and provide fast data indexing, while storage capacity nodes provide data storage space.

Distributed Content Delivery Layer: To achieve rapid data retrieval for users around the world, we have adopted IPFS' content buffering technology. This network layer is composed of data delivery nodes and data indexing nodes. The data delivery nodes are responsible for data buffering, and the data indexing nodes are responsible for data querying.

Application Service Layer: Provides API/SDK tools to support various applications.

4.2 Blockchain Layer

As shown in Figure 6, the blockchain layer is further divided into six layers: infrastructure layer, data layer, network layer, consensus layer, incentive layer and application layer. The infrastructure layer consists of hardware equipment including servers, network hardware and storage hardware for CESS blockchain. The data layer, which supports scalable data storage, provides various data processing algorithms; The network layer is for node connection, data transfer. It provides load balancing and P2P network protocols and algorithms; the consensus layer provides consensus mechanisms on transactions, with 10,000 TPS processing capacity; The incentive layer is to achieve fair income distribution through smart contracts and other incentive schemes. The application layer supports DAPPs or APPs developed by third-party developers.

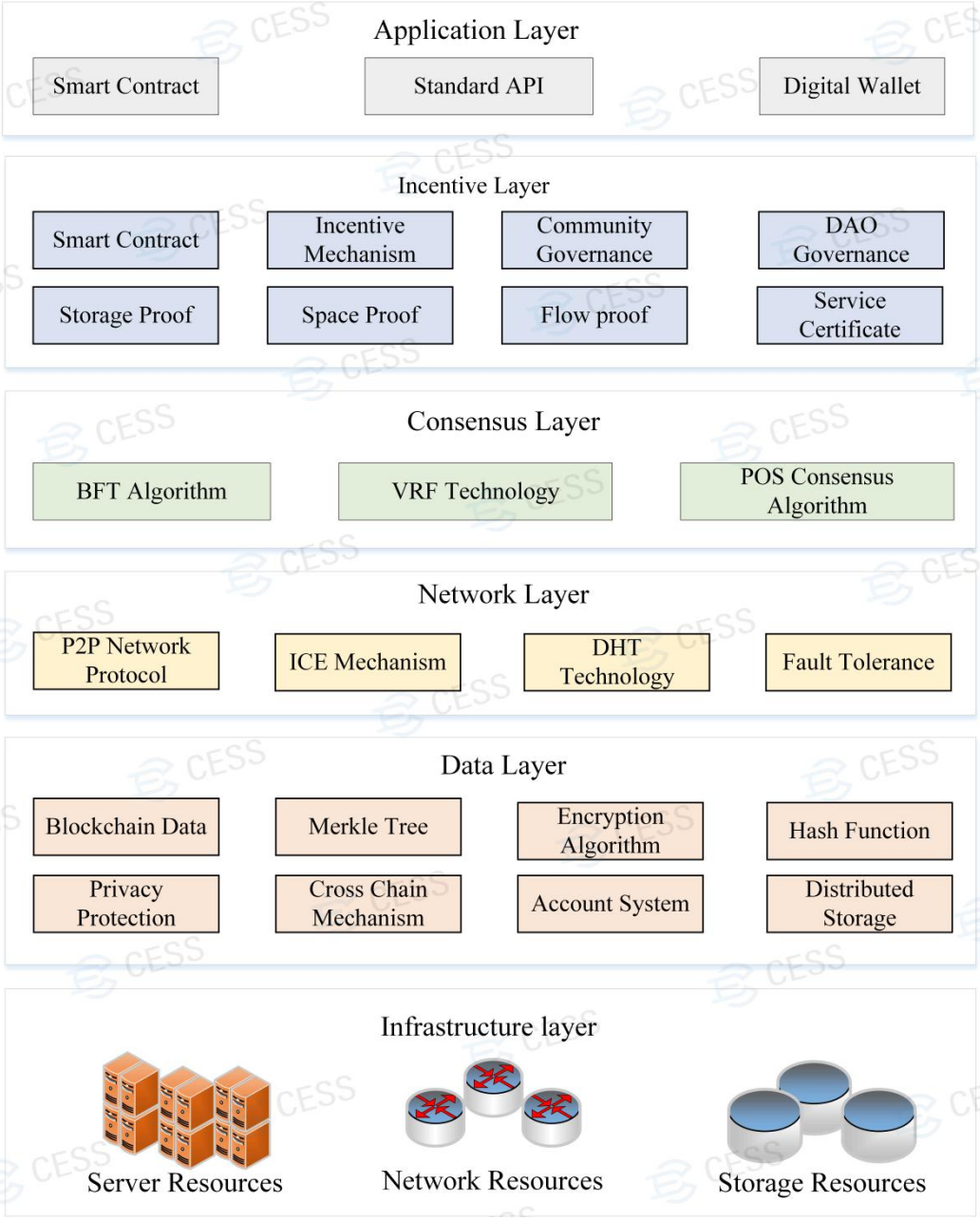

Figure 6 CESS Blockchain Architecture

4.2.1 Infrastructure Layer

In order to support upper layer applications to access storage resources, CESS needs to construct stable and reliable infrastructure facilities. According to Figure 6, CESS invites three types of global resources to join the network: Server type, Network type and Storage type. Server-type resources focus on computing performance and will carry the computing and task scheduling tasks. Network-type resources will provide network bandwidth support. In order to support users' global undifferentiated data access, CESS will use nodes with high network bandwidth to construct a content delivery network to accelerate data retrieval. Storage-type

resources are the kernel part of CESS system. It will require a large part of the project team's operational strength, to attract nodes with storage capacity to join the network, to provide a stable and reliable data storage infrastructure, and to lay a solid foundation for unified scheduling and management of CESS platform resources.

4.2.2 Data Layer

The data layer stores CESS blockchain data, as well as data files from CESS storage clients. To ensure the security and integrity of user data files, encryption algorithms are used for data transmission, storage and verification, such as digital signatures, hash algorithms, Merkle trees, and etc.

Block data: Chain data that records transactions over the entire public chain network. Some nodes need to save block data and run the whole node to ensure the security and stability of the public chain.

Distributed storage: Stores data on geographically distributed devices. It provides efficient, robust and load balanced file access. As shown in Figure 7 below:

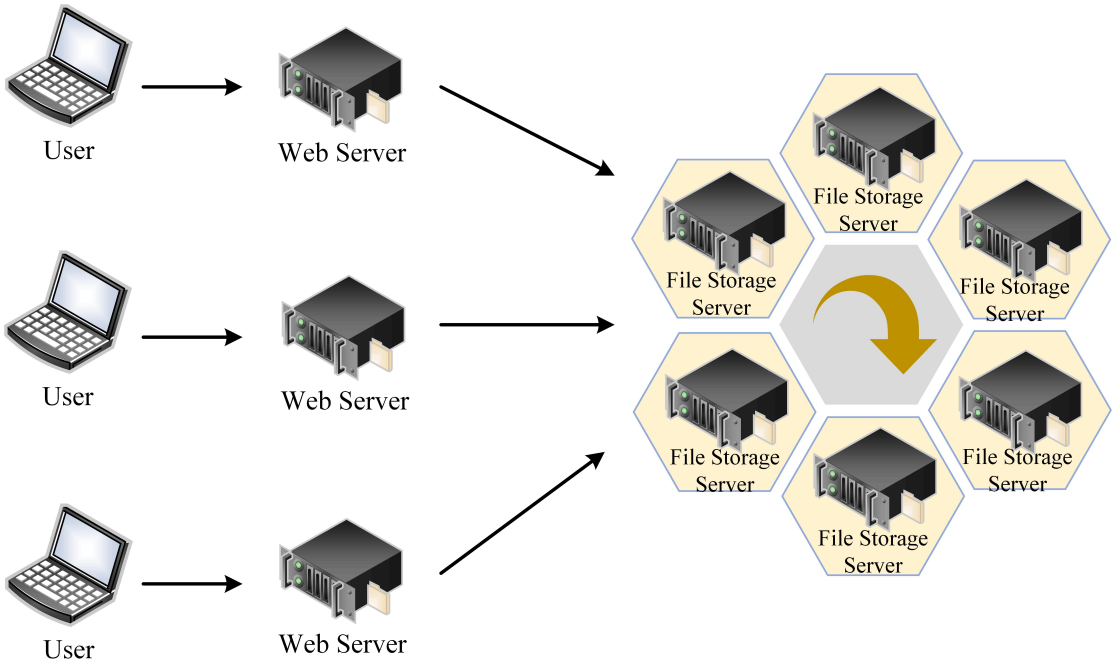

Figure 7 Distributed Storage System

Digital signature: A digital signature (also known as a public key digital signature) is a digital string that can only be forged by the sender of the information. It is also effective proof of the authenticity of the information sent by the sender. It is similar to a physical signature written on paper, but it is implemented using public key encryption technology to identify digital information. A set of digital signatures usually define two complementary operations, one for signatures and the other for verification. We use digital signatures for system authentication, data

integrity verification, etc.

Hash algorithm: A one-way cryptography, that is an irreversible mapping from clear text to cipher text, only the encryption process, no decryption process. A hash function can change any length of input to get a fixed length output, but different inputs have different outputs. This one-way characteristic of the hash function and the fixed length of the output data allow it to generate messages or data. Common hash algorithms are MD5, SHA-1, SHA256, etc. We use a hash algorithm to uniquely identify the data and ensure that it is not tampered with.

