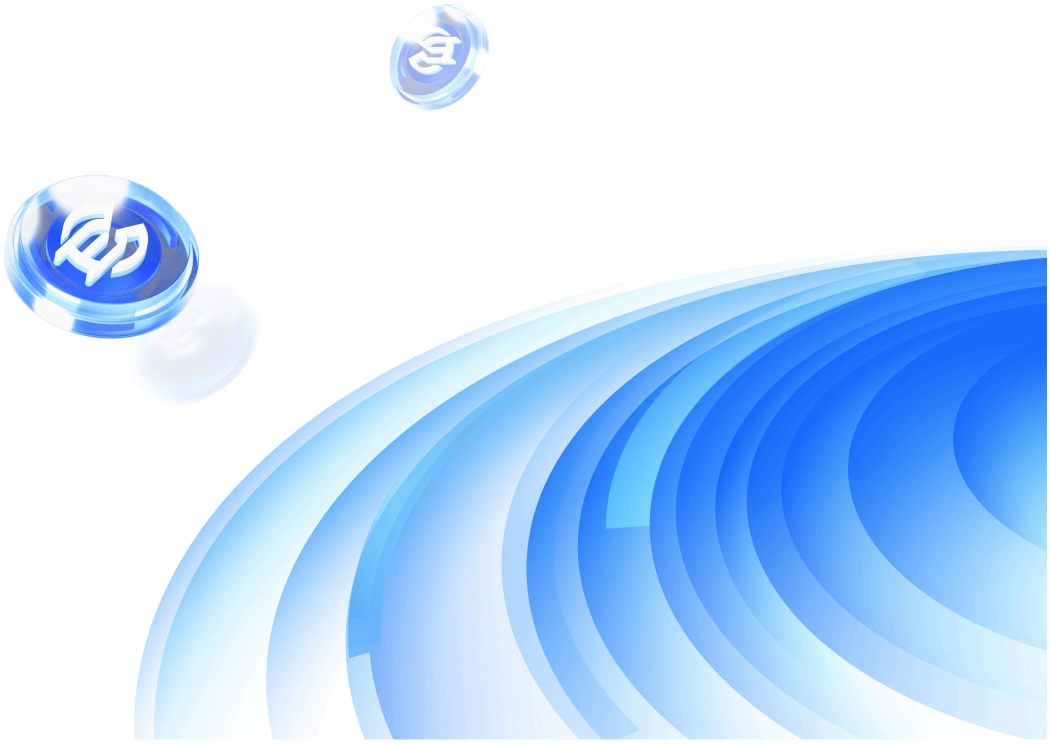
CESS

A Decentralized Data Value Infrastructure

White Paper v0.9.3

CESS Lab
June 2025



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.NETWORK/ (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.

CESS Network: A Decentralized Data Value Infrastructure

CESS Lab

hello@cess.network

V0.9.3

June 2025

Abstract

The abundant growth of data residing in the immense expanse of the AI 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, each a beacon of hope amidst the looming shadows cast by centralized control.

The CESS architecture is composed of several proprietary components, each engineered to mitigate risks associated with centralization and enhance overall network performance:

Data Integrity and Blockchain-based [1] Disaster Recovery: Proof of Data Reduplication and Recovery (PoDR^2), which enables an almost zero data loss rate with high assurance capability.

Smart Space Management: Proof of Idle Space (PoIS), optimizes available storage space by pooling all storage resources within the network, organizing storage space into idle files, and using a Merkle hash tree to verify the integrity of each idle file. This storage resource execution mode is called Smart Space Management.

Protect Data Ownership, Privacy, and Security: Mechanisms such as Multi-Format Data Rights Confirmation (MDRC), Proxy Re-encryption Technology (PReT), and Trusted Execution Environment (TEE) ensure data integrity, security, traceability, and privacy.

Massive Storage Capacity: A first-of-its-kind, Decentralized Object Storage Service (DeOSS), technology is another solution pioneered by CESS. An S3 within the decentralized industry, decentralized object-based is a mass storage service.

Empowering AI With Data Privacy: CESS AI Agent Hub leverages distributed storage, computing, and blockchain-based security to aggregate and serve AI agents. CESS AI-LINK is a Byzantine-robust [2] circuit designed to protect user privacy and data sovereignty, allowing participants in each CESS node to collaboratively train a shared model without sharing their original data.

1. Introduction

With the rise of AI, people across the spectrum—from individuals to corporations and countries—are recognizing the crucial importance of data. Serving as the foundation for AI, data is essential for future competitiveness. However, solutions from centralized cloud data centers and decentralized storage systems are flawed. The issues of data loss, slow retrieval speeds, and unclear data sovereignty are prevalent. CESS seeks to tackle these issues by providing a cutting-edge decentralized data infrastructure designed to be transparent, efficient, and fair for every community [3] member.

CESS implements the following strategies to foster a highly collaborative and efficient ecosystem: Random Rotational Selection (**R^{2}S**) to ensure a fair and effective consensus while maintaining transparency and optimizing the content delivery network to enhance speed. Proof of Idle Space (**PoIS**) and Proof of Data Reduplication and Recovery (**PoDR^2**) guarantees data availability and robust backups across strong nodes. Proxy Re-encryption Technology (**PReT**) ensures that data visibility is restricted to authorized users, maintaining privacy and security by excluding all others. **CESS AI Agent Hub** is the decentralized entry point for thousands of specialized AI agents. **CESS AI-LINK** allows participants to collaborate and train decentralized AI models without exposing their original data.

