CESS

A Blockchain-based Data Value Network Infrastructure

White Paper v0.9.1

CESS Lab

July 2024

LEGAL DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "LEGAL DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU ARE STRONGLY ADVISED TO CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER SUCCESS DAO CORP (THE **COMPANY**), ANY OF THE PROJECT CONTRIBUTORS (THE **CESS PROJECT CONTRIBUTORS**) WHO HAVE WORKED ON CESS NETWORK (AS DEFINED HEREIN) OR PROJECT TO DEVELOP CESS NETWORK IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR AND/OR VENDOR OF $CESS TOKENS (OR SUCH OTHER RE-NAMED OR SUCCESSOR TICKER CODE OR NAME OF SUCH TOKENS) (THE **DISTRIBUTOR**), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THE PAPER, DECK OR MATERIAL RELATING TO $CESS (THE **TOKEN DOCUMENTATION**) AVAILABLE ON THE WEBSITE AT HTTPS://CESS.CLOUD/ (THE **WEBSITE**, INCLUDING ANY SUB-DOMAINS THEREON) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED OR COMMUNICATED BY THE COMPANY OR ITS REPRESENTATIVES FROM TIME TO TIME.

Project purpose: You agree that you are acquiring $CESS to participate in CESS network and to obtain services on the ecosystem thereon. The Company, the Distributor and their respective affiliates would develop and contribute to the underlying source code for CESS network. The Company is acting solely as an arms' length third party in relation to the $CESS distribution, and not in the capacity as a financial advisor or fiduciary of any person with regard to the distribution of $CESS.

Nature of the Token Documentation: The Token Documentation is a conceptual paper that articulates some of the main design principles and ideas for the creation of a digital token to be known as $CESS. The Token Documentation and the Website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, any offer to sell any product, item, or asset (whether digital or otherwise), or any offer to engage in business with any external individual or entity provided in said documentation. The information herein may not be exhaustive and does not imply any element of, or solicit in any way, a legally-binding or contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Token Documentation or the Website includes information that has been obtained from third party sources, the Company, the Distributor, their respective affiliates and/or the CESS Project Contributors have not independently verified the accuracy or completeness of such information. Further, you acknowledge that the project development roadmap, platform/network functionality are subject to change and that the Token Documentation or the Website may become outdated as a result; and neither the Company nor the Distributor is under any obligation to update or correct this document in connection therewith.

Validity of Token Documentation and Website: Nothing in the Token Documentation or the Website constitutes any offer by the Company, the Distributor, or the CESS Project Contributors to sell any $CESS (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Token Documentation or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of CESS network. The agreement between the Distributor (or any third party) and you, in relation to any distribution or transfer of $CESS, is to be governed only by the separate terms and conditions of such agreement.

The information set out in the Token Documentation and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of $CESS, and no digital asset or other form of payment is to be accepted on the basis of the Token Documentation or the Website. The agreement for distribution of $CESS and/or continued holding of $CESS shall be governed by a separate set of Terms and Conditions or Token Distribution Agreement (as the case may be) setting out the terms of such distribution and/or continued holding of $CESS (the Terms and Conditions), which shall be separately provided to you or made available on the Website. The Terms and Conditions must be read together with the Token Documentation. In the event of any inconsistencies between the Terms and Conditions and the Token Documentation or the Website, the Terms and Conditions shall prevail.

Deemed Representations and Warranties: By accessing the Token Documentation or the Website (or any part thereof), you shall be deemed to represent and warrant to the Company, the Distributor, their respective affiliates, and the CESS Project Contributors as follows:

(a) in any decision to acquire any $CESS, you have not relied and shall not rely on any statement set out in the Token Documentation or the Website;

(b) you shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that $CESS may have no value, there is no guarantee or representation of value or liquidity for $CESS, and $CESS is not an investment product nor is it intended for any speculative investment whatsoever;

(d) none of the Company, the Distributor, their respective affiliates, and/or the CESS Project Contributors shall be responsible for or liable for the value of $CESS, the transferability and/or liquidity of $CESS and/or the availability of any market for $CESS through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to participate in the distribution of $CESS if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card or permanent visa holder of a geographic area or country

(i) where it is likely that the distribution of $CESS would be construed as the sale of a security (howsoever named), financial service or investment product and/or

(ii) where participation in token distributions is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, and the People's Republic of China); and to this effect you agree to provide all such identity verification document when requested in order for the relevant checks to be carried out.

The Company, the Distributor and the CESS Project Contributors do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness, or reliability of the contents of the Token Documentation or the Website, or any other materials published by the Company or the Distributor). To the maximum extent permitted by law, the Company, the Distributor, their respective affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Token Documentation or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective acquirors of $CESS should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the distribution of $CESS, the Company, the Distributor and the CESS Project Contributors.

$CESS Token: $CESS are designed to be utilized, and that is the goal of the $CESS distribution. In particular, it is highlighted that $CESS:

(a) does not have any tangible or physical manifestation, and does not have any intrinsic value (nor does any person make any representation or give any commitment as to its value);

(b) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other digital asset) or any payment obligation by the Company, the Distributor or any of their respective affiliates;

(c) does not represent or confer on the token holder any right of any form with respect to the Company, the Distributor (or any of their respective affiliates), or their revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or license rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to CESS network, the Company, the Distributor and/or their service providers;

(d) is not intended to represent any rights under a contract for differences or under any other contract the purpose or intended purpose of which is to secure a profit or avoid a loss;

(e) is not intended to be a representation of money (including electronic money), payment instrument, security, commodity, bond, debt instrument, unit in a collective investment or managed investment scheme or any other kind of financial instrument or investment;

(f) is not a loan to the Company, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Company, the Distributor or any of their respective affiliates, and there is no expectation of profit nor interest payment; and

(g) does not provide the token holder with any ownership or other interest in the Company, the Distributor or any of their respective affiliates.

Notwithstanding the $CESS distribution, users have no economic or legal right over or beneficial interest in the assets of the Company, the Distributor, or any of their affiliates after the token distribution.

For the avoidance of doubt, neither the Company nor the Distributor deals in, or is in the business of buying or selling any virtual asset or digital payment token (including $CESS). Any sales or distribution of tokens would be performed during a restricted initial period solely be for the purpose of obtaining project development funds, raising market/brand awareness, as well as community building and social engagement; this is not conducted with any element of repetitiveness or regularity which would constitute a business.

To the extent a secondary market or exchange for trading $CESS does develop, it would be run and operated wholly independently of the Company, the Distributor, the distribution of $CESS and CESS network. Neither the Company nor the Distributor will create such secondary markets nor will either entity act as an exchange for $CESS.

Informational purposes only: The information set out herein is only conceptual, and describes the future development goals for CESS network to be developed. In particular, the project roadmap in the Token Documentation is being shared in order to outline some of the plans of the CESS Project Contributors, and is provided solely for **INFORMATIONAL PURPOSES** and does not constitute any binding commitment. Please do not rely on this information in deciding whether to participate in the token distribution because ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of the Company, the Distributor or their respective affiliates, and is subject to change. Further, the Token Documentation or the Website may be amended or replaced from time to time. There are no obligations to update the Token Documentation or the Website, or to provide recipients with access to any information beyond what is provided herein.

Regulatory approval: No regulatory authority has examined or approved, whether formally or informally, any of the information set out in the Token Documentation or the Website. No such action or assurance has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Token Documentation or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

Cautionary Note on forward-looking statements: All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Company, the Distributor and/or the CESS Project Contributors, may constitute forward-looking statements (including statements regarding the intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Token Documentation, and the Company, the Distributor as well as the CESS Project Contributors expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

References to companies and platforms: The use of any company and/or platform names or trademarks herein (save for those which relate to the Company, the Distributor or their respective affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the

Token Documentation or the Website to specific companies and platforms are for illustrative purposes only.

English language: The Token Documentation and the Website may be translated into a language other than English for reference purpose only and in the event of conflict or ambiguity between the English language version and translated versions of the Token Documentation or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Token Documentation and the Website.

No Distribution: No part of the Token Documentation or the Website is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Company or the Distributor. By attending any presentation on this Token Documentation or by accepting any hard or soft copy of the Token Documentation, you agree to be bound by the foregoing limitations.

Abstract

The abundant growth of data residing in the immense expanse of the digital world evokes apprehension about centralization, especially regarding who truly owns and safeguards our data. A substantial chunk of this data remains untapped, shrouded in mystery and vulnerability. CESS has crafted a tapestry of decentralized solutions that breathe life into the digital realm in response to these pressing concerns. At the heart of CESS lies a constellation of innovative creations: the Decentralized Network Infrastructure, the Blockchain-based Online Data Sharing Platform, and the CESS AI Gap - each a beacon of hope amidst the looming shadows cast by centralized control.

The **Decentralized Network Infrastructure** is a dynamic web of interconnected peers, harnessing the power of blockchain technology[1] to eliminate the constraints imposed by traditional governance structures. This innovative system leverages a token-based economy and taps into the available resources within the network to fortify data security and access rights, revolutionizing the landscape of decentralized data storage.

The **Blockchain-based Online Data Sharing Platform** introduces a pioneering business framework that offers inexhaustible scalability for future endeavors, by leveraging a token economy centered around CESS which is supported by a milliseconds high-speed Content Decentralized Delivery Network (**CD²N**). This business model addresses critical aspects like data privacy, security, stability, rights verification, and rights preservation within the community.

CESS AI Gap, a Byzantine-Robust[2] Circuit from the CESS network, is designed to resist Byzantine attacks while ensuring privacy and data sovereignty. Through the CESS AI Gap, users within each CESS node can collaboratively train a shared AI model without disclosing their raw data. This innovative technology leverages smart contracts to delegate the execution of local models to various computing nodes within the CESS network, ranging from GPUs to GPU clusters or even Decentralized GPU Computation Web3 DePINs. CESS AI Gap revolutionizes secure and efficient machine learning processes in decentralized environments by enabling collaborative AI training without compromising data integrity.

1. Introduction

As the digital realm advances, it's a breeding ground for groundbreaking technologies and a myriad of challenges. These challenges span a wide array of issues, from data vulnerability and security to privacy concerns, transmission lags, network congestion, and escalating costs. The dawn of the AI era has further amplified these issues, with the risk of leaks involving highly sensitive data, the imposition of government privacy regulations, and the complexities of data access permissions. These elements are not just hurdles but also a call for a heightened focus on the ethical use of data.

To tackle these hurdles, we must cultivate innovative approaches that preserve data integrity, guarantee robust data assurance, and manage data sovereignty and

privacy with finesse. We need networks that can scale dynamically and adapt to changing demands, and we must steadfastly defend the rights of data owners. The use of AI must be approached with both precision and a commitment to moral principles.

CESS is a blockchain-powered decentralized cloud storage network with native CD²N, where users and creators share data on-chain, and builders can create and deploy DApps. Offering the most optimal Web3 solution for storing and retrieving high-frequency dynamic data, CESS reshapes the value distribution and circulation of data assets whilst ensuring data sovereignty and complete user privacy. Our vision is to create a secure, transparent, and high-throughput decentralized data value network. Operating as a public blockchain network with distributed storage capabilities and high-speed CD²N, CESS promotes AI advancements through web3 protocols. It serves as an innovative solution for entropy reduction in our ever-chaotic digital landscape:

$$\Delta CESS = \frac{\int \delta Q}{T} < 0$$

1.1 **Decentralized Network Infrastructure**

CESS is dedicated to developing a new global decentralized cloud storage system and a value delivery network. This network infrastructure is transparent, efficient, and provides equal opportunity for the community[3]. It enables:

- **Data interoperability:** Through cross-platform, cross-collaboration, and cross-format interactions.
- **Data trading market tracing and monitoring:** Ensures transparency and fairness.
- **Data profit rewards:** Fair and transparent rewards for network participation.

CESS adopts a phased approach to implement the above goals. In the CESS protocol, participating nodes contribute their idle resources and are motivated through a token-based economy. These nodes offer data storage, computational power, and network bandwidth coordinated and overseen by the CESS protocol. This setup provides clients with secure and efficient access to cloud data storage services via a public interface. Additionally, the protocol facilitates the connection of network nodes to establish a vast decentralized cloud storage system capable of supporting hundreds of Petabytes of storage that can scale on demand.

1.2 **Blockchain-based Online Data Sharing Platform**

CESS Introduces the Multi-format Data Rights Confirmation Mechanism (MDRC), a cutting-edge solution designed to safeguard data ownership rights across various data formats. This innovative system enables the secure uploading, sharing, and trading of digital assets within a protected marketplace, unlocking fresh perspectives and opportunities for assessing the true worth of digital assets.

This data sharing platform based on these technologies is designed for developers, creators, and consumers, fostering a collaborative environment for growth and innovation. It supports diverse content types such as literature, art, music, videos, and media.