Asymmetric encryption: An encryption algorithm that uses a different key for encryption and decryption, also known as public-private key encryption. The public key is a pair of the private keys. If the data is encrypted with the public key, only the corresponding private key can be de-crypted. Because encryption and decryption use two different keys, this algorithm is called an asymmetric encryption algorithm. Commonly used are RSA, ECC, etc. Digital signatures are an application of asymmetric encryption.

Merkle Tree: A Merkel tree (also known as a hash tree) is a tree that stores hash values. The leaves of the Merkle tree are hash values for data blocks, such as files or collections of files. A non-leaf node is a hash of its corresponding child node concatenation string. Get the Merkle tree root of the file from a trusted source before downloading data on the P2P network. Once you get the root, you can get the Merkle tree from other untrusted sources. Check the received Merkle Tree through trusted roots. If the Merkle Tree is corrupt or false, get another Merkle Tree from another source until you get a Merkle Tree that matches the trusted tree root. We can download and immediately verify a branch of Merkle Tree. Because files can be divided into small blocks, if a piece of data is corrupted, simply download it again.

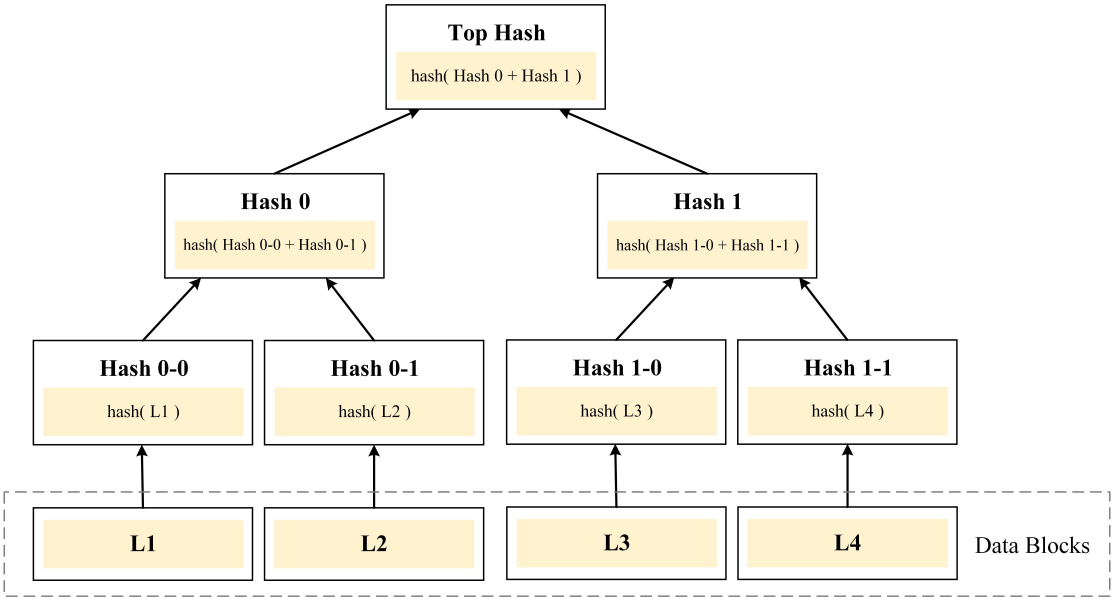

Figure 8 Merkel tree data structure

4.2.3 Network Layer

To ensure efficient access to data in the network, a DHT-based P2P storage network will be built.

P2P network: A peer-to-peer computer network is a distributed application architecture that distributes tasks and workloads among peers. It is a form of networking or a network formed by the peer-to-peer computing model in the application layer. In a P2P network environment, multiple computers connected to each other are in the same position. Each computer has the same functions, and has no master-slave. A computer can act as a server, set up shared resources for use by other computers in the network, and can also act as a workstation. Generally, the whole network does not depend on a dedicated centralized server. There are no dedicated workstations. Each computer in the network can act as both a requestor for network services and respond to requests from other computers to provide resources, services and content.

DHT: A distributed hash table is a distributed storage method. Without the need for a server, each client is responsible for a small range of routing and for storing a small portion of the data, thus enabling the addressing and storage of the entire DHT network. Users who connect to a DHT network are called nodes, and there is a routing record between the nodes, so as long as they are connected to any node already in the DHT network, the client can find more nodes to connect to the network. DHT technology is to enable any machine in the network to perform part of the server's functions, so that users' data are no longer dependent on the server.

ICE: ICE is an object-oriented middleware platform for communication between nodes. ICE provides an RPC protocol that can use either TCP/IP or UDP as the underlying transport mechanism. Nodes do not need to know their implementation. ICE also allows SSL to be used as a transport mechanism to encrypt all communication between nodes.

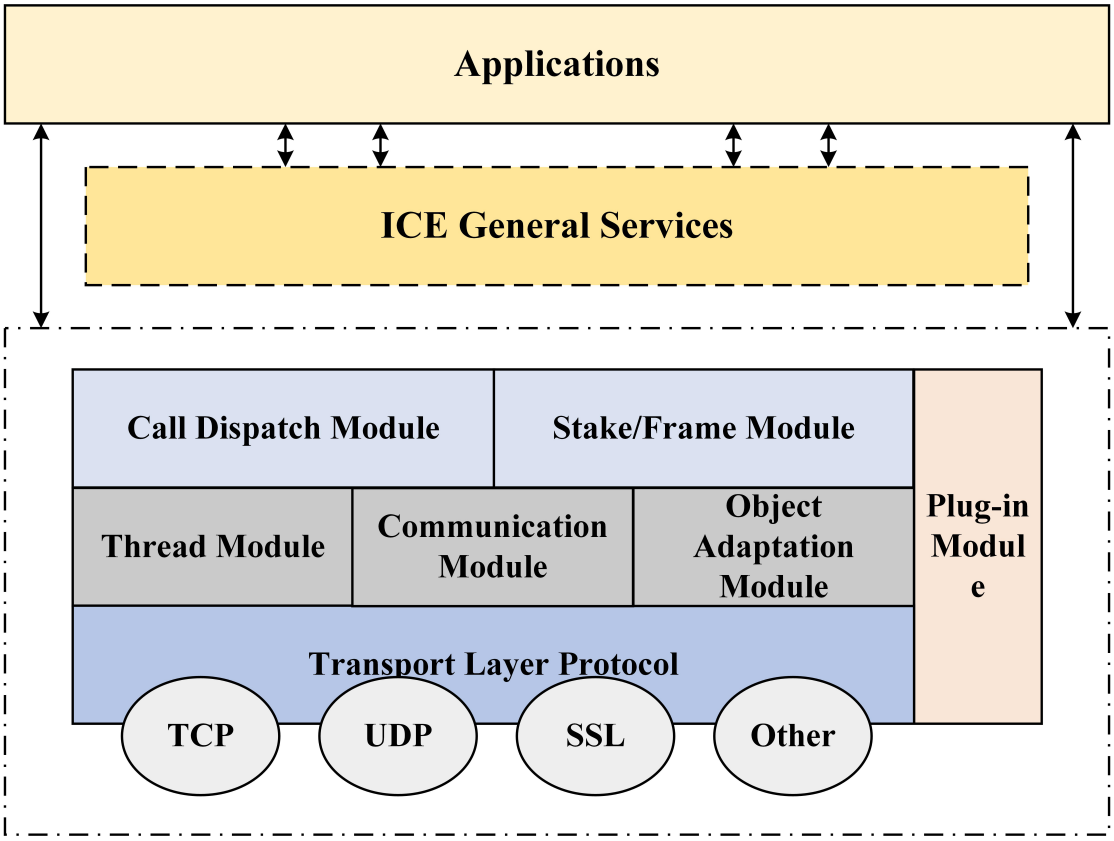

Figure 9 ICE framework

4.2.4 Consensus Layer

In order to ensure that the transactions and activities on the blockchain network can reach a consensus quickly, CESS proposes a novel Random Rotational Selection(R^2S) consensus mechanism based on Byzantine fault tolerance to improve the performance and scalability of the system. There are two types of consensus nodes in CESS network: candidate consensus nodes and on-duty consensus nodes. Theoretically, any node can become a consensus node via staking. There is no limitation to the of number of candidate consensus nodes. In order to improve reliability, CESS will use credit rating method to verify the nodes and select qualified nodes to be candidate consensus nodes. Within each time window, CESS randomly selects next 11 consensus nodes as new on-duty consensus nodes. On-duty consensus nodes will have responsibility for on-chain transaction validation, data packing, and data block generation. The goal of CESS consensus mechanism is to achieve network security, randomness and fairness to miners, and system transparency. The following are the main elements of this mechanism.

Credit rating: the consensus mechanism adopts the health score evaluation model. The module evaluates the health score of the consensus behavior of distributed energy nodes in the platform, the health score of the nodes showing honest & loyalty behavior, which provides the basis for the election of the consensus node committee when changing views, so as to improve the reliability of the consensus node and ensure the authenticity of the data on the link.

Verifiable random function: Based on a verifiable random function, CESS consensus protocol randomly selects active consensus nodes from candidate node pool. This function makes the selection of consensus nodes truly random and unpredictable. To achieve fault tolerant consensus CESS uses an improved algorithm over traditional PBFT, which maintains system consistency and robustness against malicious network attacks.