CESS's ultimate market strategy goal is to emerge as the premier provider of cutting-edge solutions and technological standard protocols for vital data encryption, management, and value extraction in the AI era. This entails addressing the data management, encryption, and business needs of at least 25% of businesses worldwide, facilitating the efficient processing of data values ranging from several billion to trillions, and enhancing efficiency and value indices derived from improved data liquidity.

CESS system architecture, functional design, code implementation, and related aspects, demonstrate a strong determination to deliver high functionality and performance.

So, what is CESS?

CESS is a blockchain-powered decentralized cloud storage network with native Content Decentralized Delivery Network (**CD^{2}N**), where users and creators share data on-chain, and builders can create and deploy Decentralized Applications (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. The vision of CESS is to create a secure, transparent, and high-throughput decentralized data value network.

CESS is a public blockchain network based on a distributed storage system with milliseconds of high-speed CD^{2}N and empowers AI innovations by web3 protocols.

CESS is the First Layer 1 with infinite decentralized data storage space with milliseconds execution.

CESS is an innovative solution for entropy reduction in our ever-chaotic digital landscape:

$$\Delta CESS = \frac{\int \delta Q}{T} < 0 \tag{1}$$

2. Architecture

2.1. Overview

The CESS network features a cutting-edge modular design (see Figure 1). Its modules are adaptable, allowing for expansion or reduction based on requirements. Each module can operate independently or be integrated with others to deliver comprehensive services as a

single platform. Additionally, these modules can connect with external ecosystems, enabling collaborative responses to the dynamic nature of today's world.
CESS features two distinct module systems: the **CESS Protocol Suite** and the **XESS AI Protocol Suite**. Within these modules, the Interface serves to connect various components.
The CESS Protocol Suite is organized into three layers: the Blockchain Layer, the Distributed Storage Resource Layer, and the Content Decentralized Delivery Network Layer.

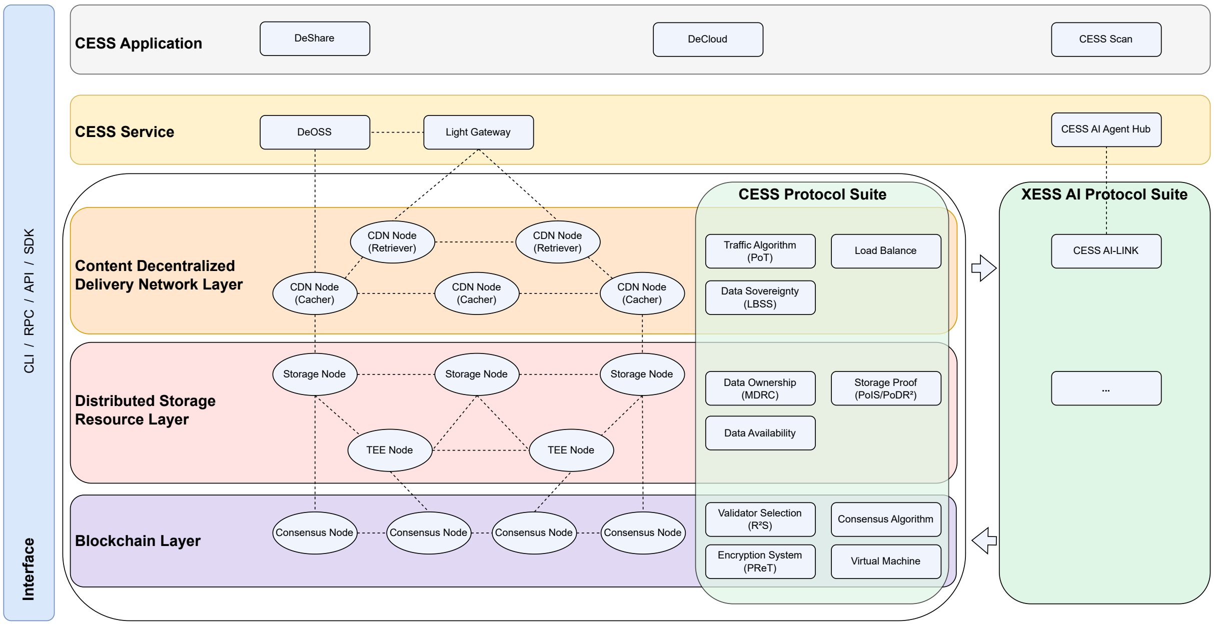


Figure 1 | *CESS Architecture*

- The **Blockchain Layer** provides blockchain solutions across the CESS network, promoting the integration of idle storage and computational resources into the network to support data storage, confirm data rights, and deliver additional application services.
- The **Distributed Storage Resource Layer** uses virtualization technology to realize the integration and pooling of storage resources. The infrastructure consists of storage capacity nodes and storage scheduling nodes.
- The **Content Decentralized Delivery Network Layer** utilizes content caching technology to ensure rapid distribution of stored data, involving both data index nodes and data delivery nodes in the process.

The **XESS AI Protocol Suite** leverages cutting-edge AI technologies to facilitate secure and private collaborative model training throughout the CESS network.