1.3 **CESS AI GAP**

In traditional federated learning (FL), a central aggregator is typically required to maintain and update the global model. However, CESS AI Gap offers a unique approach by operating as an aggregator-free FL system on a blockchain network, making it completely decentralized. Through the use of smart contracts, CESS AI Gap can effectively handle round division, model aggregation, and task updates within FL processes. Leveraging the extensive storage capabilities of CESS, various organizations can securely store their data on CESS storage nodes, ensuring privacy and data integrity through the Proof of Data Reduplication and Recovery ($PoDR^2$) mechanism.

2. **Architecture**

2.1 **Overview**

The architecture of the CESS network integrates a decentralized cloud storage network and a CD^2N, offering highly customizable solutions for decentralized data storage and real-time sharing, specifically tailored for modern high-frequency dynamic data storage and retrieval needs. We meet enterprise users' demands for massive storage capacity, location-based storage selection (LBSS), hierarchical permission management, and other custom requirements and/or compliance needs.

Supporting applications including but not limited to personalized medicine to decentralized social media and responsible AI, CESS empowers industries with data integrity, privacy, availability and sovereignty.

CESS adopts layered and loosely coupled system architecture, which is divided into **3** main components: **CESS Protocol Suite, XESS AI Protocol Suite** and **Interface**.

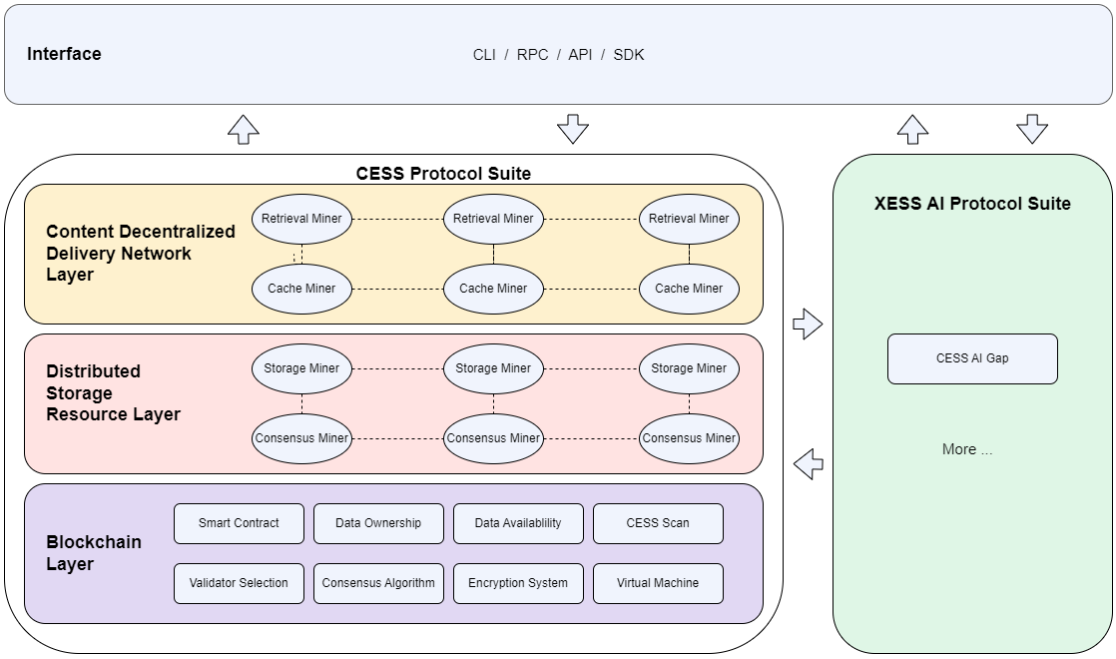

Figure 1 CESS Architecture

CESS Protocol Suite includes 3 layers: Blockchain Layer, Distributed Storage Resource Layer and Content Decentralized Delivery Network Layer.

- The **Blockchain Layer** provides blockchain service for 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 **Content Decentralized Delivery Network Layer** utilizes content caching technology to ensure rapid distribution of stored data, involving both data index miners and data delivery miners in the process.

The **XESS AI Protocol Suite** leverages advanced AI technologies to enable secure, privacy-preserving collaborative model training across the CESS network.

- The core component of the XESS AI Protocol Suite is the **CESS AI Gap**, which integrates federated learning mechanisms, allowing participants to train shared models without sharing their original data. Utilizing smart contracts, it delegates computational tasks to various nodes, ensuring efficient use of resources while maintaining data sovereignty. This suite enhances the network's AI capabilities, supporting complex AI applications and facilitating industry-wide collaboration without compromising data privacy.

The **Interface** serves as a bridge for interaction and communication between different parts of **CESS Protocol Suite** and **XESS AI Protocol Suite**, defining a set of rules and conventions that enable various components to work together and achieve the overall functionality of CESS. It also facilitates the creation, management,

and interaction with other outside blockchain networks or web3 DApps.

2.2 **CESS Protocol Suite**

2.2.1 **Blockchain Layer**

CESS has its own native blockchain, which has the following main technology stacks: physical stack, network stack, data stack, consensus stack and incentive stack.

- **The physical stack** consists of hardware equipment including servers, network hardware, and storage hardware.
- **The network stack** enables communication, load balancing, and data transfer between nodes across the network.
- **The data stack** supports scalable data storage and provides various data processing algorithms.
- **The consensus stack** provides protocols that work together to find consensus among the nodes.
- **The incentive stack** is responsible for distributing benefits through proof algorithm modeling and precise mathematical calculations.

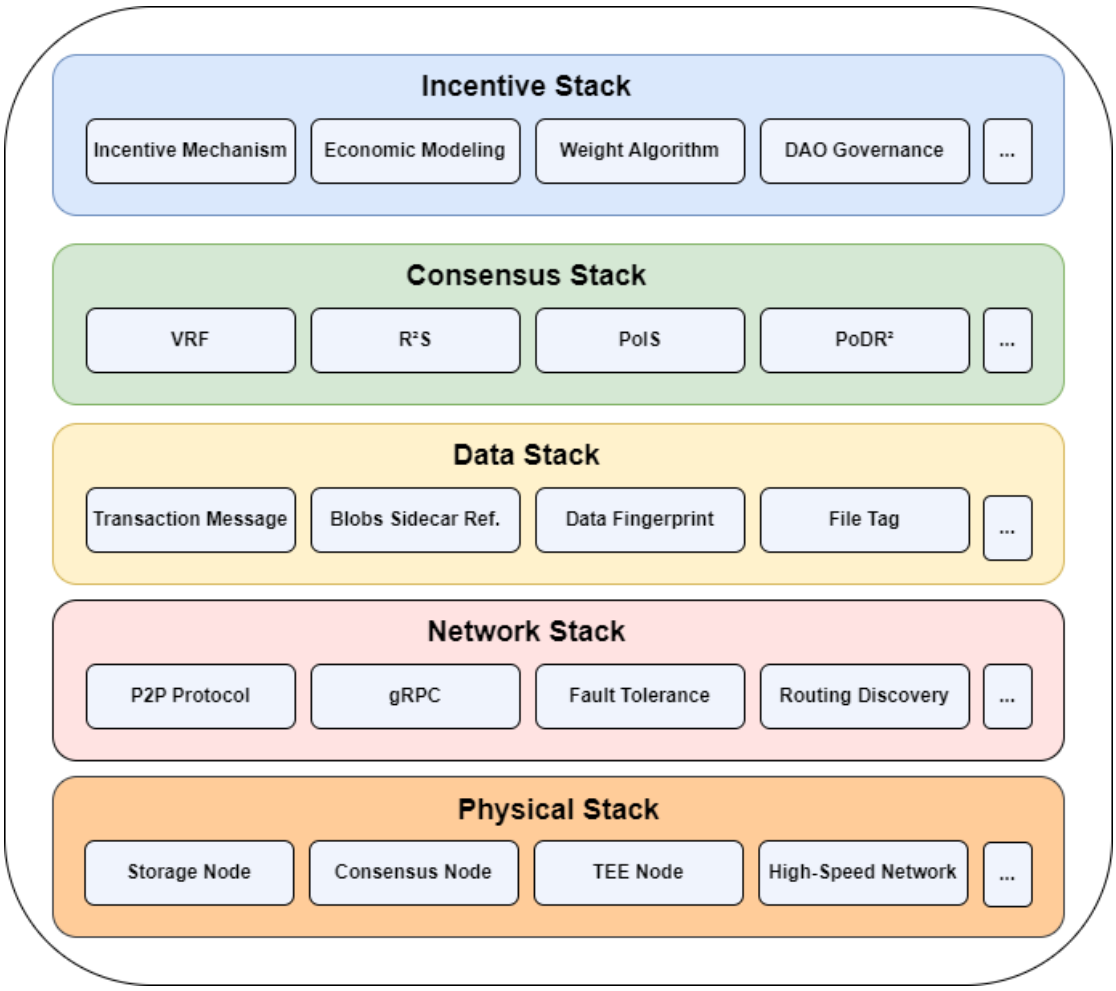

Figure 2 Blockchain Layer Technology Stack

2.2.1.1 **Infrastructure Stack**

As shown in Figure 2, CESS provides three types of global resources: computer resources, network resources, and storage resources.

- **Computer resources:** focus on computing performance and task scheduling.
- **Network resources:** provide network bandwidth and communication channels.
- **Storage resources:** the kernel part of the CESS system, providing stable and reliable storage service.

2.2.1.2 **Network Stack**

CESS uses Distributed Hash Table (DHT) technology[4] within a peer-to-peer (P2P) network[5], facilitating communication between nodes through the P2P protocol. Information and responsibilities are shared directly among network-connected nodes, with routing details kept up-to-date between them. This setup allows users to effortlessly locate and establish connections with new nodes providing they are already part of the DHT network through another node.

2.2.1.3 **Data Stack**

The data stack stores blockchain data and files' meta-data. To ensure the security and integrity of user files during data transmission, storage, and verification, various industry-ready tools are used, such as digital signatures, hashing algorithms, Merkle tree, etc.

2.2.1.4 **Consensus Stack**

To achieve rapid consensus on transactions and activities within the blockchain network, CESS employs a block authoring method called **Random Rotational Selection** (**R²S**). By integrating **R²S** with **GRANDPA** (**G**host-based **R**ecursive **AN**cestor **D**eriving **P**refix **A**greement), every node can collectively agree on the state of the chain at a specific moment at a given timestamp.

2.2.1.5 **Incentive Stack**

The storage modes manage file storage and the cache modes handle file delivery. The modes get rewards which correspond to the storage capacity, the computational resources, and the bandwidth they contribute to the CESS network.

2.2.2 **Distributed Storage Resource Layer**

CESS offers greater security, integrity, and scalability than traditional centralized storage networks. All user data files are encrypted, replicated, and sharded to ensure security and redundancy within CESS. Users are given unique private keys to access their private data. Additionally, storage nodes only store segments of data files, greatly protecting networks from data breaches.

Storage nodes 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 the CESS blockchain, and CESS storage proof algorithms guarantee the stored data integrity.

2.2.2.1 **Data Storage Process**

The CESS network has a streamlined process that ensures efficiency and security at every step of storing data. The intelligent services of CESS tailored for images, videos, and documents, making online data processing seamless for users. Additionally, CESS supports users in deleting data online. All of the data operations can be traced by CESS blockchain.

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, etc. The data fingerprints are for subsequent data rights confirmation.

Figure 3 illustrates the CESS data storage workflow.

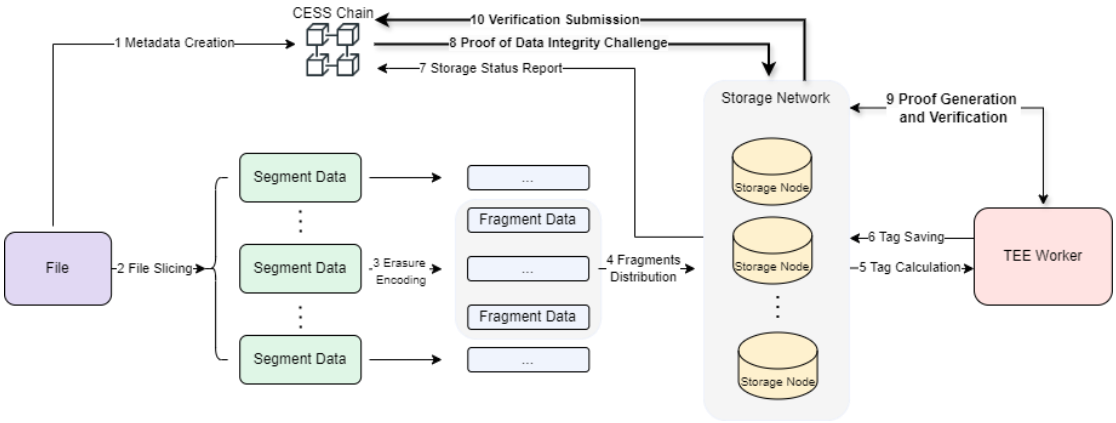

Figure 3 Data Storage Workflow

1) User data files are uploaded and pre-processed by CESS client software. Meta-data and data fingerprints are generated and submitted to the CESS chain.
2) The data file is sliced into small data segments.
3) Apply fault tolerant erasure coding, users can customize the code rate ($r = k/n$) based on the importance of the data segments. So even if the data segment copies are destroyed, they can be recovered by fault tolerant algorithms.
4) Distribute the data fragments to the CESS storage network.
5) The storage nodes apply for the data tag from the TEE Worker after receiving the file data fragments.
6) Save the data tag back to the storage node. The tag contains the signature of the verifier, which will prevent it from being tampered with.
7) Report the storage status to the CESS chain after marking the data file as reliable.
8) Periodically, the consensus node triggers and generates random challenges at

irregular intervals

9) Calculate proof of data integrity and obtain verification from the TEE worker. The storage node needs to finish the challenge before the proving deadline, otherwise the data file will not be recognized by the CESS chain

10) Submit the proof back to the CESS chain. The aggregate proofs can also be sent in batches for better efficiency.