Efficient consensus algorithm: Based on PBFT algorithm, the CESS introduces node signatures and collection nodes. Messages with node signatures are aggregated and transferred to reduce the network overhead and to implement a highly efficient PBFT algorithm.

Entry and Exit Criteria: CESS defines a set of criteria for network nodes to enter or exit candidate consensus node pool. It implements the function of dynamically adding and removing nodes from active nodes cluster without downtime, which greatly improves the system robustness.

4.2.5 Incentive layer

As a distributed file system, CESS main system resources are storage and network resources. In the CESS network, there are two types of mining nodes: Content Storage Node (CSN) and Content Delivery Node (CDN). The CSN node is responsible for file storage while the CDN node is responsible for file delivery. Miners can provide two types of resources to join the CESS network, and the CESS system will reward the miners with CESS tokens according to their contributions to the network. In order to encourage miners to join and remain in the network, it is necessary to design an incentive mechanism.

- **How to partner with CESS network**

For miners, rewards are similar to "crypto mining". CESS has designed an algorithm, namely, Contribution of Proof (COP) to calculate each miner’s contribution to the network. The Contribution of Proof algorithm is a comprehensive consensus algorithm that considers the factors of miners' storage capacity, network bandwidth and node configuration, to calculate an overall node score. Miners receive rewards in form of CESS tokens, based on their scores.

- **How to earn CESS Tokens**

In order to promote network growth, in addition to the incentive system at the technical level, CESS introduces a main node incentive mechanism. Miners who meet the incentive level will be issued CESS tokens.

1) **Storage mining**:

Miners with storage capacity join either the storage network or content delivery network to earn tokens proportional to their bandwidth and storage capacity.

2) **Consensus mining**:

Miners/nodes with qualified computational resources can deposit collaterals in form of CESS tokens to become candidate consensus nodes. If selected by CESS random consensus mechanism as 11 on-duty nodes, these nodes can earn rewards.

3) **Community contribution**:

To further promote the CESS network, developers, community members and partners can submit their proposals and receive community votes. When a quorum is established, corresponding rewards will be issued from the blockchain system.

4) Token governance will adopt the Decentralized Autonomous Organization (DAO) to achieve on-chain governance capability. CESS community transparently operates the Community Development Fund (CDF) through the votes.

- **Token Distribution**

All incentive related activities are implemented based on smart contracts which include on-chain operations of proof of miners' space and time and reward distribution. This ensures the fairness and transparency of the CESS incentive mechanism.

4.2.6 Application Layer

The API for CESS is designed to enable third-party developers to build a variety of applications, including the following:

- **Private data storage**

As a decentralized network, CESS storage has great advantages for personal private storage needs.

Personal data is sliced, encrypted, and stored on different nodes to ensure privacy protection. Meanwhile, access to user data is securely controlled by the user's unique private key.

- **Enterprise Data Storage**

CESS provides high-performance services for enterprise data storage with significantly low cost.

- **DApps**

Storing application data on a blockchain is expensive for de-centralized applications. Data from smart contracts or other applications can be stored on CESS storage nodes using the CESS API, which can result in significant cost savings.

- **Media Applications**

CESS provides low-cost bandwidth resources, which can effectively reduce the cost of

content delivery. CESS is also equipped with specially optimized scheduling and transmission algorithms for smooth data transmission, enabling and maintaining a high-quality user experience for media applications.

- **Data Exchange**

Digital assets can be traded over the CESS platform. CESS can provide methods to match sellers and buyers and handle transactions safely and reliably without requiring an intermediary. Common applications, such as the application marketplace and content platforms, can benefit from CESS.

- **Database**

CESS can be used as an enterprise database to store large amounts of historical data, replacing traditional local data storage or expensive cloud storage. In addition to enterprise data, CESS can also be used to store public databases.

CESS will also provide the necessary support for other types of storage requirements. In addition, CESS will release open-source code in future. At that time, application enthusiasts and developers will be able to participate in the development of CESS and add support for more applications.

4.3 Distributed Storage Resource Layer

Unlike existing IPFS, and other projects, CESS is designed to build a blockchain-based distributed cloud storage system. The focus is on providing consistent and efficient distributed storage services to clients by effectively managing distributed resources using virtualization technology. CESS utilizes global resources and enables users to access the data network in undifferentiated manner through distributed identity information. In terms of implementation, CESS constructs two types of infrastructure nodes: distributed content buffer nodes and distributed cloud storage nodes. The distributed content buffer network will deliver data to the nearest content buffer node according to the user's geographic location to speed up access. A distributed cloud storage network is designed to provide massive, reliable, and scalable cloud storage services.

- **Data Storage Process**

The process of storing data to CESS network by users will go through several stages, such as production, upload, processing, storage, delivery and destruction. In the production stage, users can implant applications through restful API, SDK and other means to upload data; In the storage phase, based on CESS network resources, intelligent services for pictures, videos and documents can be built to support users to process data online. During the delivery phase, over 10T of network bandwidth can be achieved through a content delivery network. In addition, CESS

supports users to delete data online and the CESS blockchain will keep track of all data operations.

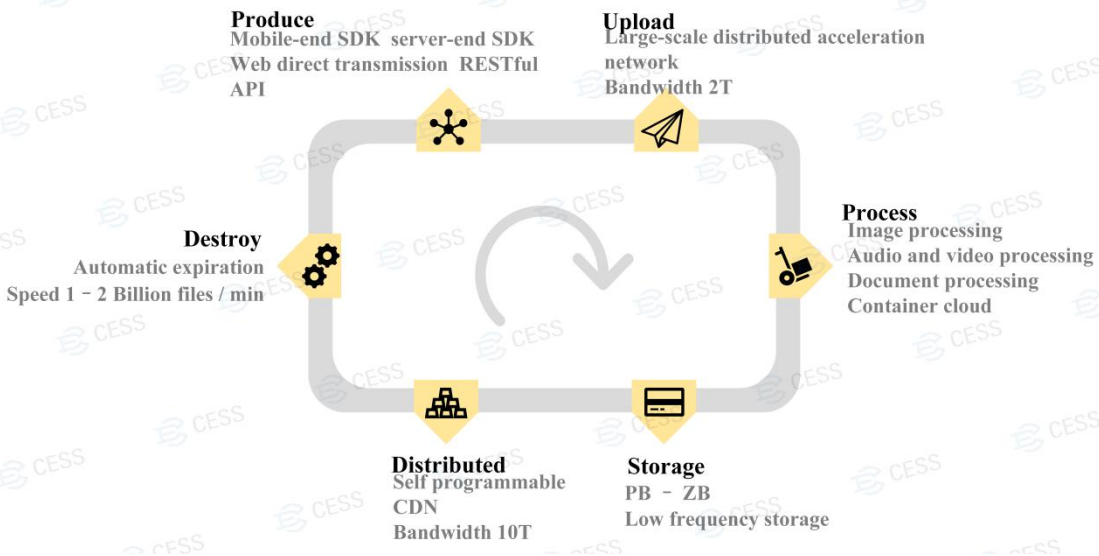

Figure 10 Data Storage Process

- **Distributed Content Delivery Network**

In order to achieve efficient file access, the system effectively combines the advantages of both CDN and P2P technologies. By forming a content delivery network layer, it effectively reduces the number of proxy servers required by the system, increases the capacity of the system, reduces the overall cost, and uses CDN technology to transfer media content to the client's autonomous domain. It also enhances the quality of media access for customers, and improves P2P network performance in a smaller autonomous system. The presence of a high-performance cache proxy server also avoids the "seed" problem in pure P2P networks.

At the same time, on the application side, the stored content in the application will be published on the publishing source node first, and the download service will be continuously provided if the source node is not offline. However, as the number of user downloads from the same source node increases, the bandwidth of that node will be exhausted and the download speed per user will be reduced. With the design of a content delivery network, a large number of tenant nodes in the network begin to save and provide downloads of the same content. As a result, users can download content from multiple nodes, which greatly improves the user experience.