- The **CESS AI Agent Hub** offers a unified entry point to access, connect, and deploy AI agents across industries. Leveraging the data advantages of CESS Network, it simplifies the complexities of AI integration while offering a decentralized, scalable, and secure infrastructure.
- The core component of the XESS AI Protocol Suite is the **CESS AI-LINK**, which integrates federated learning mechanisms, allowing participants to train shared models without sharing their original data. Utilizing smart contracts [4], 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 **CESS Protocol Suite** and **XESS AI Protocol Suite** modules, 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 native blockchain, which has the following main technology stacks (Figure 2): physical stack, network stack, data stack, consensus stack, and incentive stack.

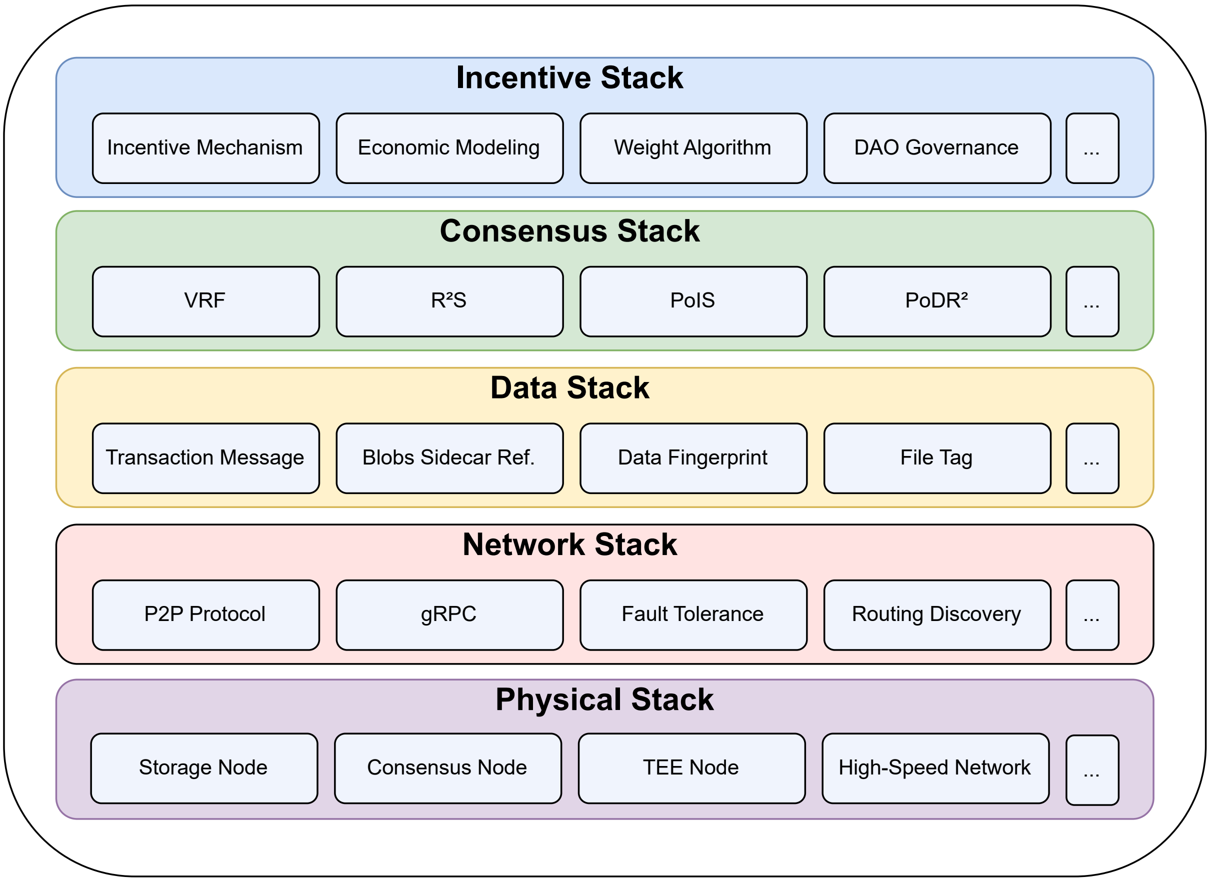


Figure 2 | *Blockchain Layer Technology Stack*

- **The physical stack** includes hardware components such as servers, networking devices, and storage.
- **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** distributes benefits through proof algorithm modeling and precise mathematical calculations.

Physical Stack

The physical stack 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.

Network Stack

CESS uses Distributed Hash Table (DHT) technology [5] within a peer-to-peer (P2P) network [6], facilitating communication between nodes through the P2P protocol. Nodes connected within the network share information and responsibilities directly, while routing information is continuously updated. 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.

Data Stack

The blockchain data and metadata are kept in the data stack to protect the security and integrity of user files throughout their transmission, storage, and verification, a range of industry-standard tools are employed. These include digital signatures, hashing algorithms, Merkle trees, and more.

Consensus Stack

CESS has developed a distinctive validator selection method known as **Random Rotational Selection ($\mathbf{R^2S}$)** to facilitate agreement on transactions and operations within the blockchain network. By combining $\mathbf{R^2S}$ with **GRANDPA**, which stands for Ghost-based Recursive ANcestor Deriving Prefix Agreement and serves as a deterministic finality mechanism, all nodes can reach a consensus on the blockchain's state at a specific moment.