Please note that steps 8 to 10 are a periodic challenge process. See 3.2.2 for details.

2.2.2.2 **Distributed Storage System**

CESS offers a comprehensively and reliably object storage service by Distributed Storage System. The upper-level applications invoke the interface of the object storage service, and the object storage module automatically maps the user's object storage space onto the lower-level unified distributed object storage space. The user data is stored in the distributed object storage engine in the form of object data.

The CESS Distributed Storage System incorporates several advanced features to enhance data availability, performance, and security. **Data redundancy and replication mechanisms** ensure high durability and resilience against node failures by replicating data across multiple nodes. The storage layer is designed for scalability and elasticity, allowing it to handle varying loads and large volumes of data efficiently by adding more storage nodes as demand grows. These storage nodes are added when users participate in the network as storage miners, contributing their unused storage resources to the CESS network. **Data sharding** further improves storage efficiency and performance by breaking down large data sets into smaller shards, which are then distributed and managed across multiple nodes.

To ensure data security, CESS employs Advanced Encryption Standards (**AES**) for data both in transit and at rest, robust access control mechanisms including Role-Based Access Control (**RBAC**) and Multi-Factor Authentication (**MFA**), and continuous auditing and monitoring tools to track data operations and access patterns in real time. These features collectively provide a robust, scalable, and secure storage solution within the CESS network.

2.2.3 **Content Decentralized Delivery Network (CD²N)**

The CESS optimizes file access efficiency by integrating CDN and P2P technologies[5]. It reduces the need for numerous proxy servers, enhance system capacity, lower costs, and sends data content to clients' autonomous domains by high-speed transfer technology. This approach improves media access quality for customers and boosts P2P network performance within a smaller autonomous system. Furthermore, a high-performance cache proxy server resolves the seed issue in pure P2P networks. Content in the application is initially published on the source node, ensuring continuous download services unless the node goes offline.

The implementation of CD²N enables multiple nodes to save and provide downloads of the same content, allowing users to download from various nodes simultaneously

for an enhanced experience. Proxy nodes create an independent P2P network with connected storage nodes lacking public network IP addresses.

Some of the key features of CESS CD²N are:

- **Dynamic Load Balancing:** The CD²N layer employs dynamic load balancing algorithms to distribute traffic efficiently across multiple nodes. This ensures that no single node becomes a bottleneck, optimizing network performance and reducing latency.
- **Edge Computing:** By integrating edge computing capabilities, the CD²N layer processes data closer to the end-users, further reducing latency and improving the speed of content delivery. Edge nodes can perform real-time data processing and caching, enhancing user experience.
- **Scalability and Elasticity:** The CD²N layer is designed to scale elastically based on demand. During peak times, additional nodes can be added to handle the increased load, while during off-peak times, resources can be scaled down to save costs.
- **Security and Privacy:** The CD²N layer incorporates advanced security protocols to ensure data integrity and privacy. Encryption techniques and secure key management are employed to protect data during transmission and storage. Additionally, the use of blockchain technology ensures a tamper-proof record of all transactions.
- **Fault Tolerance:** The network is built with fault tolerance mechanisms that detect and mitigate node failures. If a node goes offline, the system automatically redirects traffic to other available nodes, ensuring uninterrupted service.
- **Analytics and Monitoring:** Comprehensive analytics and monitoring tools are integrated into the CD²N layer, providing real-time insights into network performance, user behavior, and content popularity. This data helps optimize content distribution and improve overall efficiency.
- **Interoperability with other Networks:** The CD²N layer is designed to be interoperable with other CDN and P2P networks. This allows for seamless integration and collaboration, expanding the reach and capabilities of the network.
- **Energy Efficient:** The CD²N layer includes energy-efficient protocols and hardware configurations to minimize the carbon footprint of the network. By optimizing resource utilization and employing green technologies, the system promotes sustainability.

DeOSS (Decentralized Object Storage Service) is a decentralized object-based mass storage service that provides low-cost, secure and scalable distributed data storage services for the web3 domain.

DeOSS acts as an encryption proxy, access gateway and content distribution platform for the CESS network.

The workflow of CD²N is shown in Figure 4:

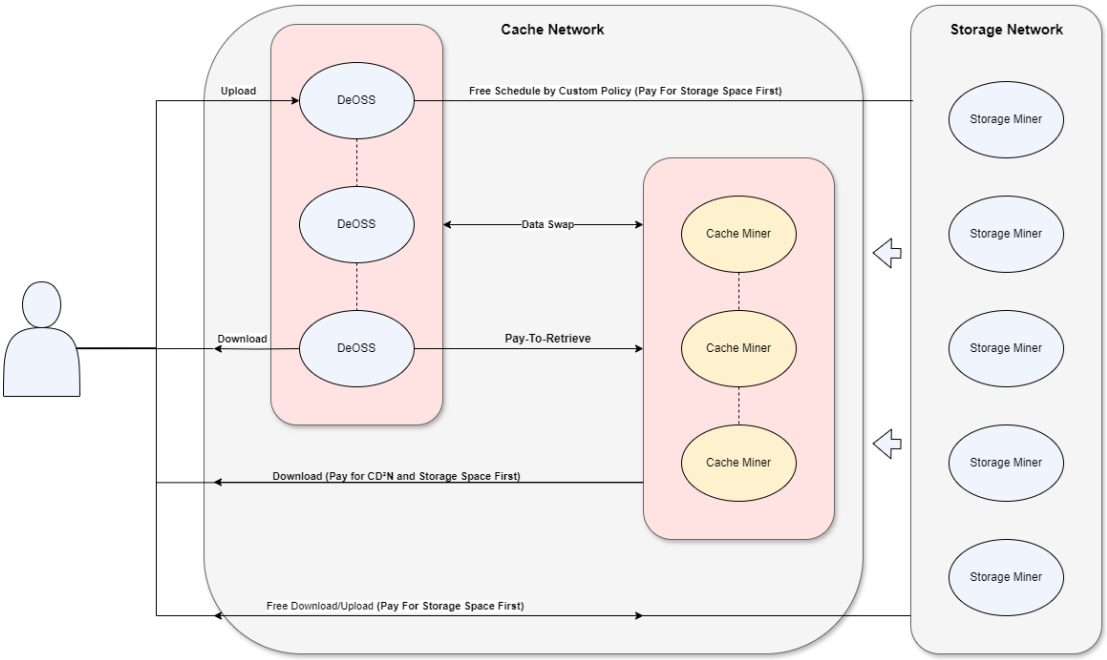

Figure 4 CD²N Network

By integrating these advanced features, the CESS system's CD²N layer provides a robust, efficient, and scalable solution for content distribution, leveraging the best of both CDN and P2P technologies to deliver an optimal user experience. This multifaceted approach ensures that users can access high-quality media content quickly and reliably, regardless of their geographic location or network conditions.

2.3 **XESS AI Protocol Suite**

Undoubtedly, AI constitutes the trend of the future. Nevertheless, in the wake of the swift progress of AI research and technology, the abuse of data, the leakage of privacy, and the legal supervision in many countries have all triggered contemplation in terms of human ethics and morality. CESS introduces the **XESS AI Protocol Suite** by leveraging our strengths in distributed storage and privacy computing. **XESS AI Protocol Suite** hopes to standardize a series of AI technologies such as distributed training, inference, and AI applications on the protocol specification, and propose solid solutions on how to create responsible AI.

The XESS AI Protocol Suite is a pivotal addition to the CESS ecosystem, designed to harness the power of artificial intelligence while ensuring data privacy and sovereignty. The XESS AI Protocol Suite operates alongside the CESS Protocol Suite and interacts directly with the Interface Layer, integrating advanced AI capabilities with the secure, decentralized infrastructure of the CESS network.

2.3.1 **CESS AI Gap**

At the heart of the XESS AI Protocol Suite is the **CESS AI Gap**, a Byzantine-robust circuit that prioritizes privacy and data sovereignty. This innovative protocol allows

participants at each CESS node to collaboratively train shared train AI models decentralized without exposing their original data. During the model training period, the CESS AI Gap leverages smart contracts to delegate local model training tasks to computing nodes within the CESS network. These computing nodes can range from GPUs and GPU clusters to decentralized GPU computation Web3 DePINs (Decentralized Physical Infrastructure Networks), enabling participants to engage in data sharing, or "mining", at any time.

2.4 **Interface**

The interface serves as a bridge for interaction and communication between different parts of **CESS Protocol Suite** and **XESS AI Protocol Suite**, defining a set of rules and conventions that enable various components to work together and achieve the overall functionality of CESS.

By defining a clear interface, the internal implementation details of CESS can be hidden, and external components only need to focus on the functions and parameters provided by the interface, without the need to understand the specific implementation methods inside. This encapsulation and abstraction improve the maintainability and scalability of CESS, making it easier to modify and upgrade the system, while also reducing the coupling between different parts of CESS.

Specifically, the Interface enables the efficient implementation of data storage services. It ensures the secure and organized management of data, allowing for seamless access and manipulation. In the context of blockchain services, the provided interfaces facilitate the creation, management, and interaction with the other blockchain networks or web3 DApps, enhancing the security and transparency of transactions.

Furthermore, the Interface contributes to the delivery of high-speed content. It optimizes the content distribution process, ensuring rapid and reliable delivery of data to end-users.

Additionally, it supports the integration and utilization of AI tools such as **CESS AI GAP** too. This enables the development and application of algorithms and models, promoting advanced capabilities of training, inference, analytics and decision-making.

3. **Key Technologies**

3.1 **Random Rotational Selection (R²S)**

CESS proposes a block authoring protocol called the Random Rotational Selection (R²S) consensus mechanism, designed to optimize and address the existing challenges. This innovative approach is paired with a deterministic finality mechanism named GRANDPA, integrated within the Substrate framework, collectively forming the consensus protocol.

The R²S mechanism allows users who wish to become node operators to join

candidate nodes freely. In each window (e.g., every 6 hours), only **11** formal rotation nodes are selected to participate in block production. Candidate nodes not involved in block production can demonstrate their capability by participating in data preprocessing and other processes, potentially becoming formal rotation nodes in future rounds.

During the process, the network scores each node's credit. If a node misbehaves which harms the network's overall interests, its score is reduced. When a node's score falls below a certain baseline, it cannot compete to become a candidate node. If formal nodes intentionally act maliciously or fail to meet network requirements, they are removed, and the network randomly selects replacement nodes from the candidate pool.

3.1.1 **Verifiable Random Function**

CESS uses the model of "randomly selecting several consensus nodes from candidate consensus nodes, and then collaboratively packaging and trading blocks through consensus algorithms", which enhances the security of the blockchain while increasing the randomness and unpredictability of node election. Each candidate consensus node has a public and private key pair. When selecting the corresponding consensus node in each time window, each candidate consensus node calculates the hash random output through the following formula:

$$\boldsymbol{R = VRF\_Hash(Sk, Seed)}\ )$$

$$\boldsymbol{P = VRF\_Proof(Sk, Seed)}$$

Within this function, the private key, denoted as *Sk*, belongs to the node. The Seed, a specific piece of information within a block on the CESS chain, cannot be anticipated beforehand. R represents a random hash output and P signifies a proof hash. By following these steps, the verifier can confirm that both values were generated by the node that owns them:

$$\boldsymbol{R = VRF\_P2H(P)}$$

$$\boldsymbol{VRF\_Verify(Pk, Seed, P)}$$

Pk represents the public key of the authenticated node within this group. Utilizing the algorithm described, the consensus nodes will be identified as the **11** nodes with the lowest hash random output. In cases where more than **11** nodes are chosen, a credibility score will be used to filter out the excess nodes.

3.1.2 **Admission and Exit**

Although CESS does not have strict entry criteria for nodes, a need to comply with the fundamental operational and resource contribution indicators for network operation conditions is mandated. Additionally, nodes are required to pledge a specific amount of CESS tokens as a preventive measure against malicious activities. Upon completing the token pledge, nodes can participate in the process.

If a node decides to leave, the network will evaluate whether to reimburse the entire

collateral tokens depending on the node's performance while active. In an optimal scenario, if the node functions smoothly without encountering prolonged disconnects or deliberate misconduct, the network will fully refund the collateral tokens. This entry process acts as a deterrent against attacks and bolsters consensus security across the network.