The overall design of the Distributed Content Delivery Network Layer is perfectly combined with blockchain technology. Storage nodes form CDNs with proxy nodes in each region. Proxy nodes form a relatively independent P2P network with the following storage nodes without public network IP. Node contribution awards are issued through smart contracts, forming an autonomous network for development, as shown in Figure 11 :

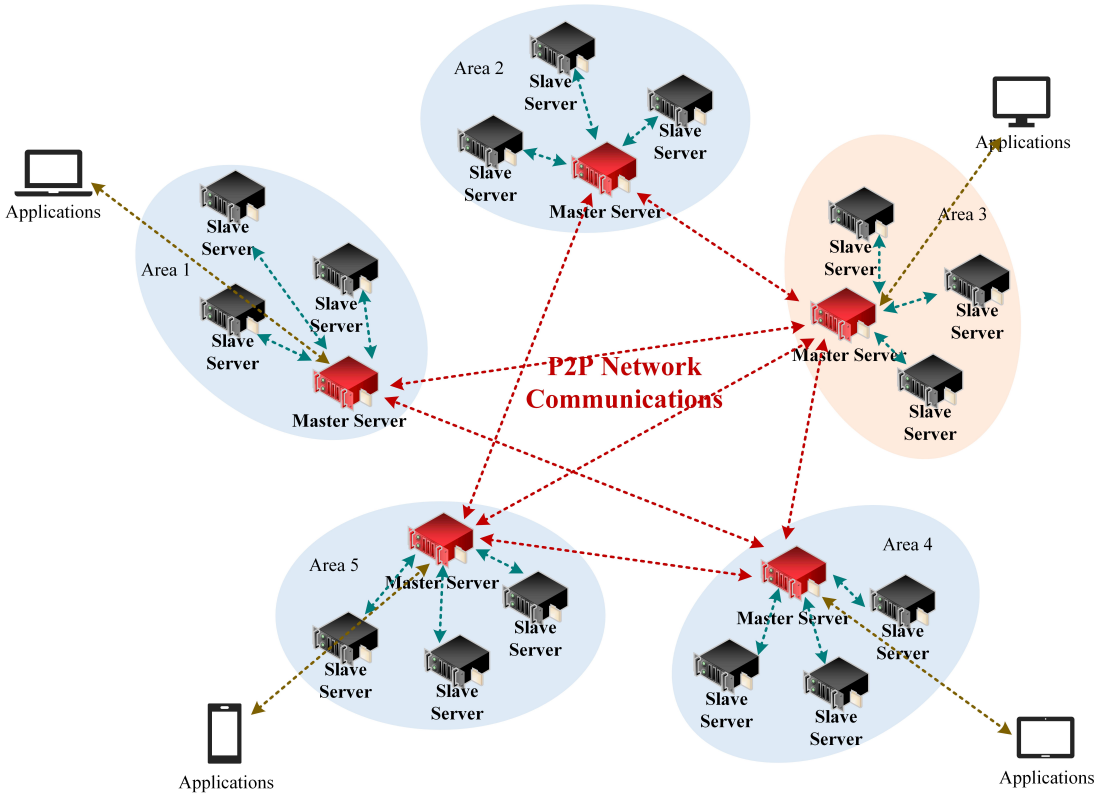

Figure 11 Distributed Content Cache Network

- **Distributed Cloud Storage Network**

To meet different storage needs, we will design and implement a polymorphic data storage access interface to provide storage services in the form of APIs for a variety of applications. As shown in the Figure 12 below, on top of the unified distributed object storage engine, the polymorphic data access service provides object storage, block storage and file system storage for the upper application in a standard API way, providing a comprehensive and friendly data storage service support for the top application.

CESS will provide an improved and reliable object storage service. The upper application calls the object storage service interface. The object storage module automatically completes the mapping of the user object storage space to the lower unified distributed object storage space. User data is stored in the distributed object storage engine as object data.

CESS will provide the block device storage service. The upper application calls the block device service interface. The block storage module automatically completes the mapping of the user's block device operation, data read and write operation to the unified distributed object storage space at the bottom. The users' data on the block device will eventually be stored in the distributed object storage engine as object data, supporting snapshot, cloning and other functions.

For generic file systems, the POSIX file system module provides a POSIX-compliant file system interface, supports both kernel file system and user space file system (FUSE) modes, and

calls the POSIX file system interface by upper applications. The POSIX file system module and the POSIX file system metadata manager (responsible for mapping and transforming POSIX file system space to object storage space) jointly complete the mapping of user's POSIX file operations to the underlying unified distributed object storage space. Users' data in the POSIX file system is ultimately stored in the distributed object storage engine as object data.

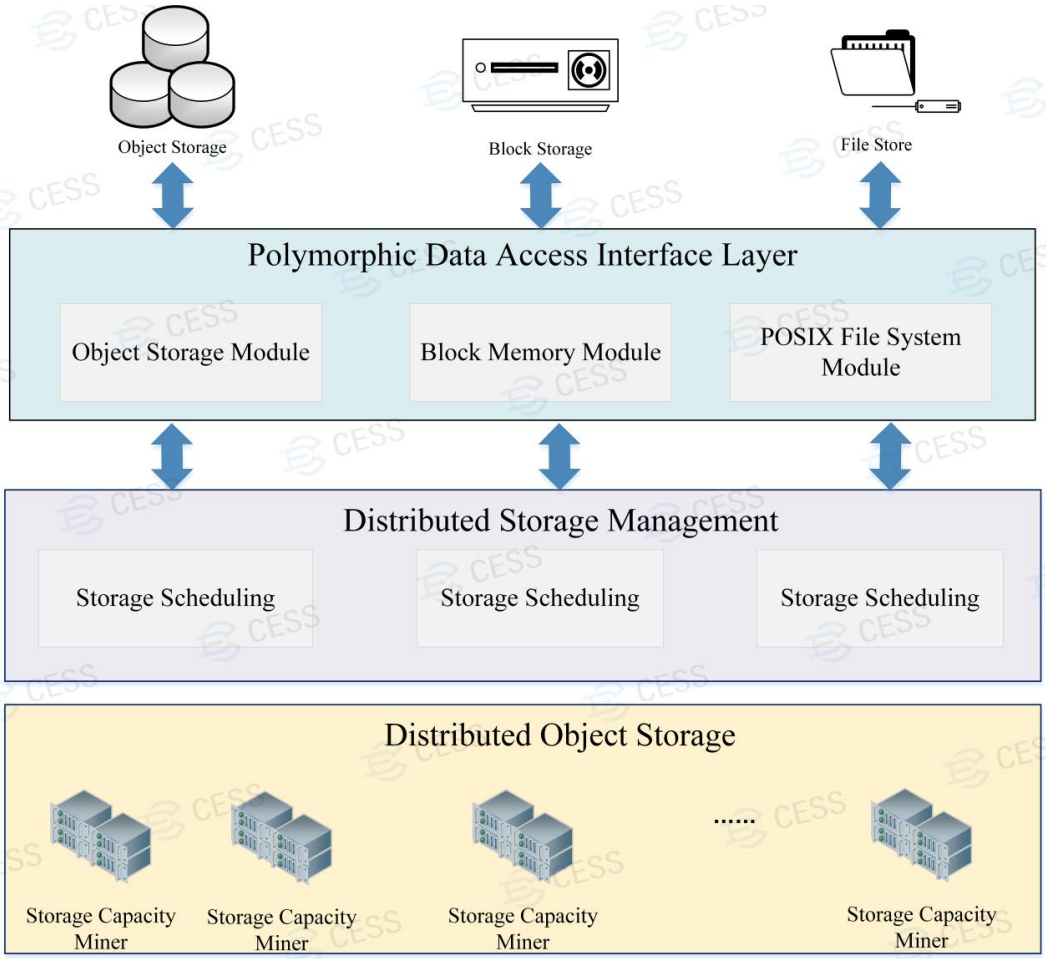

Figure 12 Distributed Storage Network Architecture Design

5. Key Technologies

5.1 Key Technology 1, Multiple-Format Data Rights Confirmation Mechanism (MDRC)

CESS is committed to create a strong data-rights-protected marketplace for data originators. Without proper data rights protection enforcements, a data exchange market will become the best candidate for cyber piracy and will not be able to provide high quality contents to end users. With this in mind, CESS have designed a unique **Multi-format Data Rights Confirmation Mechanism (MDRC)**, which extracts data fingerprint from each data file to generate data certificate ID. By comparing similarities between data fingerprints, the system identifies data lineages of data files, and may take appropriate actions to prevent possible violations, and to provide strong evidences for owners' data rights protection.

CESS MDRC mechanism workflow is shown in the figure below.

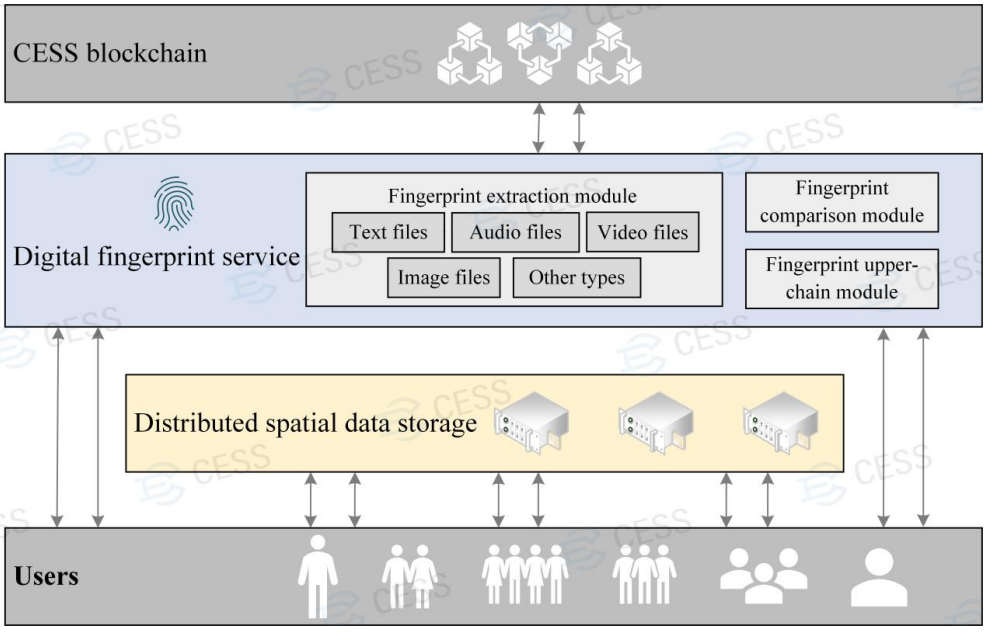

Figure 13 CESS Multi-format Data Fingerprints Extraction Mechanism Architecture

CESS MDRC mechanism is built on the concept of data fingerprints. As illustrated in Figure 14, CESS MDRC mechanism is located in CESS user interface layer, and pre-processes user data before transmitting to data storage nodes. The pre-processing includes: extracting data fingerprints, submitting data fingerprints info to blockchain, and performing data fingerprints comparisons. CESS data fingerprints extraction algorithm is designed to process different data types that require very different extraction methods. It can handle text, photos, audio, video, and other data formats.