Incentive Stack

The storage nodes manage file storage and the CDN nodes handle file delivery. These nodes get rewards corresponding 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 data integrity.

Data Storage Process

The CESS network boasts a refined procedure that guarantees efficiency and security throughout the data storage process. With intelligent services specifically designed for handling images, videos, and documents, CESS simplifies online data processing for its users while providing the ability to remove online data. Every data operation is trackable through the CESS blockchain.
When a client requests to store a data file, the CESS platform initiates a pre-processing step that extracts and stores the file's metadata and data fingerprints. This pre-processing also manages the replication of the data file and applies fault-tolerant erasure coding. The metadata encompasses details like the data owner's identity and associated keywords, while the data fingerprints are used for data ownership rights confirmation.
Figure 3 illustrates the CESS data storage workflow:

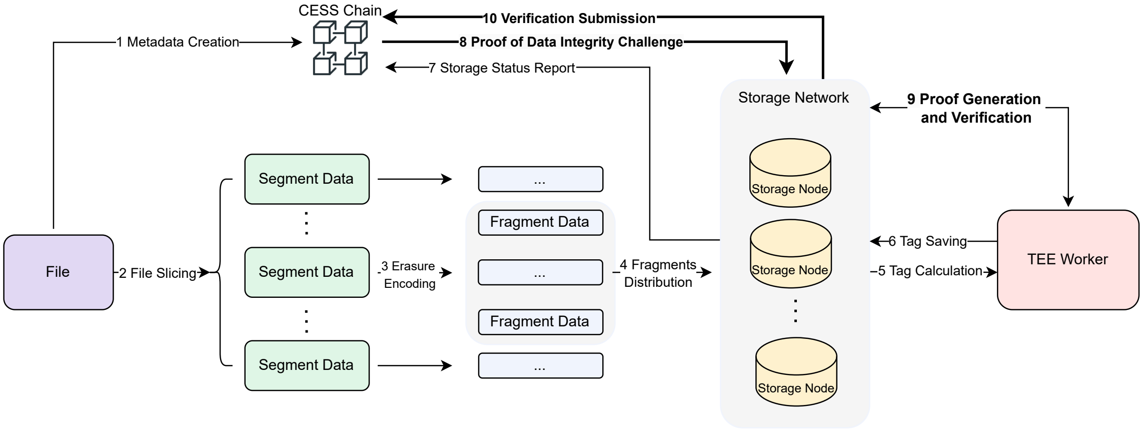


Figure 3 | *Data Storage Workflow*

1) User data files are uploaded and pre-processed by CESS client software. Metadata 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.

Steps 8 to 10 are a periodic challenge process.

Distributed Storage System

CESS offers a comprehensive and reliable object storage service by the 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 as object data.

The CESS Distributed Storage System incorporates advanced features that enhance data availability, performance, and security. By implementing **Data redundancy and replication mechanisms**, the system achieves high durability and resilience, safeguarding against node failures by distributing copies of data across various nodes. The storage infrastructure is built to be scalable and adaptable, efficiently managing varying workloads and large data volumes by expanding with additional storage nodes as demand increases. These storage nodes are added when users participate in the network as storage nodes, 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.

CESS guarantees data protection by utilizing Advanced Encryption Standards (AES) to secure information in transit and at rest. The network further strengthens security through robust access control mechanisms such as Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA). Moreover, it uses continuous auditing and monitoring tools to track data activities and access patterns as they occur. These elements offer a secure, scalable, and reliable storage solution within the CESS network.

2.2.3. Content Decentralized Delivery Network (CD^{2}N)

File access from CESS optimizes efficiency by integrating CDN and P2P technologies[5]. It reduces the need for numerous proxy servers, enhances system capacity, lowers costs, and sends data content to clients' autonomous domains by high-speed transfer technology. This improves the media access quality and boosts P2P network performance within a smaller autonomous system. The high-performance cache proxy server resolves the seed problem in pure peer-to-peer networks. Content is first published on the source node within the application, guaranteeing uninterrupted download services unless the node goes offline.

The implementation of CD^{2}N saves and provides downloads of the same content to multiple nodes, enabling 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 CD^{2}N are:

- **Dynamic Load Balancing**: The CD^{2}N 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 CD^{2}N 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 CD^{2}N layer is built to adjust its capacity according to demand fluctuations. AS demand grows, more nodes can be introduced to manage the extra load. Conversely, when demand decreases, resources can be reduced to minimize costs.
- **Security and Privacy**: The CD^{2}N layer incorporates advanced security measures to maintain data privacy and integrity. It implements encryption and secure key management for safeguarding data in transit and at rest. The blockchain technology is applied to create immutable ledgers for 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, providing uninterrupted service.
- **Analytics and Monitoring**: Comprehensive analytics and monitoring tools are integrated into the CD^{2}N 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 CD^{2}N 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 CD^{2}N layer includes energy-efficient protocols and hardware configurations to minimize the network carbon footprint. By optimizing resource utilization and employing green technologies, the system promotes sustainability.