3.1.3 **Election and Block Production Process**

Compared with the Polkadot consensus mechanism, R²S focuses on node election and block generation. The following is the overall process:

- Nodes register as consensus nodes through staking, the current staking amount is 3 million.
- Validators will change with each era, following a rotation based on their score ranking. The **11** nodes with the highest scores are selected as validators for the era.
- The final score is based on a combination of the credit score, the staking score and the VRF score determined by VRF[6]. Please refer to section 5.5 for the score calculation function.
- The selected validators generate blocks in order.
- Blocks confirmation is the same as GRANDPA.
- The last epoch of each era begins the election of validators for the next era.

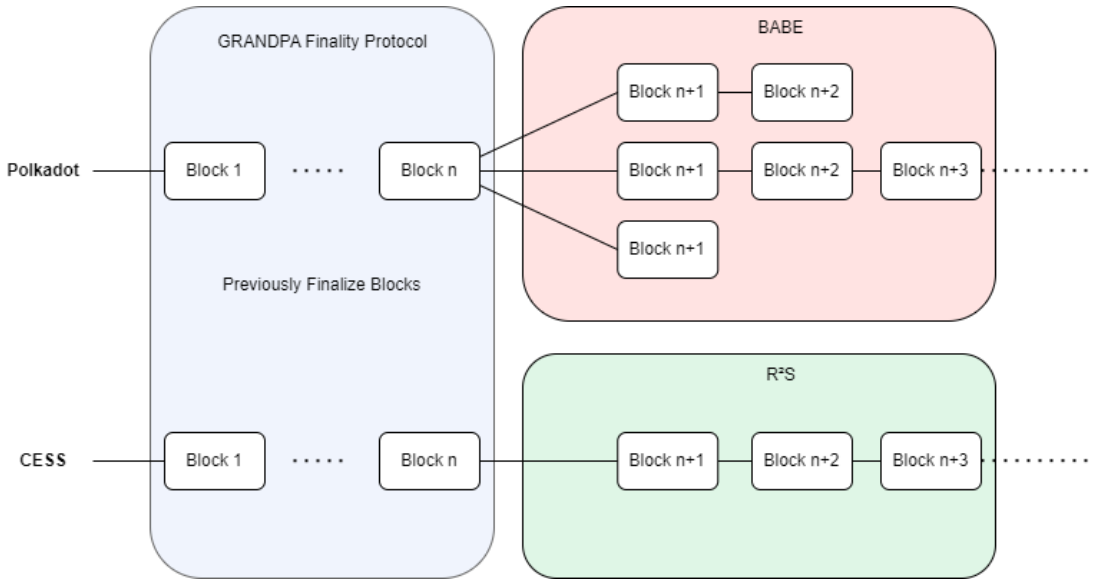

Figure 5 The block generation difference between R²S and BABE

Upon joining the CESS network, consensus nodes must maintain network integrity and manage tasks such as data preprocessing. To motivate active participation, CESS utilizes a credit-based system that evaluates the performance of each consensus node based on its workload as a validator, encompassing various tasks such as:

- Total number of bytes for processing inservice files.

- Verify the total number of bytes of inservice files and idle space during random challenges.
- Total number of bytes to authenticate or replace idle space.

3.1.4 **Advantages of R²S**

Avoid Monopoly and Centralization

The R²S mechanism ensures a decentralized approach to storing block history, preventing excessive centralization of large miners that could harm the network's development.

Improve Consensus Efficiency

CESS selects **11** nodes within each era using R²S for block generation and verification. These **11** nodes take turns in block generation, ensuring efficient consensus and decentralization.

On-Chain Transaction Processing

CESS can achieve efficient on-chain metadata processing, enabling direct implementation of data storage addressing and ensuring data authenticity through the blockchain mechanism.

3.2 **Multiple Data Storage Proof Algorithm**

The landscape of decentralized storage networks, exemplified by projects like Storj and Filecoin, underscores the feasibility of leveraging blockchain technology to construct such networks. Users increasingly tend to contribute their idle storage resources to decentralized storage networks, seeking corresponding benefits. However, ensuring data integrity in such networks is a pressing concern, primarily due to potential cheating behaviors among participants.

Cheating behaviors, notably storage space fraud and outsourcing attacks, pose significant challenges. These behaviors involve miners providing falsified storage space or colluding to subvert data reliability by storing multiple copies of data on seemingly independent miners. Various mechanisms have been proposed to address these challenges, including proof of storage, proof of replication, and proof of space-time. While effective in theory and practice, certain mechanisms may encounter efficiency bottlenecks, particularly in data retrieval.

In response, CESS has introduced two innovative techniques to enhance its storage services: Proof of Idle Space (PoIS) and Proof of Data Reduplication and Recovery (PoDR²). PoIS validates the storage space offered by the storage miners, which does not include the user's data; hence called idle space (aka. idle segment). On the other hand, PoDR² is used to verify the user's data (aka. service segment) stored by storage miners.

3.2.1 **Proof of Idle Space (PoIS)**

Since the trustworthiness of every node in the storage network cannot be guaranteed, CESS cannot access the unused space on nodes in the same way as traditional computer disk management. One effective method is to use randomly generated data to fill these empty spaces. The actual available space on each node can be determined by measuring the amount of filled data. It is also necessary to implement security mechanisms like storage proof to ensure this random data is consistently stored on nodes, warranting a reliable and accessible storage space. When uploading user files, swapping out large sections of unused data can convert idle space into functional storage capacity.

The Proof of Idle Space (PoIS) mechanism involves authentication, verification, and replacing idle space for storage nodes. Similar to the proof of inservice data storage mechanism, proof of idle space also needs to check the integrity of idle data through random challenges and verification processes. In contrast to user-provided inservice data, idle data (idle files) are created by storage nodes in a specific manner. This distinction results in significant differences in implementing the proof of idle space and storage-proof algorithms. There has been a lot of research on proof of space, and it is widely used in various distributed storage systems or blockchain consensus protocols. Most existing space-proof algorithms manage large or whole storage spaces, such as Filecoin's replication proof, Chia's spatiotemporal proof, etc. However, because the CESS system needs to meet dynamic operations such as user data insertion and deletion, replacing large space will be very slow. Therefore, the CESS idle space-proof mechanism has made certain improvements to better adapt to dynamic changes in space.

3.2.1.1 **Accumulator**

An accumulator is a fixed-length byte sequence (or digest) obtained through a series of element "accumulation operations". One frequently employed function is to verify the presence of an element within a set, thanks to its unordered and flattened attributes that facilitate the seamless addition or removal of elements dynamically. "Accumulation operation" refers to embedding elements from a set into an accumulator through certain cryptographic calculations.

The efficiency of calculating the accumulator and element evidence is significantly reduced when dealing with a large number of elements. To address this issue, a three-layer multi-level accumulator is applied to enhance calculation efficiency by optimizing idle space utilization. In this multi-level structure, the upper accumulator element is comprised of multiple sub-accumulators. When updating an element within a sub-accumulator, only its parent accumulator and sibling accumulators' evidence need to be recalculated layer by layer, without necessitating updates to other elements. For instance, in the illustrated two-level accumulator scenario (Figure 6, updating an element in sub-acc1 only requires recalculating sub-acc1 and ACC, followed by updating the evidence of sub-acc2...sub-accN to minimize unnecessary element updates.

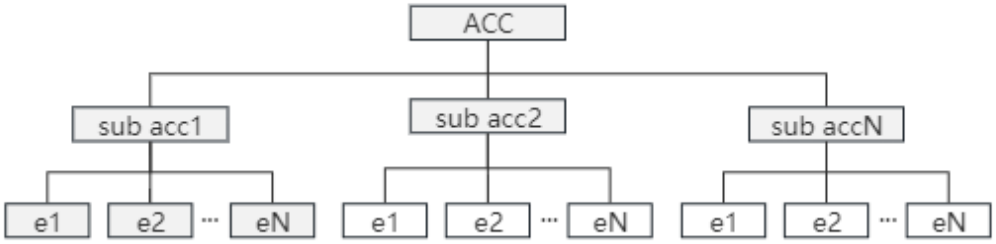

Figure 6 Accumulator and Sub-Accumulator

3.2.1.2 **Idle File Generation**

When idle files are generated by a prover, three conditions need to be met to ensure security.

- **Prevention of Compression:** Generated idle files cannot be compressed, as this would allow provers to authenticate more space at a lower cost.
- **Protection against Temporary Generation:** Idle files must not be temporarily generated during random challenges to prevent generation and space-time attacks.
- **Avoidance of Cross-Authentication:** Provers must be unable to use one idle file to authenticate multiple spaces, or use someone else's idle file to authenticate their own space. This measure prevents witch attacks and external attacks.

CESS employs a stone-laying game on a stacked binary expander to generate idle files that meet these security conditions

A Stacked Bipartite Expander is a complex structure consisting of multiple layers of bipartite graphs stacked on top of each other. Bipartite graphs are a special type of Directed Acyclic Graph (DAG). In these graphs, the vertex set V is split into two distinct subsets, with edges connecting vertices from each subset without any connections between vertices within the same subset. The example in Figure 7 illustrates a stacked bipartite expander with K - 1 layers, N - 4 vertices per layer, and D - 2 degrees per vertex. Vertices that do not have any incoming edges are known as source points (e.g., the V0 layer), while those without outgoing edges are referred to as sink points (e.g., the Vk layer).

By using this structure, CESS can generate idle files securely, ensuring the integrity and authenticity of the storage space.

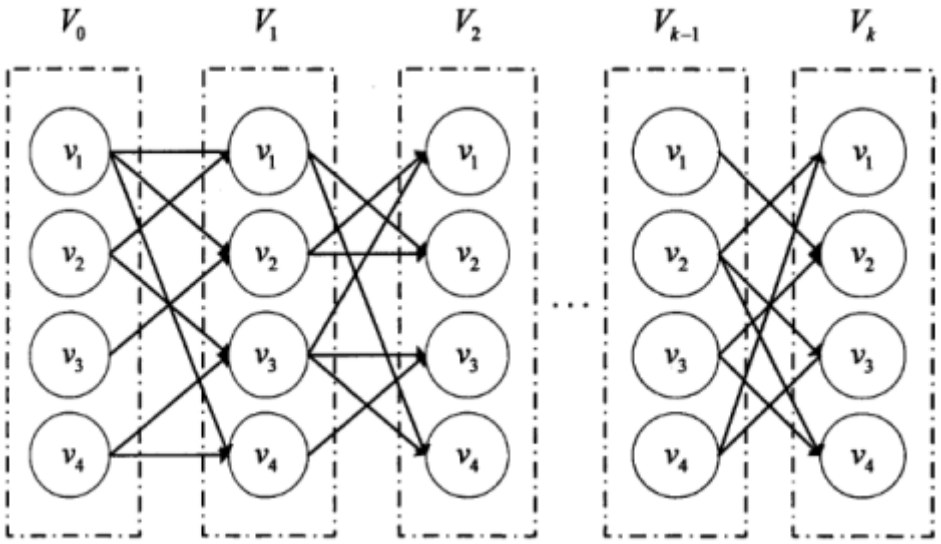

Figure 7. Idle File Generation

One of the key features of PoIS is its dynamic proof of space mechanism, which allows miners to manage their stored space. This mechanism involves a two-layer accumulator structure, where the first layer accumulates all idle files, and the second layer proves the space of individual idle segments. Miners can add or delete idle segments as needed, and they must respond to challenges from verifiers to prove the integrity of their stored space.

3.2.2 **Proof of Data Reduplication and Recovery (PoDR²)**

The Proof of Data Reduplication and Recovery (PoDR²) mechanism in CESS reassures data availability using Erasure Coding (EC). This technique involves breaking data into fragments, expanding and encoding them with redundant data pieces, and storing them across different storage miners. The erasure coding redundancy enhances network reliability and can tolerate system failures.

In addition to Erasure Coding, CESS PoDR² implements Proof of Data Possession (PDP)[7] to prevent cheating behaviors. When a user uploads a file to the CESS network, PoDR² begins by slicing the file into multiple fragments. Fault-tolerant erasure coding is then calculated, as depicted in the diagram below.

The file fragments and erasure-encoded data are distributed to randomly selected storage miners in the CESS network. Metadata of those fragments, including segment hash, location of the segment, size, and other details, is recorded on the CESS blockchain.