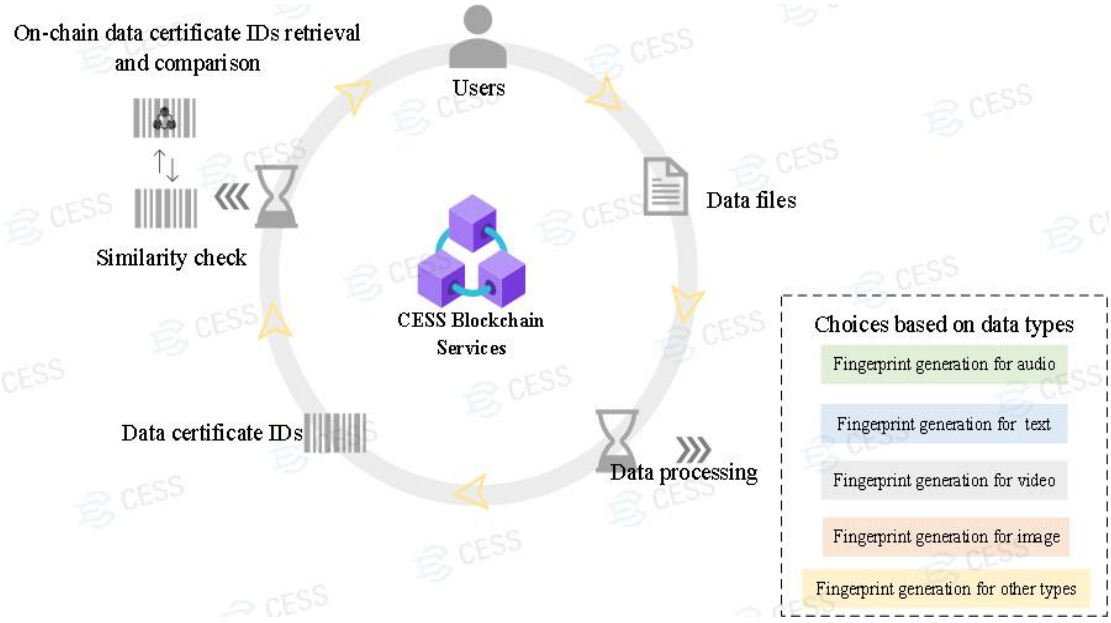

Figure14 CESS (MDRC) Mechanism Workflow

For text data type, advanced word segmentation methods for different natural languages are implemented. Combined with semantic natural language understanding, data fingerprints are generated. For photo data type, data fingerprints extraction is based on characteristics of color, shape, texture, space and etc. And then apply further transformational algorithm to improve fingerprint accuracy. For audio data type, sampling and quantization methods are applied to the original data first, then use the Fast Fourier Transform method to obtain data characteristics. Our algorithm supports extraction of audio intensity feature, time and space, frequency, musical feature, perceptual feature, and so on. For video data type, key video frames are extracted and then processed similarly as photo data type. Besides the above data types, CESS can also process other data types, via MD5 hash or SHA hash functions to obtain data fingerprints.

Once a data file's fingerprint is extracted, the system runs "Simhash" algorithm to calculate similarity hash value as data certificate ID. In Simhash algorithm, similar features are hashed to similar hash values. Similarities are measured by the bitwise hamming distance between the hash values. Simhash function is known for its runtime speed and high accuracy. Based on this method, CESS system detects data lineages and similarities between data files, and provide clients with data rights protection service.

Finally, CESS data rights service can store user date file certificate IDs on blockchain through smart contracts, for further support of data rights confirmation.

5.2 Key Technology 2: Cross-chain Mechanism for Multi-chain Interoperability

As the number of blockchain networks explode, multi-chain coexistence and/or cross-chain collaboration will become increasingly inevitable. Due to different infra-structures of private and public blockchains, blockchains are disconnected and run independently. The isolation hinders

interoperations between different blockchains and greatly limits the development of blockchain networks. Cross-chain technology bridges the gap across multiple blockchain platforms, plays important role in multi-chain interoperability and provides unlimited opportunities for the growth of networks. CESS seeks to provide a cross-chain interoperability solution by implementing an integrated cross-chain relay mechanism, to support digital asset transfer, information exchange and application collaboration between different blockchain platforms. Our solution enables interconnections between different blockchains so that clients can transfer values without intermediaries or 3rd parties, hence reducing transaction costs.

In the CESS network, cross-chain relay and parallel chains provide the infrastructure to achieve cross-chain interoperability with other homogeneous and heterogeneous chains, respectively. Among homogeneous chains, the security mechanisms, consensus algorithms, network topology and block validation logics are compatible, therefore the implementation of cross-chain interoperability is relatively easier. Generally, route forwarding based on cross-chain relay can achieve transaction transmission and data exchange between different chains. The cross-chain interoperability between heterogeneous chains is much more complex. Message validations and cross-chain interactions between untrusted blockchains can be achieved by cross-chain-relay-based state validations and synchronized consensus methods. The CESS cross-chain interoperability mechanism is shown in the figure below.

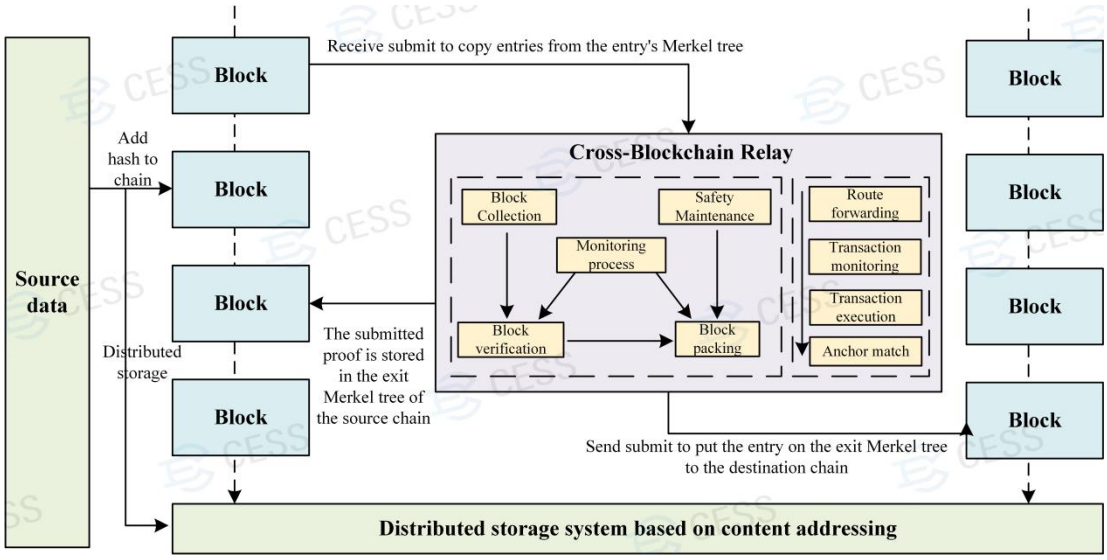

Figure 15 CESS Cross-chain Mechanism

The CESS cross-chain mechanism focuses on the basic inter-blockchain protocol standardization. It achieves standardization in many aspects, including cross-chain messages input & output path, message authentication, unified message format, message validation proof and cross-chain transaction execution result proof. Our mechanism builds a solid foundation for cross-chain operation security.

With regard to multi-chain communication and data consistency validation, cross-chain relay approach, via a relay component and a proof transformation component, enables realization of complete cross-chain inter-operations. CESS cross-chain mechanism workflow is as follows: First, each blockchain obtains a unique own identifier given by the protocol, to be used as message sender and receiver identity. The blockchain of ledger sender submits message data to the relay component and the proof transformation component to convert the data to a self-described data package in normalized format. The data package is then transmitted to the receiver chain. The receiver side's relay component extracts the ledger and proof data and submits to its blockchain. The receiver blockchain validates the ledger and executes transactions. The workflow is shown in the figure below.