The Decentralized Object Storage Service (DeOSS) is a decentralized object-based mass storage service that provides low-cost, secure, and scalable distributed data storage services for the web3 domain. It acts as an encryption proxy, access gateway, and content distribution platform for the CESS network.
The workflow of CD^{2}N is shown in Figure 4.
By integrating these advanced features, the CESS system's CD^{2}N layer provides a robust, efficient, and scalable solution for content distribution, leveraging the 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 geographic location or network conditions.

2.3. XESS AI Protocol Suite

Undoubtedly, AI constitutes the future trend. Nevertheless, in the wake of the rapid progress of AI research and technology, data abuse, the leakage of privacy, and legal supervision in many countries have all triggered the contemplation of human ethics and morality. CESS introduces the **XESS AI Protocol Suite** by leveraging our strengths in distributed storage and privacy computing standardizing AI technologies such as distributed training, inference, and AI applications on the protocol specification, and proposing solid solutions for creating responsible AI.
The XESS AI Protocol Suite is a pivotal addition to the CESS ecosystem, designed to harness the power of artificial intelligence while preserving data privacy and sovereignty. The XESS AI Protocol Suite operates alongside the CESS Protocol Suite with the Interface Layer, integrating advanced AI capabilities with the secure, decentralized infrastructure of the CESS network. As a multi-component service architecture for different AI application scenarios, system architects

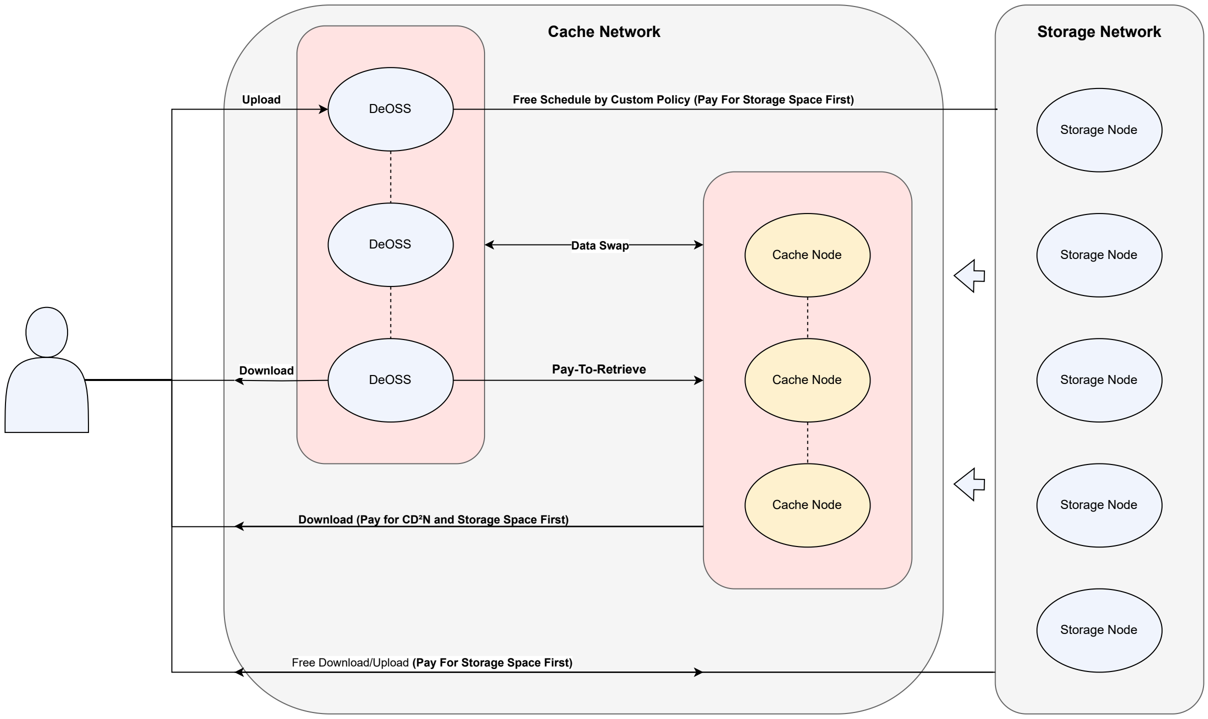


Figure 4 | *CD^2N Network*

can select the underlying components, build their service platform, and provide services to the outside world.

2.3.1. *CESS AI Agent Hub*

The core of **CESS AI Agent Hub** is the network's decentralized infrastructure and XESS AI Protocol Suite, which leverages distributed storage, computing, and blockchain-based security to aggregate and serve AI agents. The unique feature of CESS AI Agent Hub lies in its decentralized structure. Utilizing Blockchain technology and distributed computing, this platform enables the deployment and orchestration of AI agents in a decentralized manner.

2.3.2. *CESS AI-LINK*

CESS AI-LINK is central to the XESS AI Protocol Suite, a Byzantine-resilient system designed to prioritize privacy and uphold 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-LINK 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 Decentralized Physical Infrastructure Networks (**DePIN**s), enabling participants to engage in data sharing, or "mining", at any time.
The mission of CESS AI-LINK is empowering responsible AI by integrating trusted DePIN resources.

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, and reducing the coupling between different parts of the CESS network.

The Interface enables the efficient implementation of data storage services. It ensures secure and organized data management, allowing seamless access and manipulation. For 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. It contributes to delivering high-speed content, optimizes content distribution, and reliable high-performance data to end-users.