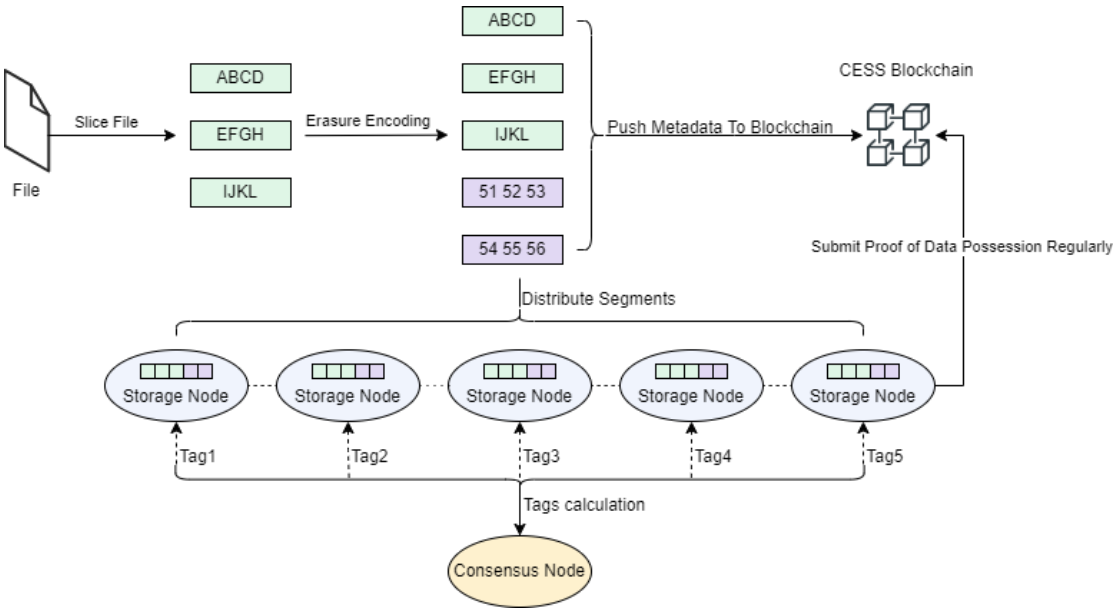

Figure 8. PoDR² Process

When a storage miner receives file fragments, they promptly request the Trusted Execution Environment (TEE) of the consensus miner to calculate PoDR² Tags. These tags are then saved alongside the file segment and utilized for generating PDP proofs[7]. After all storage miners have securely stored the file fragments, the CESS network regularly tasks them with computing proofs for randomly chosen file fragments and sends them to the blockchain for rewards. Failure to retain the file segment or tags will prevent a miner from producing proofs within the specified timeframe, resulting in penalties for failing to meet proof requirements.

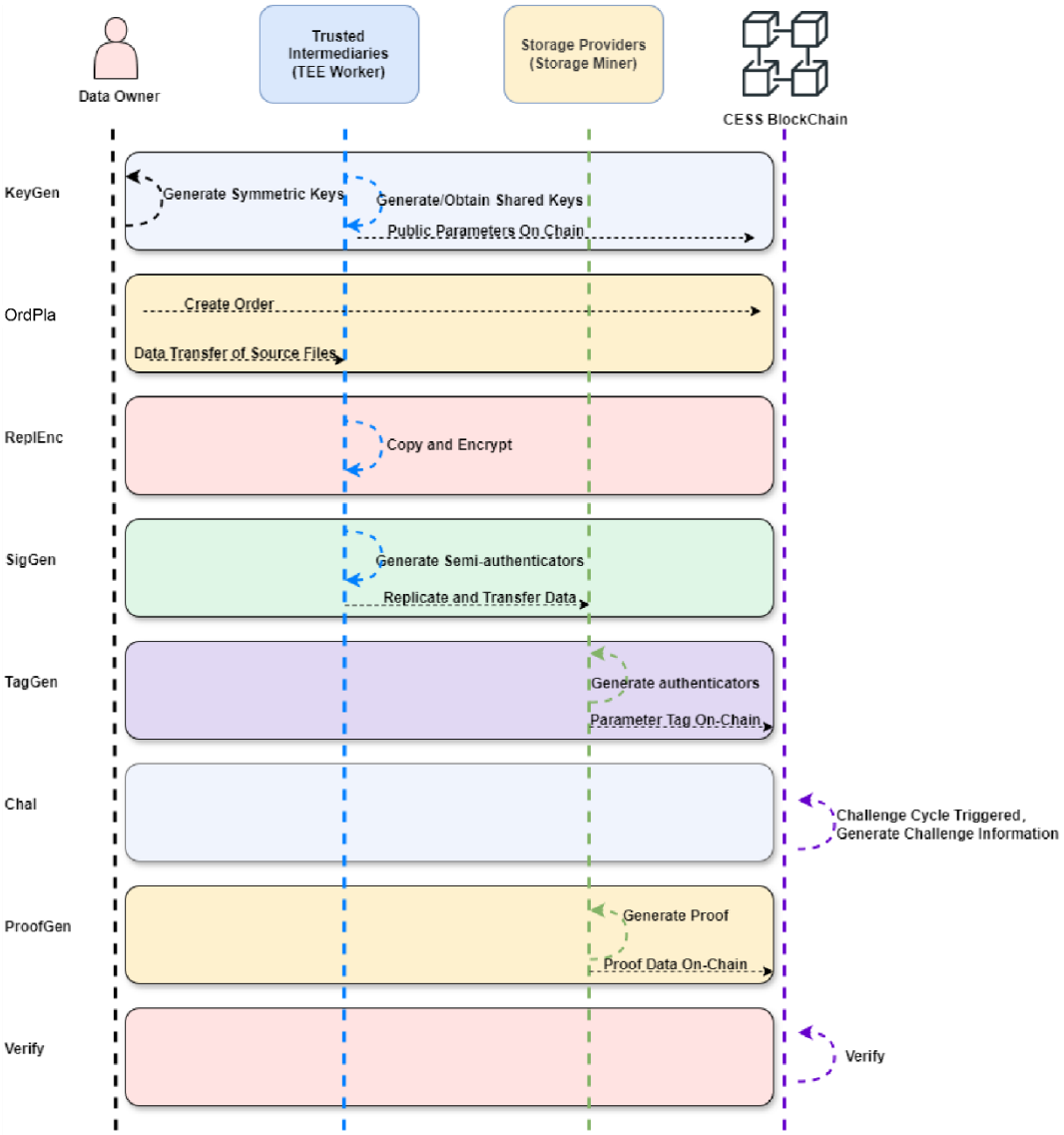

Figure 9. The algorithm workflow of PoDR²

The algorithm workflow of PoDR² as follows:

- $\boldsymbol{KeyGen(\pi,\ k)}$: This algorithm is executed by *TI* and the *DO*. It takes the system public parameters π,and the system security parameters *k* as inputs and outputs the *DO*'s set of symmetric keys k_{set}, as well as the *TI*'s public parameters *pk* and private parameters *sk.*
- $\boldsymbol{OrdPla(F)}$: The algorithm is executed by the *DO*, taking file *F* as input and calling the smart contract on the *BN* to create storage order. It outputs the unique order identifier ID_{ord} and the file metadata *(name, h).*
- $\boldsymbol{ReplEnc(F,\ k_{set})}$: The algorithm is executed by the *TI*, taking *F* and k_{set} as inputs. It outputs a set of encoded replicas called $C = \{C_i\}$.
- $\boldsymbol{SigGen(c,\ sk)}$ **:** The algorithm is executed by the *TI*. taking the encoded replica *c* and *sk* as inputs. It outputs a tag *t, ξ* and semi-authenticators $\{\delta_i\}$.
- $\boldsymbol{TagGen(c,\ pk,\ t,\ \xi,\ \{\delta_i\})}$: The algorithm is executed by the *SP*, taking *c, pk, t, ξ* and $\{\delta_i\}$ as inputs. It outputs a set of authenticators $\{\delta_i\}$.

- $\boldsymbol{Chal}()$: The algorithm is triggered by the smart contract on the *BN*, and it outputs the challenges $chal = \{(i, v_i)\}$.

- $\boldsymbol{ProofGen}(\boldsymbol{chal}, \boldsymbol{c})$: The algorithm is executed by the SP, taking the encoded replica *c*, challenges $chal = \{(i, v_i)\}$, and the authenticators $\{\sigma_i\}$ as inputs, and outputs the $Proof(\mu, \sigma)$.

- $\boldsymbol{Verify}(\boldsymbol{pk}, \boldsymbol{\mu}, \boldsymbol{\sigma})$: The algorithm is triggered by the smart contract on the *BN*, taking the *pk* and the $Proof(\mu, \sigma)$ as inputs, and outputs the verification result.

Were,

DO: Data Owners

TI: Trusted Intermediaries

SP: Storage Providers

BN: Blockchain Network

If a file segment is lost due to a natural disaster or a miner leaving the network, PoDR² can identify and replace the missing segment by replicating it to another storage miner, guaranteeing the file remains accessible.

3.2.2.1 **Handling Large Files**

Tagging large files can be a time and resource-consuming task, particularly in a TEE environment. Due to limited computing resources, generating tags for extensive files may not be feasible. To address this issue, CESS PoDR² divides the data into smaller segments before fragmentation, enabling support for files of any size. This approach simplifies the process of computing Erasure coding, making it easier to handle large files.

By breaking down large files into manageable segments, the CESS network can maintain efficient tagging and verification processes, ensuring data integrity and availability across the network.

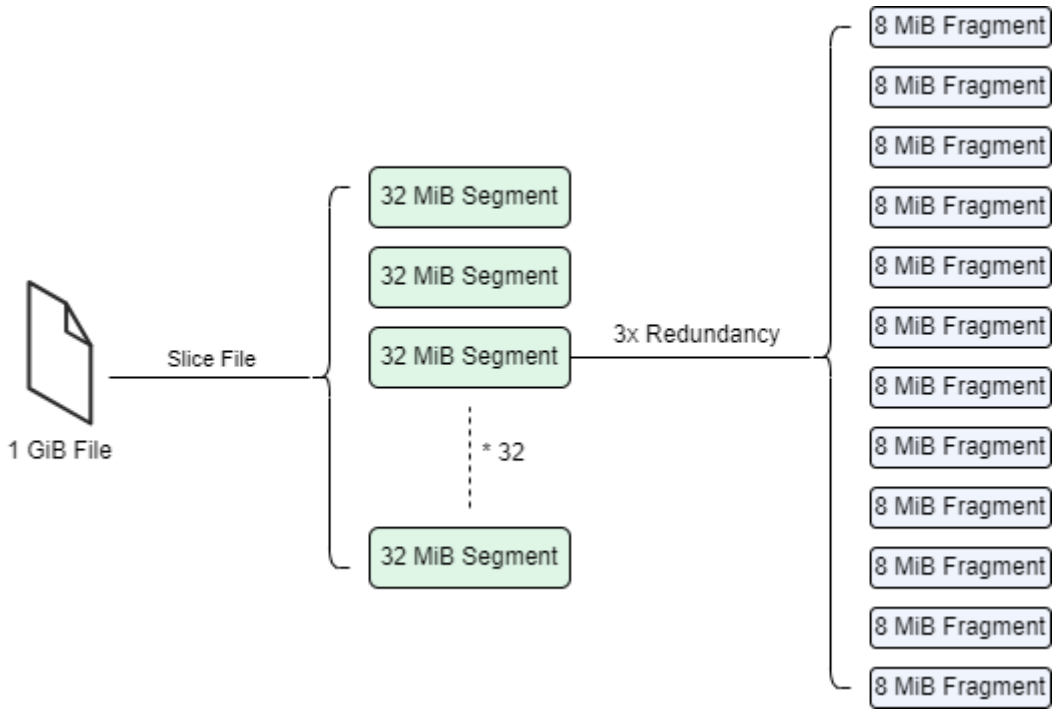

Figure 10. Slicing File into Fragments

3.2.2.2 **Trusted Execution Environment**

In the CESS network, consensus miners are configured with a TEE, which is a secure area of a processor that helps code and data loaded inside it to be protected concerning confidentiality and integrity. The data in the TEE is encrypted and isolated from other programs running on the system, preventing any third party from accessing the data loaded within it.

CESS TEE consists of a private key pair unknown to external applications. This key is used to compute PoDR² Tags for each data fragment. The tag contains information like the fragment name and secret information encrypted by the PoDR² TEE's private key based on PDP[7][8]. In addition, computing tags are time and resource-intensive, making storage miners compute their fragment tags in advance. Failing to do so can result in storage miners not producing storage proofs in time and being penalized.

3.3 **Proxy Re-encryption**

To safeguard user data, CESS employs encryption and disperses it among multiple storage miners. The primary objective of CESS is to establish a platform centered on data equity, facilitating encrypted data circulation and sharing across different entities. To improve data sharing within CESS, we will develop a decentralized proxy re-encryption[9][10] system to enable owners to swap data without compromising its confidentiality. Users can designate their uploaded data as public or private. Private data segments are encrypted before being distributed to storage miners. If authorized by the owner, the proxy re-encryption mechanism can grant access to specified entities by encrypting the nodes stored on the miner, allowing designated parties to securely access others' data using their private keys.