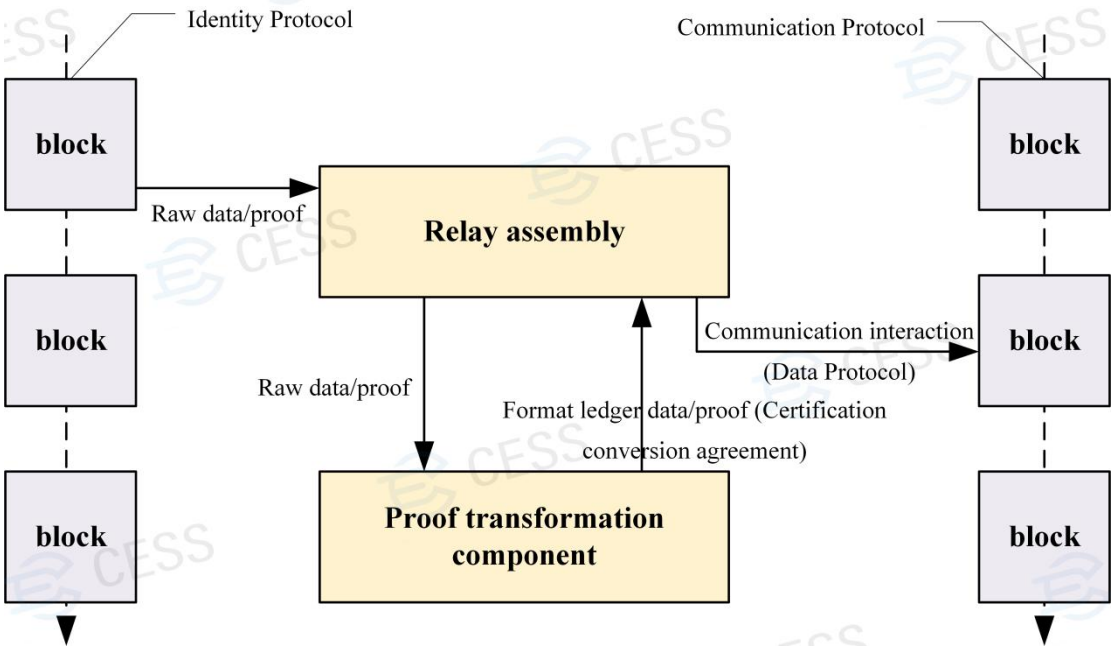

Figure 16 CESS Cross-chain Data Proof and Communication Architecture

The identity protocol identifies a blockchain in these attributes: chain identity, chain type, data model, data content, on-chain proof, root of validation, etc. The identity protocol allows two blockchains to establish mutual recognition. Without altering the data semantics, the transformation protocol converts data types, data proofs, and root of trust. The data protocol allows mutual recognition of data from different blockchains, to enable data validation. Finally, the communication protocol supports smart contracts to exchange information with each other, across different blockchains.

5.3 Key Technology 3, Proxy Re-encryption

To ensure data security, all user data stored on the CESS are usually encrypted first and then distributed to multiple storage nodes. One of our most important goals is to enable data sharing securely on CESS platform without having data contents exposed. We have designed a proxy

re-encryption mechanism that allows users to trade or share data files without leaving data contents publicly readable. Data files, when they are uploaded, are marked either private or public. For private data files, they are encrypted after sharded, then sent to storage nodes to store. When data file owners authorize to transfer the files to other users, CESS uses proxy re-encryption mechanism to re-encrypt data segments stored on nodes, and allow only the authorized users to use private keys to retrieve data files.

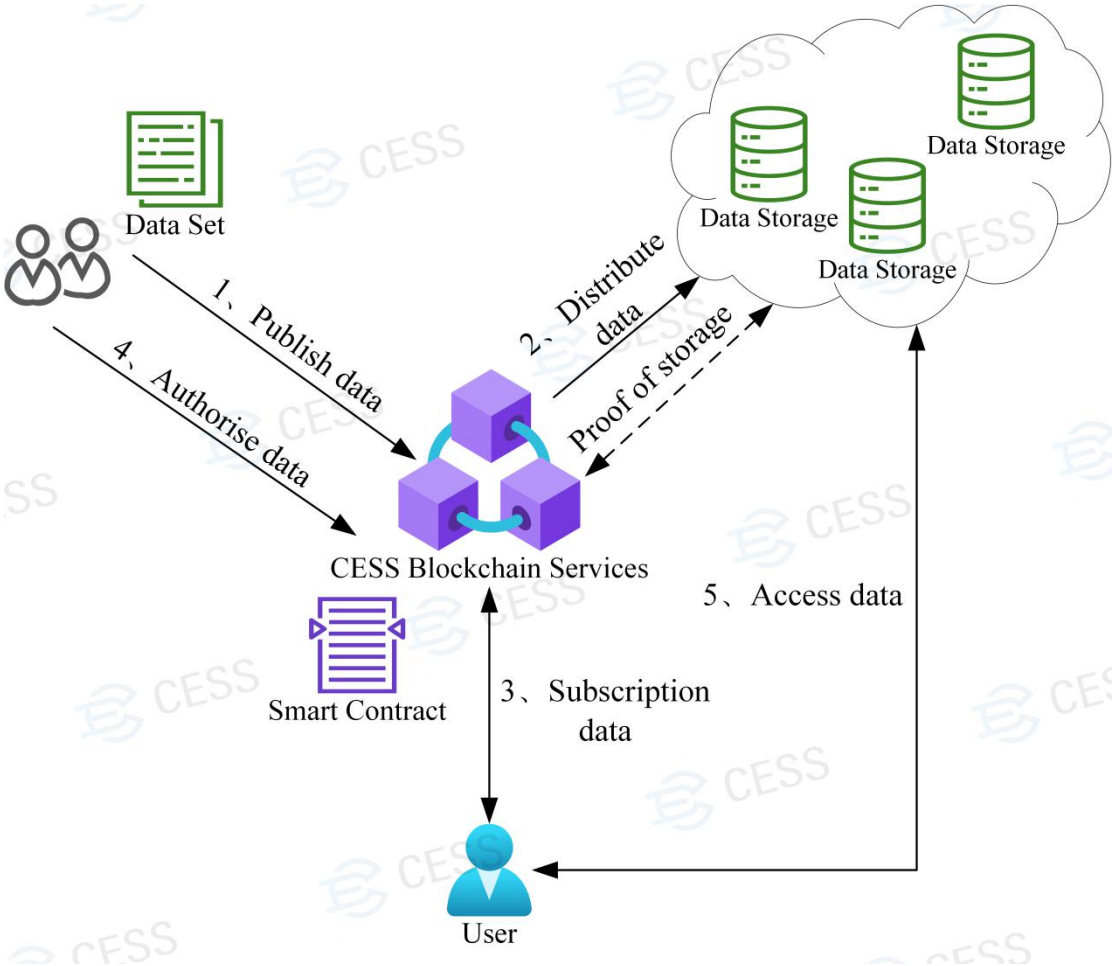

Figure 17 CESS Proxy Re-encryption

5.4 Key Technology 4, Multiple Data Storage Proof Schemes

As a decentralized P2P network, the most important system task is to manage untrusted nodes to ensure data security and integrity. In response to this, CESS has implemented various interactive schemes to verify and prove that miners have indeed stored and maintained the data as they are assigned to. These schemes are also needed to determine miner incentives and penalties. CESS data storage proof schemes include: Proof of Replication (PoRep), Proof of SpaceTime (PoSt), Proof of Data Reduplication and Recovery (PoDR2), Proof of Flow (PoF), and Proof of Available storage (PoAs).

First, when a user stores a file, the system uses the PoRep scheme to guarantee that miners

have replicated the data as assigned. The PoRep scheme is an interactive proof algorithm that requires a storage node to provide a proof to a verifier node, proving that users' data has been copied and stored on the dedicated physical storage. The PoRep scheme has the ability to prevent Sybil attack, outsourcing attacks and generation attacks.

Secondly, in order to verify that data files indeed remain on storage nodes during contract period of files, the Proof of SpaceTime (PoSt) scheme is implemented. PoSt can be understood as continuous proof of replication. Storage nodes must continuously generate certificates, and periodically submit certificates. If storage nodes do not submit certificates in time during the submission cycle, the nodes will not get rewards for the period, and the credit scores of the nodes will be reduced, so are the miners' income.

Thirdly, CESS introduces a new scheme, Proof of Data Reduplication and Recovery (PoDR2), to guarantee that the system always holds multiple copies of user data files to be used. Here is how it works: A user data file is replicated, by default, to three identical copies. For each file copy, meta-data (tags) for verification are generated and submitted to the CESS chain, which will be used as the reference of the PoDR2 proof scheme. Data files copies are sliced into small data segments and are distributed to storage nodes to store. During the lifecycle of data files, miners must provide proof of integrity to verifiers. As illustrated below, there are two phases: initialization phase and verification phase. In the initialization phase, meta-data (tags) for PoDR2 scheme are generated (steps 2 & 3); data segments are distributed to storage nodes (steps 4 & 5); meta-data (tags) are sent to CESS blockchain (step 6). In the verification phase, verifier nodes and storages nodes request and provide PoDR2 integrity certificates periodically (steps 2 & 3).