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

3. Key Technologies

3.1. Random Rotational Selection (R^{2}S)

The **Random Rotational Selection (R^{2}S)** consensus mechanism facilitates block production and manages on-chain transactions efficiently. This mechanism provides an open framework for users aspiring to become node operators, allowing them to join the pool of **candidate nodes**.

Within each window (e.g., every 3600 blocks), the R^{2}S protocol dynamically selects **11 rotation nodes** from the candidate pool to participate in block production. Candidate nodes not selected for block production are assigned auxiliary tasks, such as data preprocessing, enabling them to demonstrate their operational capabilities. This participation increases their likelihood of promotion to formal rotation nodes in subsequent rounds.

The R^{2}S mechanism integrates a **credit scoring system** evaluating node behavior and performance. Nodes engaging in malicious activities or failing to meet network requirements are penalized, resulting in a reduced credit score. Nodes with scores below a predefined threshold are disqualified from the candidate pool, preventing them from participating in future rotations. Similarly, formal rotation nodes that act maliciously or fail to fulfill their obligations are promptly removed. The protocol is continuous and fair by randomly selecting replacement nodes from the candidate pool.

R^{2}S optimizes security, decentralization, and efficiency by integrating a merit-based selection process with randomness and robust penalty measures, reassuring dependable block creation and smooth transaction handling within the CESS ecosystem.

3.1.1. Verifiable Random Function (VRF)

The CESS consensus model enhances blockchain security by introducing randomness and unpredictability in node selection. The model **randomly selects consensus nodes** from a pool of candidate nodes, which then collaborate to package and validate blocks using the consensus algorithms. Each candidate node is assigned a **public-private key pair $\boldsymbol{Pk}, \boldsymbol{Sk}$**. During each window, the selection of consensus nodes is determined by calculating a random hash output using the following formula:

$$\boldsymbol{R = VRF\_Hash\ (Sk, Seed)} \tag{2}$$

$$\boldsymbol{P = VRF\_Proof\ (Sk, Seed)} \tag{3}$$

Where:

- $\boldsymbol{Sk}$:The private key belonging to the candidate node,
- $\boldsymbol{Seed}$:A unique, unpredictable value derived from specific block information on the CESS chain,
- $\boldsymbol{R}$:A random hash output,
- $\boldsymbol{P}$:A proof hash confirming the authenticity of $\boldsymbol{R}$.

To verify the authenticity of the outputs, a verifier performs the following operations:

$$\boldsymbol{R = VRF\_P2H\ (P)} \tag{4}$$

$$\boldsymbol{VRF\_Verify\ (Pk, Seed, P)} \tag{5}$$

Where $\boldsymbol{Pk}$ is the public key of the corresponding candidate node. This process ensures that both $\boldsymbol{R}$ and $\boldsymbol{P}$ were generated by the node owning the private key $\boldsymbol{Sk}$.

Based on this algorithm, the consensus nodes for the time window are identified as the **11** nodes with the lowest random hash outputs $\boldsymbol{R}$. If the selection process yields more than **11** nodes, a **credibility scoring system** filters out the excess nodes, ensuring only the most reliable nodes participate in block production.

This approach combines verifiable randomness, cryptographic integrity, and a credibility-based filtering mechanism to strengthen security, fairness, and efficiency.

3.1.2. Access and Exit Regime

While CESS imposes no stringent entry requirements for nodes, participants must adhere to baseline operational and resource contribution standards necessary for network functionality. The nodes are required to stake a predefined amount of **$CESS** tokens as collateral to mitigate the risk of malicious activities. Once the token staking process is complete, nodes become eligible to participate in network operations.

For nodes to exit, the network conducts a performance evaluation determining the reimbursement of the staked tokens. In ideal circumstances—where the node maintains consistent connectivity, meets operational expectations, and refrains from malicious behavior—the collateral is fully refunded. However, penalties may apply for nodes exhibiting prolonged disconnections or intentional misconduct, resulting in partial or complete forfeiture of the staked tokens.

This Regime incentivizes honest behavior and strengthens network security by deterring attacks while promoting stable consensus operations.

3.1.3. Election and Block Production Process

The R^{2}S mechanism places a greater emphasis on node election and block production. The process demonstrates randomness, fairness, and efficiency in node selection while optimizing block generation. Below is an overview of the R^{2}S process:

- Nodes register as consensus nodes through staking, the current staking amount is **3 million $CESS** tokens.

- 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 [7].
- The selected validators generate blocks in order.
- The last epoch of each era begins the election of validators for the next era.