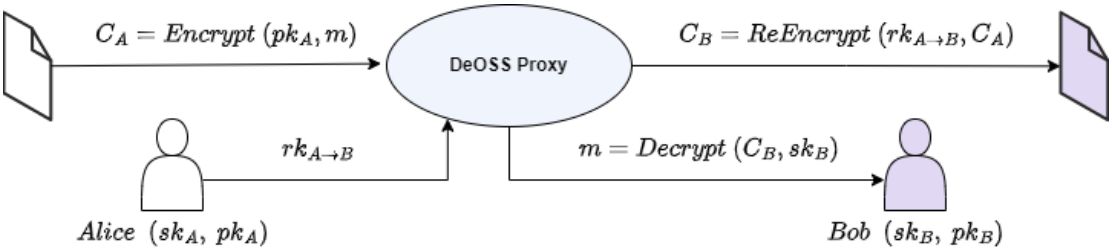

Figure 11. Proxy Re-encryption

- As shown in Figure 11, we use DeoSS as the ReEncryption proxy:
- Alice encrypts a message m, with Alice's public key pk_A, resulting in ciphertext C_A.
- Alice decides to delegate access to message m to Bob, who has the key pair $(sk_B,\ pk_B)$.
- Alice creates a re-encryption key using her secret key and Bob's public key:

$$\boldsymbol{rk_{A\to B} = rekey}(sk_A, pk_B)$$

- DeOSS Proxy will re-encrypt C_A and which gets transformed into C_B:

$$C_B = \boldsymbol{ReEncrypt}(\boldsymbol{rk_{A\to B}}, C_A)$$

- Bob can then decrypt C_B using his secret key sk_B, and get the Plaintext message m:

$$\boldsymbol{m = Decrypt}(C_B, sk_B)$$

3.4 **Multiple-Format Data Rights Confirmation Mechanism (MDRC)**

Without strong enforcement of data rights protection, a data exchange market is vulnerable to cyber piracy, potentially undermining its ability to provide exclusive content to users. In response, CESS has introduced a cutting-edge on-chain Multi-format Data Rights Confirmation Mechanism (MDRC) that assigns a unique data certificate ID to each file by extracting a data fingerprint. This ID comparison system helps detect and prevent data rights violations, ensuring the protection of premium content quality. By comparing these digital fingerprints, the MDRC can detect any connections between different sets of data. This connection serves as evidence of the data's origin, enhancing copyright protection and bolstering data copyright enforcement.

For instance, if a content creator uploads an original piece of music to the CESS network, MDRC will generate a unique digital fingerprint for that file. If another user later uploads a similar piece of music, MDRC will evaluate the resemblance between the two digital fingerprints to identify any potential copyright infringement.

Overall, MDRC enhances the integrity and quality of the data trade market by providing robust data copyright protection. The following Figure 12 illustrates the overall process of MDRC:

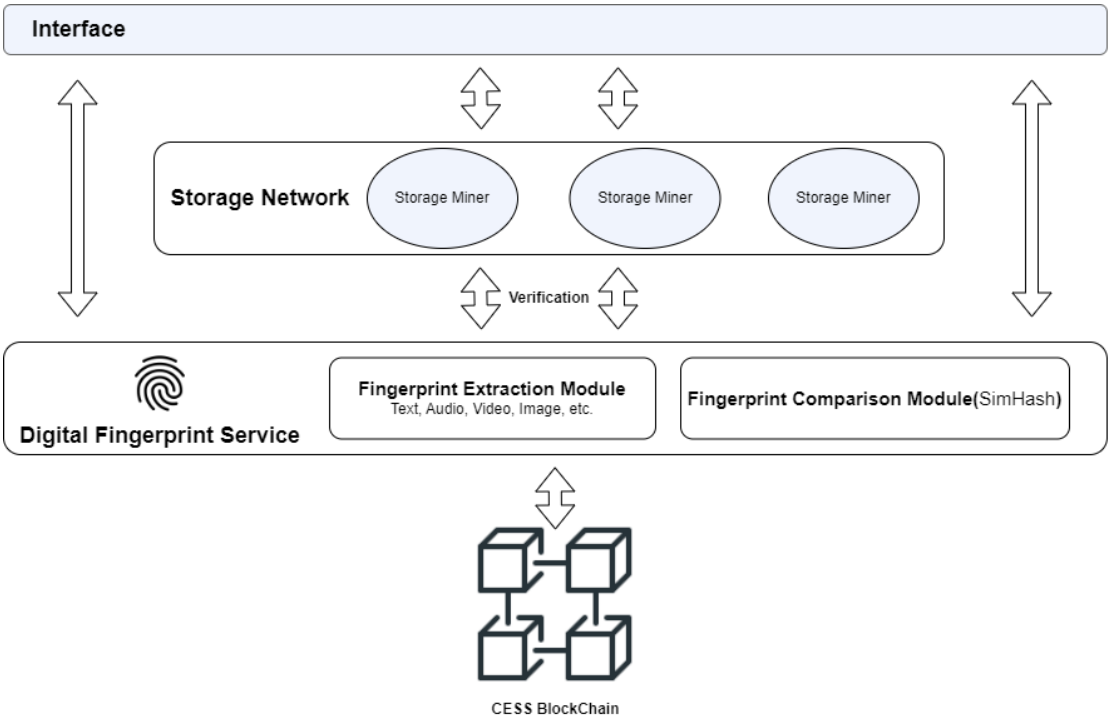

Figure 12. Multiple-Format Data Rights Confirmation Mechanism (MDRC)

Users initially process data files through the digital fingerprint mechanism to obtain their data fingerprints. This process operates at the user layer and involves three main stages: fingerprint extraction, on-chain embedding, and comparison.

The digital fingerprint algorithms used vary depending on the type of data:

- **Text Data**: For text data, advanced segmentation algorithms are selected for different types of natural language. Corresponding fingerprints are generated based on the latent semantic space.
- **Image Data**: Image data feature extraction includes color features, shape features, texture features, and spatial relationship features. Algorithms are used for feature transformation to improve the accuracy of image digital fingerprints.
- **Audio Data**: Audio data processing starts with sampling and quantizing the signal. A fast Fourier transform is then performed to extract features such as energy, time-domain, frequency-domain, music theory, and perceptual features.
- **Video Data**: Feature extraction for video data primarily involves extracting key frames, which are then processed using image feature extraction techniques.

CESS also supports digital fingerprint extraction methods for other data types that can serve as operation credentials for auditing purposes such as system operation logs, event behavior trajectories, and daily purchase vouchers. For specific technology implementations of these different data types, simple MD5 or SHA values are used as their respective digital fingerprints.

After obtaining the data fingerprint, users calculate it using the Simhash algorithm[11]. This process involves probabilistic dimensionality reduction of high-dimensional data, mapping it to a fingerprint with a small number of fixed digits. The resulting similarity

hash serves as a copyright mark for the source data.

CESS utilizes hamming distance detection technology to compare the copyright identifier with existing identifiers on the blockchain. This enables data lineage and similarity detection, providing users with reference information. When users upload source data to the CESS platform, the copyright identifier is stored on-chain through copyright identification storage services, facilitated by smart contracts. This process offers essential data support for subsequent data rights confirmation.

3.5 **CESS AI Gap**

Different organizations each have their private data. Some (or all) of the private data cannot be shared with the outside world because of sensitivity and some are due to national legal issues. Because of this, valuable data cannot be used for generating AI modules.

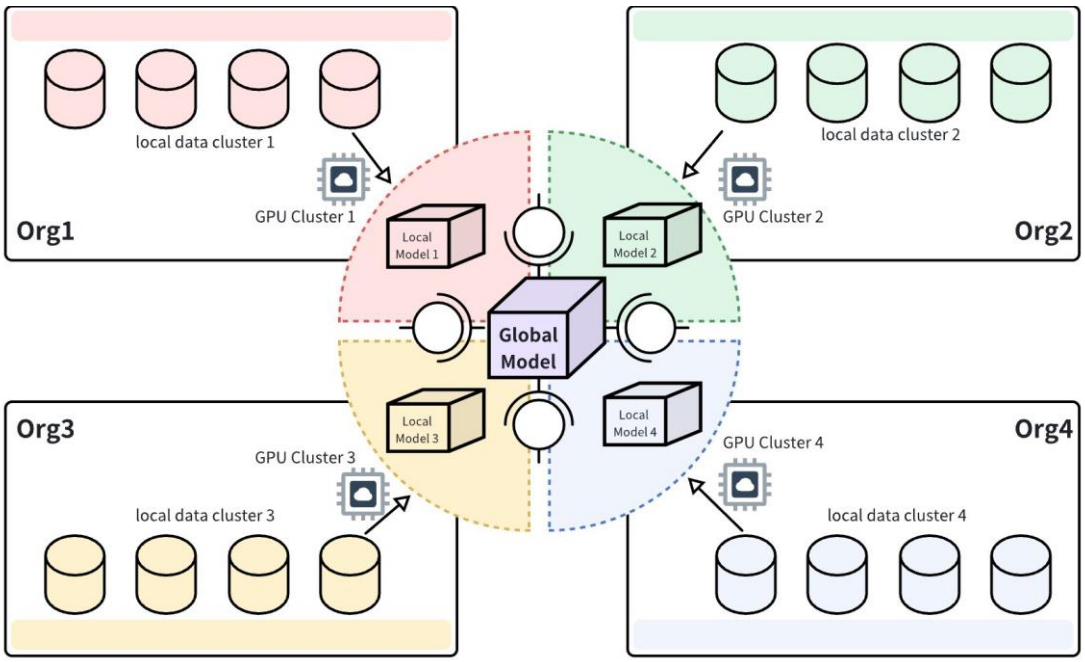

Figure 13. CESS AI Gap

In the realm of organizational data exchange and model development, the utilization of the CESS network presents a sophisticated avenue for sharing parameters and models among various entities. Through the employment of CESS AI Gap, an encryption mechanism characterized by its Byzantine-robust circuit with a focus on data privacy preservation, organizations can engage in iterative processes to refine and enhance their models securely. This mechanism operates under the orchestration of smart contracts, which schedule and coordinate the training of these AI models in a manner that adheres to stringent data privacy regulations.

The overarching goal of this process is to establish a shared global AI model that encapsulates the collective insights gleaned from diverse datasets without compromising individual data privacy rights or flouting legal statutes. By consolidating contributions from disparate sources within a secure framework, organizations can

collaboratively construct an optimal model that transcends industry-specific boundaries. Notably, this methodology ensures that sensitive data remains localized and protected throughout the model development process, thereby preventing any breaches or violations of regulatory compliance standards. Ultimately, this approach empowers organizations to create versatile AI models capable of addressing multifaceted challenges across industries on a global scale while upholding stringent data privacy protocols.

4. **Use Scenarios**

The CESS network offers a variety of use scenarios that leverage its secure infrastructure for data storage, retrieval, and management. These scenarios showcase the versatility and potential applications of CESS in different domains.

4.1 **DA Service**

The DA (Data Availability) Service is a crucial use case of the CESS network, offering a robust solution for ensuring continuous and reliable access to data. Below are some key details of the DA Layer:

- **Ensuring Data Availability:** The DA Service ensures that data is always accessible, even in the event of network disruptions or node failures. By replicating data across multiple nodes, it provides redundancy and fault tolerance, ensuring that data remains available despite potential issues with individual nodes.
- **Layer 2 Storage for Blockchain Networks:** The DA Service can perform as a Layer 2 storage solution for major blockchain networks like Bitcoin (BTC), Ethereum (ETH), etc. This use case allows these blockchain networks to offload large datasets to the CESS network, reducing on-chain storage costs and improving transaction speeds while maintaining decentralized and secure storage.
- **Applications in Various Sectors:** The robust and scalable nature of the DA Service makes it suitable for a wide range of applications, including decentralized finance (DeFi), enterprise storage solutions, and large-scale data management systems. These applications benefit from the DA Service's ability to provide reliable and secure data storage without relying on centralized services.

4.2 **VR Streaming Media**

The CESS network is ideal for VR streaming media, offering high-speed data transfer and low latency. By integrating CDN and P2P technologies, CESS ensures seamless streaming of VR content, providing users with an immersive experience. The decentralized nature of the network eliminates bottlenecks and single points of failure, enhancing the reliability and quality of VR streaming.

4.3 **Data Lake**

CESS supports the creation of data lakes, enabling organizations to store and analyze large volumes of unstructured data. The system's polymorphic data storage access interface provides a unified API for accessing object, block, and file storage, making it easy to integrate various data sources. With CESS, organizations can build scalable and cost-effective data lakes that support advanced analytics and machine learning applications.

4.4 **Distributed AI Training**

CESS facilitates distributed AI training by providing secure and scalable storage for training data. The network's high bandwidth and low latency ensure efficient data transfer between nodes, allowing for faster training times. By leveraging the CESS network, AI developers can collaborate on training models without compromising data privacy or security, thanks to the use of federated learning and encryption techniques.

4.5 **AIGC Innovation**

CESS supports AI-generated content (AIGC) innovation by providing a secure and scalable platform for storing and processing large datasets. The network's distributed architecture allows for efficient data sharing and collaboration among AI researchers and developers. With CESS, AIGC applications can leverage the power of decentralized storage to enhance creativity and innovation while maintaining data integrity and security.