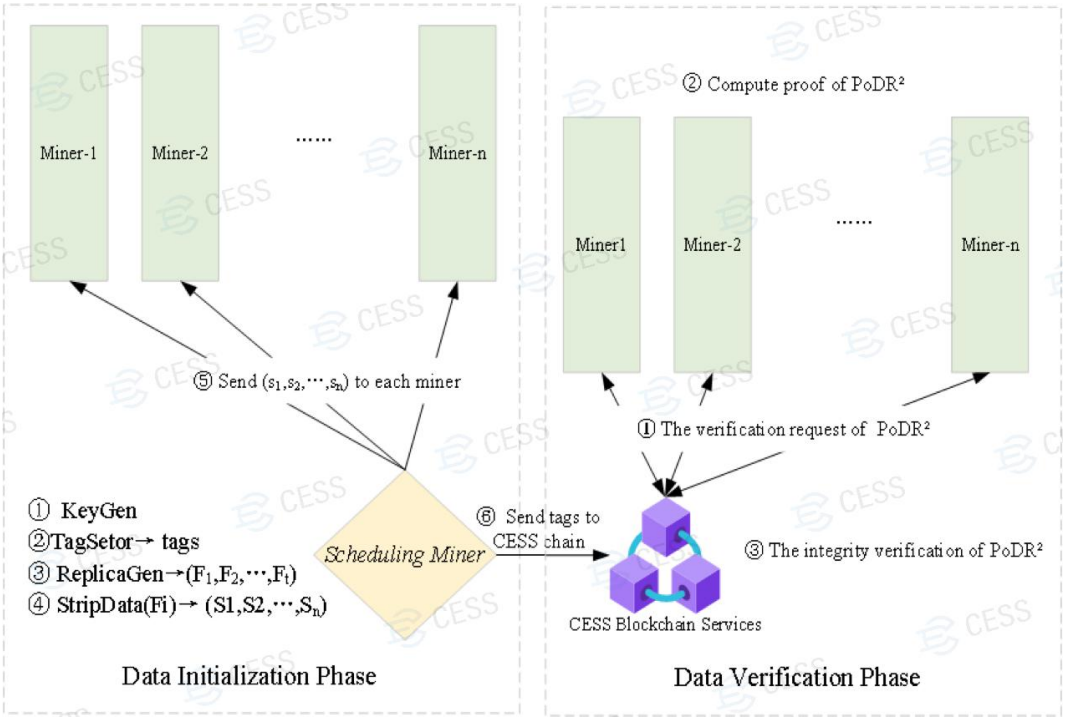

Figure 18 CESS Poof of Data Reduplication and Recovery (PoDR2)

Additionally, CESS has implemented a traffic proof algorithm, Proof of Flow (PoF), to measure and calculate the traffic bandwidth contributed by nodes. In PoF, storage nodes are required to periodically report incoming and outgoing traffic load to verifier nodes, therefore prove node contributions to the network.

Lastly, considering the fluctuation of network environment, CESS uses Proof of Available Storage scheme (PoAs) to verify that nodes have sufficient storage capacity and stability. On one hand, CESS periodic checks nodes to obtain physical storage status; on the other hand, this information is used as one factor in calculating nodes' credit scores. Nodes with high credit scores have higher priorities to be selected to store data files.

6. Security Mechanisms

CESS takes strict security measures to ensure the integrity and reliability of its stored data, and the security of transactions on blockchain.

6.1 Data Security

CESS guarantees user data security from three aspects: data availability, data integrity and data privacy. As described in previous chapters, all users' data files are stored as encrypted data segments; CESS has implemented a fault tolerant erasure coding method to protect data completeness against node failure and other malicious attacks. The CESS multiple proof schemes ensure the data integrity of each network node.

6.2 Consensus Security

Blockchain, as a de-centralized distributed public database, are maintained jointly by distributed nodes using cryptographic protocols. Byzantine attacks are ones in which an attacker controls a number of authorized nodes in a communication network and arbitrarily interferes with or destroys the network, thus preventing a consensus among the blockchain nodes. It might happen that the data on the CESS blockchain are purged during an attack.

To this end, CESS platform builds a hybrid and efficient consensus module. The PBFT algorithm is an effective fault-tolerant consensus algorithm that can accommodate up to one-third of malicious nodes in the network. When there are f Byzantine nodes (malicious nodes) in the system, the entire network must have 3f+1 replica node to ensure that the entire network can make correct judgments. This effectively prevents malicious behavior on the chain.

6.3 Transaction Security

To regulate the use of smart contracts and to avoid the abuse of CESS storage and computing resources, CESS has designed a functional module to monitor and audit the blockchain transactions. As shown in below figure, CESS transaction audit module is a comprehensive data analysis function based on data on blockchain, private key management and transaction management. It provides a visualization of decentralized transaction execution, and transaction monitoring and auditing functionality.

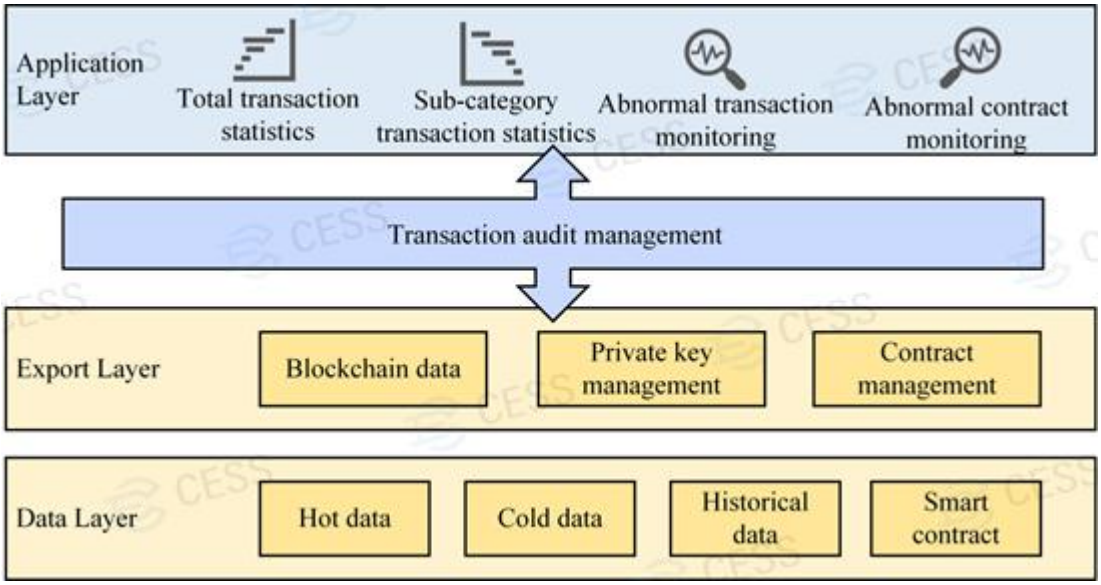

Figure 19 Transaction Audit Framework Diagram

The transaction audit items include:

1) Total number of user transactions. This is to monitor the daily number of transactions of each external account.
2) Total number of transactions for each transaction type. This is to monitor the daily number of transactions for each transaction type, each external account.
3) Abnormal transaction user accounts. Monitor abnormal user accounts that are not registered on blockchain middleware platform.
4) Abnormal transaction execution. Monitor on-chain transaction execution and transactions not on white-list (not registered on blockchain middleware platform).

7. Economic Model

7.1 Roles and Functions

The CESS network operations require a variety of roles to participate in, including storage miners and consensus miners.

Storage miners, including content storage miners and content delivery miners, are responsible for storage network construction, storage and mining, and participating in storage market transactions. Storage miners provide data storage and earn rewards by proving their data storage. Content delivery miners cache and deliver data segments to requesters, and earn rewards too.

Consensus miners are responsible for verifying network transactions and storage miners' work, and for producing blocks of CESS chain. CESS Random Rotational Selection(R^2S) consensus mechanism selects 11 nodes during a given cycle.

7.2 Storage Capacity Model

In order to ensure the reasonable profits of storage minors and to truly achieve the fairness and benefits of storage miners, the CESS network has built a complete storage capacity model evaluation system, and mathematically measures each miner's performance. The system calls this measurement the "credit score" and rewards the miner according to the range of credit score. Indicators that affect a miner's credit score are as follows:

- Basic Operation Indicators

  1. Node Configuration

  2. How long the node is online

  3. Upload and download bandwidth of the node

- Resource Contribution Indicators

  1. Size of storage files

  2. Node's contribution volume to network traffic

These are the existing indicators to build the model. Subsequently, indicators will be continuously enriched to improve the storage capacity model, through AI machine learning, self-adjustment and improvement.

7.3 Storage Award

1) Evaluation of Basic Operating Indicators

Verify with PoAs algorithm and rate the available storage service of the node.

2) Assessment of Resource Contribution Indicators

Storage file size: The system uses the PoRep and PoSt algorithms.

The contribution traffic of a node network is mainly the traffic between the nodes. The traffic proof algorithm (PoF) is used.

The storage nodes of the CESS network and the rewards of the storage miners are allocated reasonably through their contributions, and the contribution value R is determined by their cumulative storage proof as follows:

$$R = (\alpha f(PoSt) + \beta f(PoRep) + rf(PoF) + df(PoAs)) * x$$

x is the staking parameter, if the cumulative contribution of two miners is equal, the miners who serve longer in the future will be assigned a higher staking parameter and thus a higher mining reward. The default values for each proven scale factor are shown in Table 1 below:

Scale factor	describe	Default value
α	PoSt	40%
β	PoRep	20%
r	PoF	30%
d	PoAs	10%

Table 1 Default scale factor values for each demonstration

During the early deployment of CESS, it is expected that the amount of data stored and storage transactions will be low. In order to encourage new miners to join the network and provide available storage services, the PoAs scale factor will be increased during this period. As storage increases, the scale factor for PoAs decreases, while the scale factor for other storage certificates will be increased.