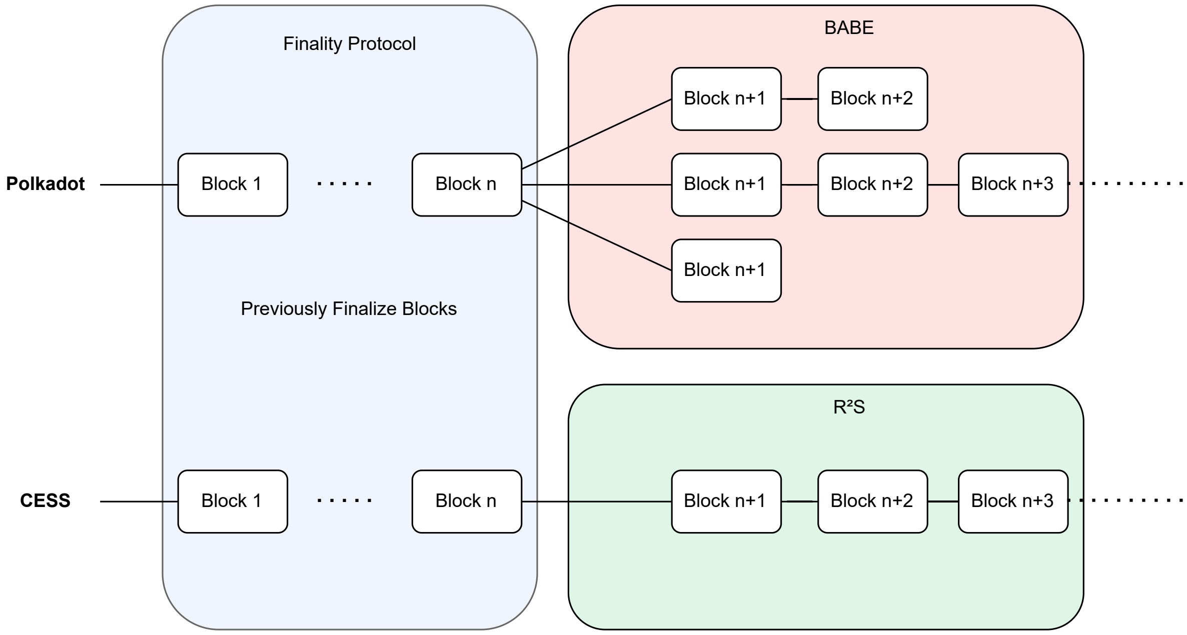


Figure 5 | *The Block Generation Difference between R^2S and BABE*

Upon joining the CESS network, consensus nodes uphold network integrity and perform critical tasks, including data preprocessing. CESS uses a credit-based system that evaluates each node's performance based on its contributions as a validator to incentivize active and reliable participation. This evaluation encompasses a variety of responsibilities, such as:

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

3.1.4. Advantages of R^2S

Avoid Monopoly and Centralization

The R^2S mechanism, is a decentralized approach to storing block history, preventing excessive centralization of large nodes that could harm the network's development.

Improve Consensus Efficiency

CESS selects 11 nodes within each era using R^2S 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

Web3 users are increasingly incentivized to contribute their idle storage resources to decentralized storage networks in exchange for rewards and utility. However, ensuring data integrity within these networks remains a critical challenge due to the prevalence of malicious behaviors among participants.

Two primary threats to data reliability are **storage space fraud** and **outsourcing attacks**. Storage space fraud involves nodes misrepresenting their available storage capacity: while outsourcing attacks occur when nodes collude to store multiple replicas of the same data across ostensibly independent nodes, undermining data redundancy and reliability.

Various cryptographic mechanisms have been proposed to mitigate these threats, including Proof of Storage, Proof of Replication, and Proof of Space-Time. These methods are designed to verify the authenticity of storage claims and ensure data is stored securely and redundantly. While these approaches have proven effective in theoretical and practical implementations, some may encounter scalability and efficiency bottlenecks, particularly in high-frequency data retrieval scenarios. Addressing these limitations is essential for maintaining the performance and security of decentralized storage networks, especially as they scale to support advanced applications like AI and Web3 ecosystems.

CESS introduced two innovative technologies to enhance its storage services: **Proof of Idle Space (PoIS)** and **Proof of Data Reduplication and Recovery (PoDR^2)**. **PoIS** validates the storage space offered by the storage nodes, which does not include the user's data; hence, idle space (aka. idle segment). **PoDR^2** is used to verify the user's data (aka. service segment) stored by storage nodes.

3.2.1. Proof of Idle Space (PoIS)

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. A viable solution involves using randomly generated data to occupy these vacant spaces. The available space on each node can be determined by calculating the volume 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 includes authentication, verification, and replacing idle space for storage nodes. Similar to the proof of in-service 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. To efficiently handle high-frequency dynamic operations like inserting and deleting user data, replacing large blocks of space tends to be sluggish. The CESS idle space-proof mechanism has been enhanced to accommodate the dynamic changes in storage.

Accumulator

An accumulator is a fixed-length byte sequence (or digest) obtained through a series of element "accumulation operations". One frequently used function is verifying 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 many elements. 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 includes multiple sub-accumulators. When updating an element within a sub-accumulator, only its parent and sibling accumulators' evidence needed recalculation layer by layer, without updates to other elements. For instance, in the illustrated two-level accumulator scenario (Figure 6), updating an element in *sub-acc*1 only requires recalculating *sub-acc*1 and *ACC*, followed by updating the evidence of *sub-acc*2...*sub-accN* to minimize unnecessary element updates.