4.6 **Web3 Games**

The CESS network enhances Web3 gaming by providing secure and scalable storage for game assets and player data. By leveraging blockchain technology, CESS ensures the authenticity and ownership of in-game assets, enabling secure and transparent transactions. The decentralized nature of the network also enhances the performance and reliability of online gaming, providing a seamless experience for players.

4.7 **Real World Assets (RWA)**

CESS enables the tokenization and secure storage of real-world assets (RWA) on the blockchain. By digitizing physical assets, such as real estate or art, and storing their provenance and ownership data on the CESS network, users can trade and manage these assets securely and transparently. This approach ensures the integrity and authenticity of asset data, providing a reliable foundation for RWA transactions.

4.8 **Distributed Network Disk**

CESS provides a unique Distributed Network Disk service for end users that offers several key benefits over traditional providers of Network Disk services. These advantages include enhanced security, protection of ownership rights, cost-effectiveness, and increased storage capacity. Unlike conventional cloud server-based storage solutions, CESS stores data across multiple independent nodes, eliminating reliance on centralized services. This decentralized approach establishes faster download and upload speeds without any restrictions. By leveraging blockchain technology and cutting-edge cryptographic techniques, CESS guarantees data privacy and security without central servers or potential data loss risks. Additionally, CESS enables storage nodes to dynamically join the network and contribute their unused space, allowing limitless expansion of the network's storage capabilities.

4.9 **Decentralized Digital Assets Marketplace**

The secure storage and decentralization of digital assets provenance and trading data are imperative for building trust in the digital assets marketplace. To validate NFTs, developers and owners upload their files, verified by CESS using the Multi-format Data Rights Confirmation Mechanism (MDRC). Following this verification process, the data files are distributed to storage nodes. CESS automatically captures important structural, subject, and semantic characteristics in its vector space. This efficient process ensures accurate indexing and mapping for improved public discovery and secure private retrieval of digital assets within the system.

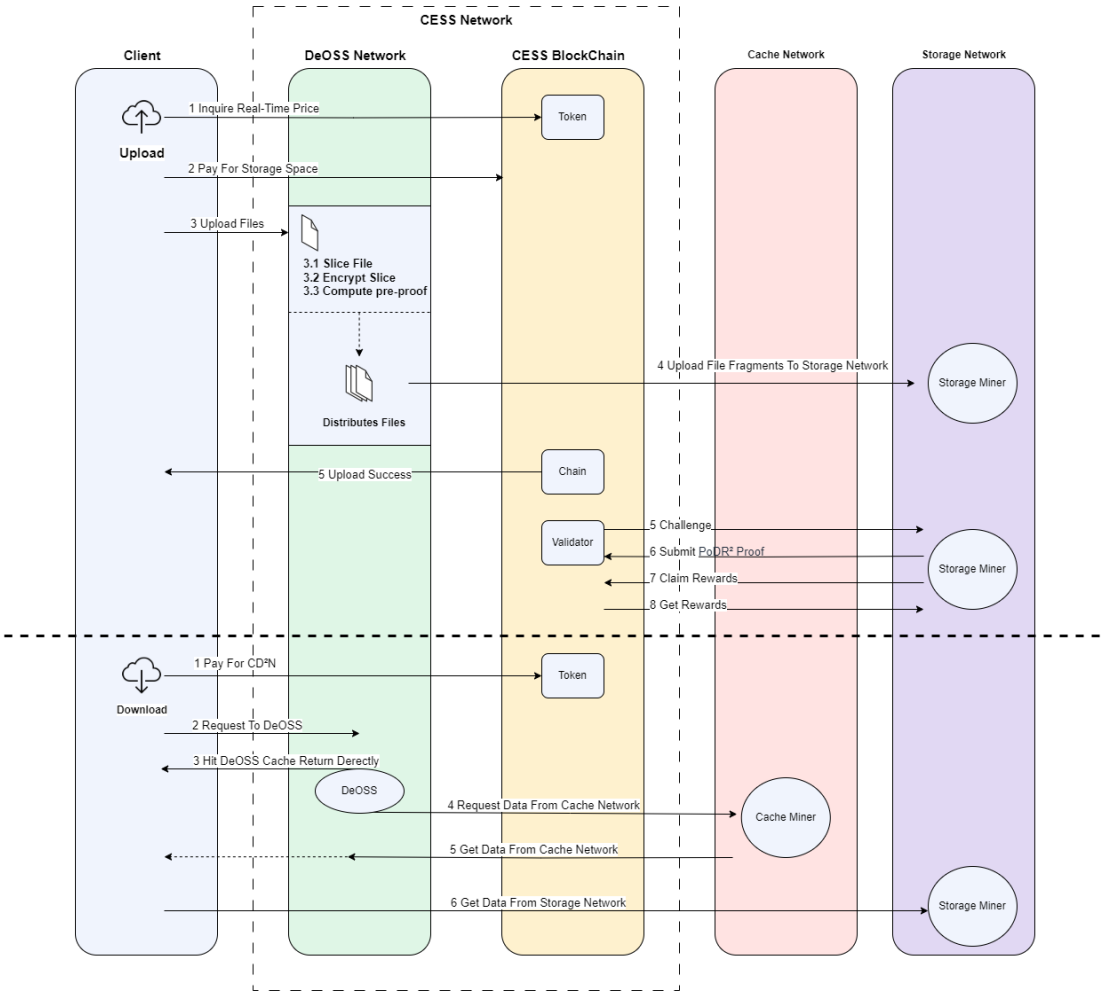

Figure 14. Client-Platform Interaction

A typical CESS client and platform interaction involves several steps:

- **Querying Storage Price:** The data storage client queries the CESS chain to obtain the current storage price.
- **Placing an Order:** The client submits an order for data files via an on-chain smart contract.
- **Uploading Data:** Once the payment is made and the order is approved, the client uploads the data file using the API. The file is not directly uploaded to storage nodes but to a CESS storage scheduling node.
- **Data Processing:** The scheduling node, with a secure hardware environment (Trusted Execution Environment or TEE) processes, encrypts, and shards the data file.
- **Data Distribution:** The scheduling node distributes data segments to storage nodes.

4.10 **Data Rights Protection**

From the clients' perspective, CESS delivers as a decentralized and user-managed data content-sharing platform. The platform's mission is to return data ownership to

users, encouraging them to explore the value of their digital assets while safeguarding their rights. To achieve this, CESS has implemented an on-chain smart contract-based data-sharing platform that is self-executing, fair, and transparent. This encompasses the entire data rights confirmation, tracking, and protection lifecycle.

CESS offers two types of smart contracts with different client-profit models. When users upload data files, they can choose their preferred model values. CESS generates data file attributes based on user inputs, including client-profit model type, whitelist, blacklist, and other preferences. These attributes are published alongside the user data.

When a data file is retrieved by clients of the data provider, the underlying smart contract executes according to the program set by the data file owner. The system checks the data file attributes to verify whether the data buyers have permission to retrieve the files. If the permission checks are successful, the system charges buyers according to the client-profit model and begins the data download.

CESS data users can also customize their data file attributes. All data file retrieval records are recorded on the blockchain, providing a traceable history. The CESS data rights protection mechanism includes a recording module that allows users to view their data file retrieval records, offering strong evidence for user data rights protection.

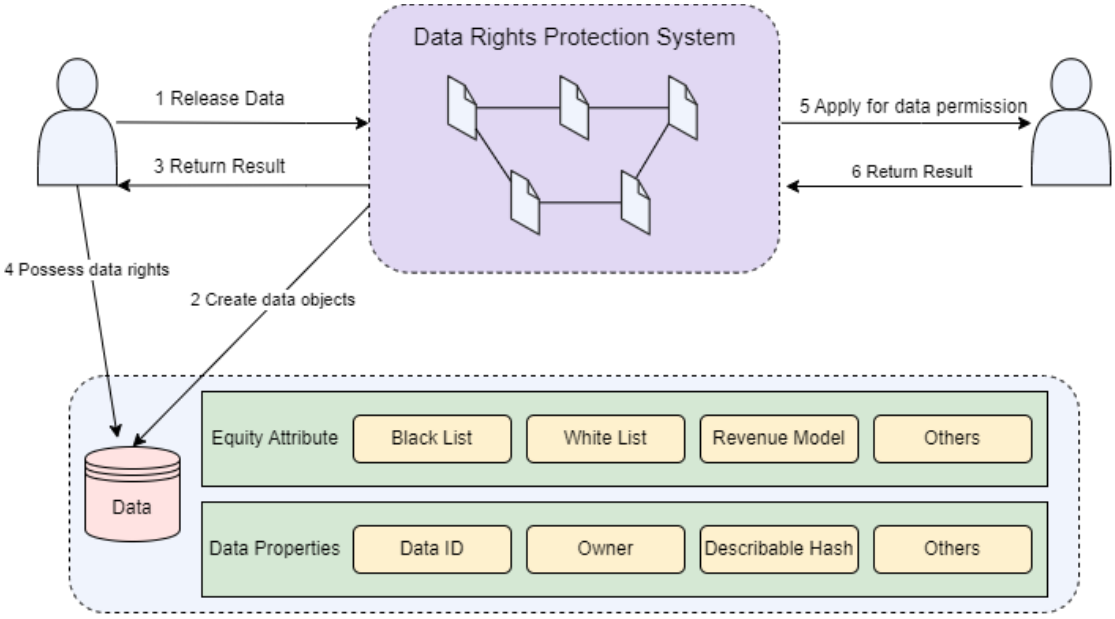

Figure 15. Data Right Confirmation and Protection

5. **Economic Model**

5.1 **Overview**

The design of the CESS network incentive model is to encourage miners to provide dependable, high-quality storage services, upholding the network's stability. By employing precise mathematical computations, our model evaluates the roles played

by nodes within the network and fairly distributes rewards.

CESS decentralized cloud storage is designed to make everyone satisfy their data storage requirements by leasing cost-effective hard drive space within a peer-to-peer network. The functioning of the CESS network hinges on various roles:

- **Storage Nodes:** Responsible for data storage and distribution.
- **Consensus Nodes:** Responsible for recording transactions.

The economic structure plays a vital role in defining the storage capacities of nodes, evaluating their contributions to the network, and allocating rewards accordingly. This financial framework is an essential element of decentralized storage systems.

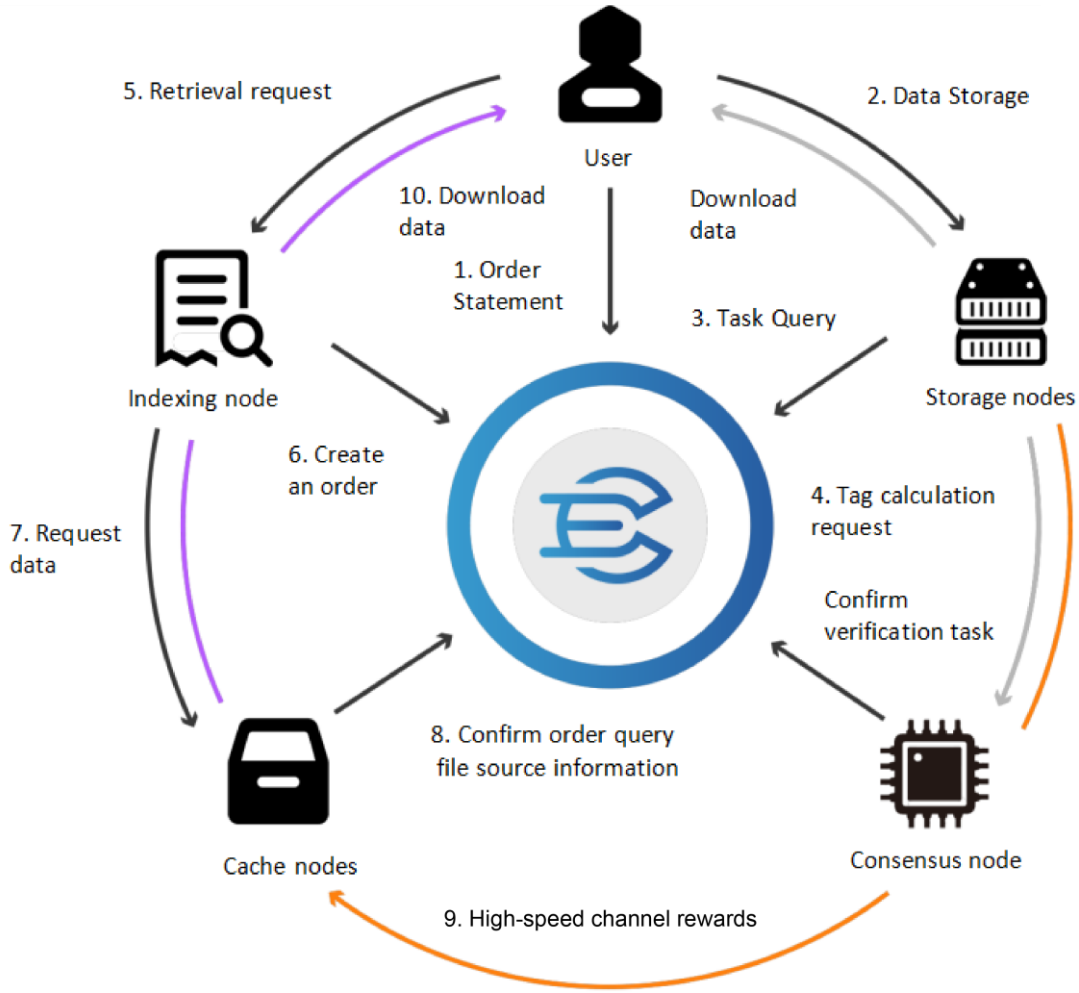

Figure 16. Economic Model

5.2 **Roles and Functions**

The operation of the CESS network necessitates the participation of various roles to support its upkeep and operation. In the initial stage of network creation, there are four primary roles: Storage-miner, Consensus-miner, Retrieval-miner, and Cache-miner.