7.4 CESS Token Allocation

- 15%, Initial contributors, linear vesting for 6 years
- 55%, Miners, linear vesting, halved every 4 years
- 10%, Community/DAO/incentives and advertisements
- 5%, Cooperative partners, DAO
- 5%, Reserved for emergency use and future ecology development
- 10%, Financing for future development

8. Decentralized Transactions and Storage Mining

8.1 Storage Markets: Verifiable and Trusted Markets

On commercial storage market, there is an industry chain of "storage suppliers to applications to end users". CESS will improve this industry chain and create an open trading market for clients. In the CESS economy, the storage market is a verifiable and trusted trading market where customers (buyers) can purchase low-cost storage space directly from the CESS storage system to store data.The CESS storage market agreement is based on the following:

- Placing Orders

Storage price is open and transparent. Clients can decide their own order prices based on market situations, and submit orders to CESS chain. Only blockchain-approved orders can be accepted by the system. Once orders are accepted, they cannot be modified.

- Storage miners allocating resources

In order to maintain the stability of the storage market and prevent bad behaviors from storage miners, storage miners must stake a certain number of tokens in proportion to their storage size to system token pool. The transaction fees paid by clients are put in the token pool too. Only after the verification process is completed, the transaction fees will be transferred to the storage miners' accounts.

- Self-organized processing

Storage miners must periodically report and prove the integrity of their stored data to verifiers. Verifier nodes must conduct verifications.

8.2 Storage mining: commercial implementation of decentralized storage

The implementation of decentralized storage requires miners to store valid data not random data. The storage miners need to become qualified and to stake a collateral in CESS tokens. If miners do not keep their promise and data integrity can't be verified, the system will deduct penalties from their accounts. The transaction fees will be refunded to clients. If data integrity verifications are successful, the miners are rewarded CESS tokens in their accounts.

8.3 Storage Brokers: Improving Resource Integration in the Economy

Decentralization is not absolutely equivalent to disintermediation, especially in scenarios such as enterprise-level resource allocation, where the matching of individual storage miners and storage demand in the trading market is obviously inefficient and uneconomic. The emergence of storage brokers solves the problem. They can provide and match large scale storage demands with storage resources. The existence of broker service will greatly improve the efficiency of the storage market.

9. Community Governance

The CESS Decentralized Autonomous Organization (DAO) is represented by a set of computer programs with transparency. CESS token holders within the ecosystem can become members of CESS DAO of the highest order authority, independent of any centralized agency. Each member can participate in issuing proposals and voting resulting in the governance of the community. In the CESS ecology, the community governance structure is developed with the formation of community consensus to have a fair, just, and effective governance, and with important suggestions for the ecological development to drive the CESS Decentralized cloud storage and data network ecology to their full potential.

The assets management of CESS DAO monitored in the market, is achieved in an open, transparent manner as with community governance. CESS DAO strives to achieve decentralization with the openness of rules, codes, the entire incentive system, and the regulatory mechanism to be publicly available. Everyone in the decentralized community can participate equally with transparency in the community governance and operation.

10. Future Outlook

Don Tapscott, one of the world's leading authorities on the impact of technology on business and society, once said "The technology likely to have the greatest impact on the next few decades has arrived. And it's not social media, it's not big data, it's not robotics, it's not even AI. So, what if there were not only an Internet of information, what if there were an Internet of value – some kind of vast, global, distributed ledger, running on millions of computers and available to everybody. And where every kind of asset, from money to music, could be stored, moved, transacted, exchanged and managed, all without powerful intermediaries? You will be surprised to learn that it's the underlying technology of digital currencies like Bitcoin. It's called the Blockchain. Now it's not the most sonorous word in the world, but I believe that this is now the next generation of the Internet, and that it holds vast promise for every business, every society and for all of you, individually."

Quoting Don Tapscott, CESS, is a firm believer in the digital economy brought forth by the Blockchain technology, fully devoted to promote the interconnection of data in an open, impartial, and secure network environment and extremely motivated towards the development of Web 3.0.

Reference

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260.

[2] Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." OSDI. Vol. 99. No. 1999. 1999.

[3] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance and proactive recovery." ACM Transactions on Computer Systems (TOCS) 20.4 (2002): 398-461.

[4] Bach, Leo Maxim, Branko Mihaljevic, and Mario Zagar. "Comparative analysis of blockchain consensus algorithms." 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018.

[5] Gramoli, Vincent. "From blockchain consensus back to Byzantine consensus." Future Generation Computer Systems 107 (2020): 760-769.

[6] Milutinovic, Mitar, et al. "Proof of luck: An efficient blockchain consensus protocol." proceedings of the 1st Workshop on System Software for Trusted Execution. 2016.

[7] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[8] Data object store and server for a cloud storage environment, including data deduplication and data management across multiple cloud storage sites, 2012.

[9] Lakshman, Avinash, and Prashant Malik. "Cassandra: a decentralized structured storage system." ACM SIGOPS Operating Systems Review 44.2 (2010): 35-40.

[10] Lipton, Alexander, and Adrien Treccani. Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics. World Scientific, 2021.

[11] Bhutta, Muhammad Nasir Mumtaz, et al. "A Survey on Blockchain Technology: Evolution, Architecture and Security." IEEE Access 9 (2021): 61048-61073.

[12] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).

[13] Karagiannis, Thomas, et al. "Transport layer identification of P2P traffic." Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. 2004.

[14] Pouwelse, Johan, et al. "The bittorrent p2p file-sharing system: Measurements and analysis." International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2005.

[15] Balakrishnan, Hari, et al. "Looking up data in P2P systems." Communications of the ACM 46.2 (2003): 43-48.

[16] Rhea, Sean, et al. "Handling churn in a DHT." Proceedings of the USENIX Annual Technical Conference. Vol. 6. 2004.

[17] Rhea, Sean, et al. "OpenDHT: a public DHT service and its uses." Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications. 2005.

[18] Micali, Silvio, Michael Rabin, and Salil Vadhan. "Verifiable random functions." 40th annual symposium on foundations of computer science (cat. No. 99CB37039). IEEE, 1999.

[19] Dodis, Yevgeniy, and Aleksandr Yampolskiy. "A verifiable random function with short proofs and keys." International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2005.

[20] Bitansky, Nir. "Verifiable random functions from non-interactive witness-indistinguishable proofs." Journal of Cryptology 33.2 (2020): 459-493.

[21] David, Bernardo, et al. "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2018.

[22] Lamport, Leslie. "Paxos made simple." ACM Sigact News 32.4 (2001): 18-25.

[23] Chang, Fay, et al. "Bigtable: A distributed storage system for structured data." ACM Transactions on Computer Systems (TOCS) 26.2 (2008): 1-26.

[24] Dimakis, Alexandros G., et al. "Network coding for distributed storage systems." IEEE transactions on information theory 56.9 (2010): 4539-4551.

[25] Rawat, Ankit Singh, et al. "Locality and availability in distributed storage." IEEE Transactions on Information Theory 62.8 (2016): 4481-4493.

[26] Hasan, Ragib, et al. "A survey of peer-to-peer storage techniques for distributed file systems." International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II. Vol. 2. IEEE, 2005.

[27] Herlihy, Maurice. "Atomic cross-chain swaps." Proceedings of the 2018 ACM symposium on principles of distributed computing. 2018.

[28] Wood, Gavin. "Polkadot: Vision for a heterogeneous multi-chain framework." White Paper 21 (2016).

[29] Amiri, Mohammad Javad, Divyakant Agrawal, and Amr El Abbadi. "Caper: a cross-application permissioned blockchain." Proceedings of the VLDB Endowment 12.11 (2019): 1385-1398.

[30] Garoffolo, Alberto, Dmytro Kaidalov, and Roman Oliynykov. "Zendoo: a zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains." 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2020.

[31] Green, Matthew, and Giuseppe Ateniese. "Identity-based proxy re-encryption." International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2007.

[32] Ateniese, Giuseppe, et al. "Improved proxy re-encryption schemes with applications to secure distributed storage." ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1-30.

[33] Ateniese, Giuseppe, Karyn Benson, and Susan Hohenberger. "Key-private proxy re-encryption." Cryptographers' Track at the RSA Conference. Springer, Berlin, Heidelberg, 2009.

[34] Libert, Benoit, and Damien Vergnaud. "Unidirectional chosen-ciphertext secure proxy re-encryption." IEEE Transactions on Information Theory 57.3 (2011): 1786-1802.

[35] Rumelhart, David E., et al. "Sequential thought processes in PDP models." Parallel distributed processing: explorations in the microstructures of cognition 2 (1986): 3-57.

[36] Curtmola, Reza, et al. "MR-PDP: Multiple-replica provable data possession." 2008 the 28th international conference on distributed computing systems. IEEE, 2008.

[37] Shacham, Hovav, and Brent Waters. "Compact proofs of retrievability." International conference on the theory and application of cryptology and information security. Springer, Berlin, Heidelberg, 2008.

[38] Juels, Ari, and Burton S. Kaliski Jr. "PORs: Proofs of retrievability for large files." Proceedings of the 14th ACM conference on Computer and communications security. 2007.

[39] Barsoum, Ayad F., and M. Anwar Hasan. "Provable multicopy dynamic data possession in cloud computing systems." IEEE Transactions on Information Forensics and Security 10.3 (2014): 485-497.

[40] Sadowski, Caitlin, and Greg Levin. "Simhash: Hash-based similarity detection." Technical report, Google (2007).

[41] Uddin, Md Sharif, et al. "On the effectiveness of simhash for detecting near-miss clones in large scale software systems." 2011 18th Working Conference on Reverse Engineering. IEEE, 2011.