5.2.1 **Storage miners**

Storage miners play a crucial role in the growth of the CESS network by providing necessary data storage capacity for the application layer. The effectiveness of these miners significantly impacts the network's performance. A verification procedure is in place to validate each miner node's storage capabilities, ensuring service excellence. Incentives, including mining rewards and a portion of storage service fees, are provided to encourage and reward these miners.

Storage miners provide massive, reliable, and scalable cloud storage services.

5.2.2 **Consensus Miners**

Consensus miners within the CESS network are essential for organizing transactions, validating them, maintaining blockchain data across the network, and supervising storage miners to guarantee their reliability. In return for their contributions, consensus miners are granted mining rewards. Furthermore, TEE-Workers are incentivized through mining rewards and a portion of storage service fees.

5.2.3 **Retrieval Miners**

Retrieval miners provide data retrieval services to the network by responding to "Get" requests and retrieving the requested data for users. After receiving a data retrieval request, retrieval miners search for the storage miner with the best overall performance to enhance the efficiency of data retrieval. Unlike storage miners, retrieval miners do not need to provide staking, submit stored data, or provide storage proofs. Unlike consensus miners, retrieval miners are not involved in transaction packaging or transaction verification.

5.2.4 **Cache Miners**

Cache miners deliver data to users, consensus miners, and storage miners quickly by efficiently indexing and distributing components.

Cache miners enhance data accessibility by employing a location-based storage selection (LBSS) recognition algorithm to dispatch data to the nearest content buffer node.

Cache miners receive mining rewards as incentives.

5.3 **Token Allocation Model**

CESS methodically arranges how to allocate CESS tokens among early adopters, miners, and partners.

CESS plans to publish a total of 10 billion tokens, with the following allocation:

- **Initial Contributors:** 15% of tokens are allocated to initial contributors.
- **Early Investors:** 10% of tokens are allocated to early investors.

- **Community Development, Incentives, and Advertising Expenses:** 10% of tokens are allocated for these purposes.
- **Cloud Partner Business Cooperation:** 5% of tokens are allocated for cooperation with cloud partners.
- **Foundation Reservation:** 5% of tokens are reserved for emergencies and future ecological development.
- For the storage network, up to 55% of the tokens are allocated as node incentives:
- **Storage Nodes:** 30% of tokens are allocated to storage nodes.
- **Consensus Nodes:** 15% of tokens are allocated to consensus nodes.
- **Cache Layer:** 10% of tokens are used for cache layer construction.

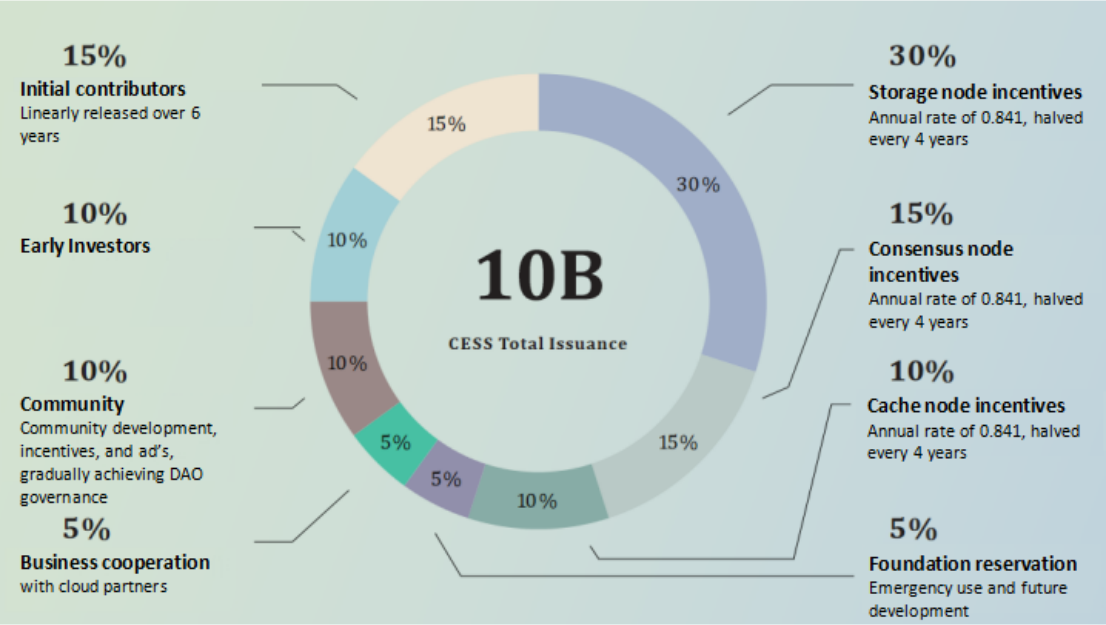

Figure 17. Token Allocation Model

5.4 **Consensus Node Incentive**

Consensus nodes are chosen at random using a rotating mechanism called Random Rotational Selection (R²S). Every era, **11** consensus nodes are selected from a pool of eligible candidates by R²S algorithm to produce blocks for the blockchain system. These nodes will be rewarded for their participation in block production. Their duties include packaging, verifying transactions, and storing blockchain data throughout the network. Incentives in the form of mining rewards are provided to encourage their continued participation.

5.5 **R²S consensus algorithm**

Upon joining the CESS network, every consensus node is required to maintain the network state and carry out data storage audits. To incentivize active participation in

these duties, a credit system has been implemented. This system evaluates each consensus node's credit score by considering the combined workload of TEE Workers linked to that node. The credit score is determined based on various factors, including:

- Total number of bytes to process inservice files.
- The total number of bytes of authentication/replacement idle space.
- Verify the total number of bytes of inservice data and idle space in random challenges.

  In each round of Era, validators are rotated based on their credit scores. According to the R²S mechanism, the **11** nodes with the highest scores are selected as validators for the Era.

- **R²S Score:** R²S score is calculated by the formula:

$$CreditScore * 0.5 + StakingScore * 0.3 + VRFScore * 0.2$$

5.6 **Node Incentive Mechanism**

Consensus nodes join the CESS storage network by staking a certain number of tokens and receive rewards based on the workload of participating in the consensus. For each Era, validators receive rewards in proportion to the Era points they collect. Era points are reward points obtained through payable actions, such as:

- Generate non-uncle block
- Generate a reference to a previously unreferenced uncle block
- Generate a referenced uncle block

(Note: Era is a collection of multiple epochs. After one era ends, the reward is settled. An era is about 6 hours.)

Uncle block is a relay chain block that is effective in all aspects but fails to become the main block. This happens when two or more validators become block producers in the same time slot, and the block produced by one validator reaches the next block producer before the other blocks. We call lagging blocks uncle blocks.

After every Era, rewards will be distributed. Regardless of their staking amount, all validators will split the block production rewards equally. However, individual validators' rewards may differ based on their Era points. While earning Era points involves some randomness and can be influenced by factors like network connection strength, validators who consistently perform well should generally accumulate a similar total of Era points over a significant number of Eras.

In addition, the validator can also receive a "tip" from the transaction sender as an incentive to include the transaction in the block it generates.

When a consensus node exits the network, it goes through a cooling-off period. During the cooling-off period, the pledged deposit is frozen and can only be redeemed after it is unfrozen.

5.7 **Storage Node Incentive**

Storage nodes play a crucial role in the CESS network by offering storage space, data storage, download services, and data verification. They can manage disk usage and allocate storage for network services. The more storage they provide, the greater benefits they receive. While allocating space is important, the advantages of storing data surpass those of simply providing space. Additionally, offering download services not only generates profits but also boosts scores. A positive credit increases the chances of attracting data storage requests and achieving higher profits.

Storage nodes demonstrate the authenticity of their certified unused capacity and stored inservice data by completing random challenges. These validated storage capabilities will be the foundation for contribution to the CESS network. Following the completion of a random challenge, storage nodes have the opportunity to share token rewards in proportion to their storage capabilities across the network.

The CESS network issues bonuses sourced from each Era. Each Era produces a fixed quantity of CESS tokens distributed according to the current bonus (total reward) ratio to the power of storage nodes compared to the total power in the present round. The power of storage nodes is determined by two components: idle space (idle_space) and inservice space (inservice_space). This design is to incentivize storage nodes to store real data. The calculation is shown below:

- **Storage Node Power**, which is calculated by the formula:

$$Inservice\ data(in\ bytes) * 0.7 + idle\ space(in\ bytes) * 0.3$$

- **Reward Per Round Distribution**, the Rewards are distributed based on the proportion of storage node power to the total power of the network. It is calculated by the formula:

$$\frac{(Total\ reward\ of\ this\ Era) * (hash\ power\ of\ the\ storage\ nodes)}{Total\ hash\ power\ of\ CESS\ network\ at\ the\ end\ of\ this\ Era}$$

Storage nodes join the storage network by pledging a set number of tokens, determined by their declared storage computing abilities. Once on the network, they can exit the network at any time but are required to assist the CESS network in completing data transfers to ensure the security of user data in the storage network.

Should a storage node repeatedly fail to complete random challenges throughout the service period by experiencing events like shutdowns, power outages, network disconnections, termination of mining processes, removal of hard drives, or deletion of user data, it will be forcibly expelled from the network and the funds pledged in its account will be deducted as a consequence.

6. **Transactions and Mining**

6.1 **Storage Markets: Verifiable and Trusted Markets**

Within the commercial storage sector, a network of providers offering storage

solutions to consumers exists. CESS aims to enhance this network and establish a verifiable and trusted marketplace. In the realm of CESS, the storage industry functions as a reliable and authenticated trading platform, allowing clients to procure affordable storage space directly from the CESS system for data storage purposes. The terms governing transactions in the CESS storage market are as follows:

- **Placing Orders:** The pricing structure for storage is completely transparent, allowing clients to set their prices according to market conditions before submitting orders to the CESS chain. The system only processes orders that have been validated. Once an order has been approved, it is final and cannot be altered.
- **Storage miners allocating resources:** 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 in the system token pool. The transaction fees paid by clients are put in the token pool too. Once 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.

6.2 **Storage Mining: Commercial Implementation of Decentralized Storage**

Implementation of decentralized storage requires miners to store legitimate data rather than arbitrary information. These storage miners are required to meet certain qualifications and stake CESS tokens as collateral. Failure to uphold their commitment and ensure data integrity will result in penalties deducted from their accounts, with transaction fees refunded to clients. Conversely, successful data integrity verification will earn mining rewards as CESS tokens deposited into their accounts.

6.3 **Storage Brokers: Improving Resource Integration in the Economy**

In enterprise-level resource allocation, decentralization does not always equate to disintermediation. This is particularly evident in the inefficiency and economic challenges when matching individual storage miners with storage demand in the trading market. The emergence of storage brokers effectively solves this issue by facilitating the provision and alignment of large-scale storage demands with available resources. By incorporating a broker service, the efficiency of the storage market can be significantly enhanced.

7. **Community Governance**

The CESS Decentralized Autonomous Organization (DAO) is an innovative entity that functions through a series of transparent computer programs, enabling a decentralized system of governance. Within this framework, individuals who hold CESS tokens are granted the opportunity to become top-tier members of the DAO, empowered with significant authority independent of centralized control. This structure allows members to propose and participate in voting on various governance matters, thereby influencing the trajectory and development of the community.

Central to the operation of the CESS DAO is the principle of community consensus, which serves as the driving force behind the organization's fair and effective governance processes. Through active participation and engagement in decision-making, members collectively shape the direction of the CESS ecosystem toward its optimal potential. Furthermore, asset management within the DAO is conducted with utmost transparency, reflecting a commitment to principles of community-driven governance. By openly sharing rules, codes, incentives, and regulatory mechanisms, CESS aims to achieve decentralization and inclusivity within its network by providing equal opportunities for all individuals to engage in community governance activities.

8. **References**

[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] Sangeet Paul Choudary, Marshall.W.Van Alstyne, and Geoffrey G.Parker. "Platform Revolution, How Networked Markets are Transforming the Economy", 2016.

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

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

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

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

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

[9] 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.

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

[11] 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.