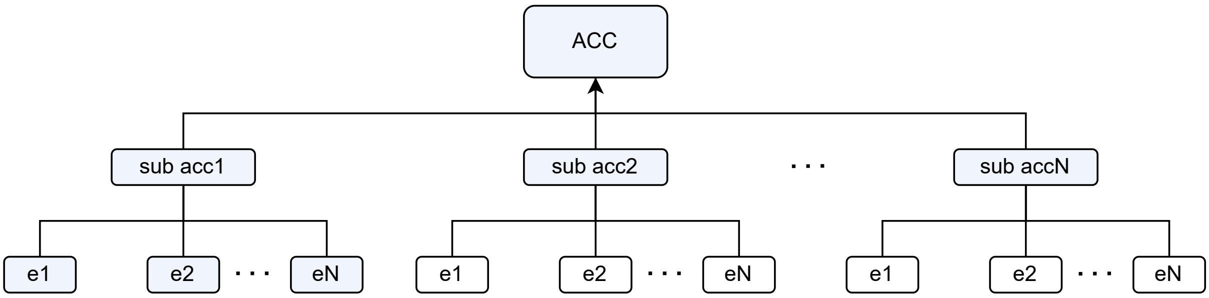


Figure 6 | *Accumulator and Sub-Accumulator*

Idle File Generation

Three criteria must be fulfilled whenever a prover creates idle files for 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 should not be able to use one idle file to authenticate multiple spaces or authenticate their space with idle files that do not belong to themselves. Thus, we can prevent witch attacks or other 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 $\boldsymbol{K+1}$ layers, $\boldsymbol{N} = \mathbf{4}$ vertices per layer, and $\boldsymbol{D} = \mathbf{2}$ in-degrees per vertex. Vertices that do not have any incoming edges are known as source points (e.g., the $\boldsymbol{V}_0$ layer), while those without outgoing edges are referred to as sink points (e.g., the $\boldsymbol{V}_k$ layer).

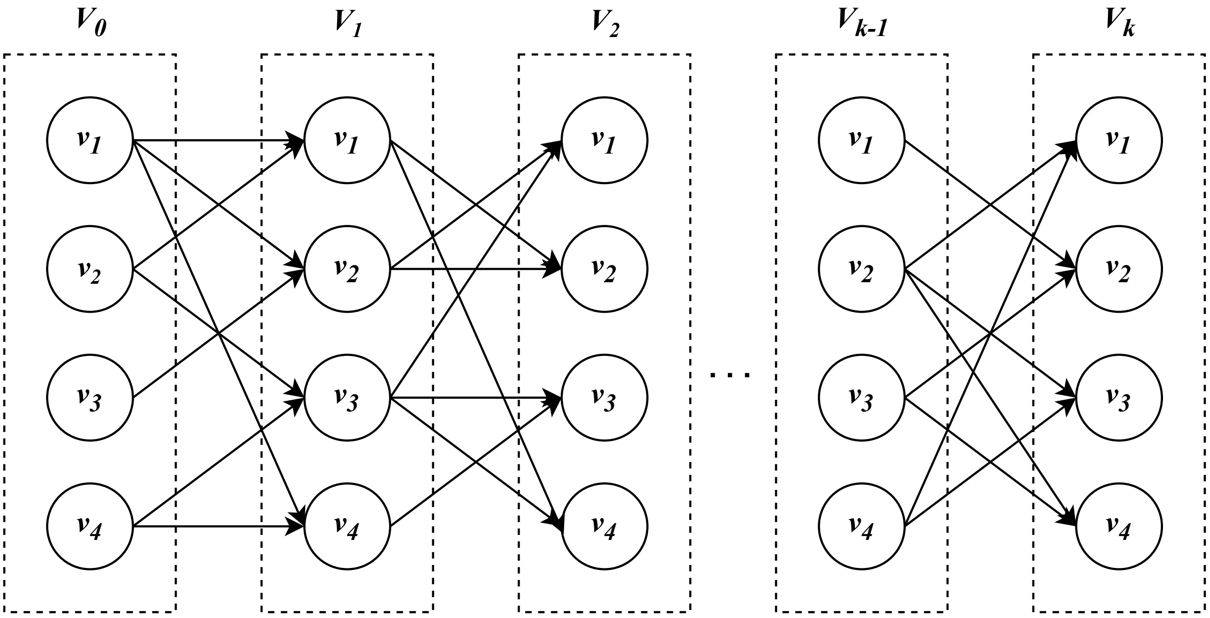


Figure 7 | *Idle File Generation*

One of the key features of PoIS is its dynamic proof of space mechanism, which allows nodes 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. Nodes can add or delete idle segments as needed, and they must respond to challenges from verifiers for the integrity of their stored space.

3.2.2. *Proof of Data Reduplication and Recovery (PoDR^2)*

The Proof of Data Reduplication and Recovery (PoDR^2) mechanism in the CESS network reassures data availability using Erasure Coding (EC). This technology involves breaking data into fragments, expanding and encoding them with redundant data pieces, and storing them across different storage nodes. The erasure coding redundancy enhances network reliability and can tolerate system failures.

In addition to Erasure Coding, CESS PoDR^2 implements Proof of Data Possession (PDP) [8] to prevent cheating behaviors. When a user uploads a file to the CESS network, PoDR^2 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 nodes 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).

When a storage node receives file fragments, it promptly requests the Trusted Execution Environment (TEE) of the consensus node to calculate PoDR^2 Tags. These tags are then saved alongside the file segment and utilized for generating PDP [8] proofs. After all storage nodes 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 node from producing proofs within the specified timeframe, resulting in penalties for failing to meet proof requirements.

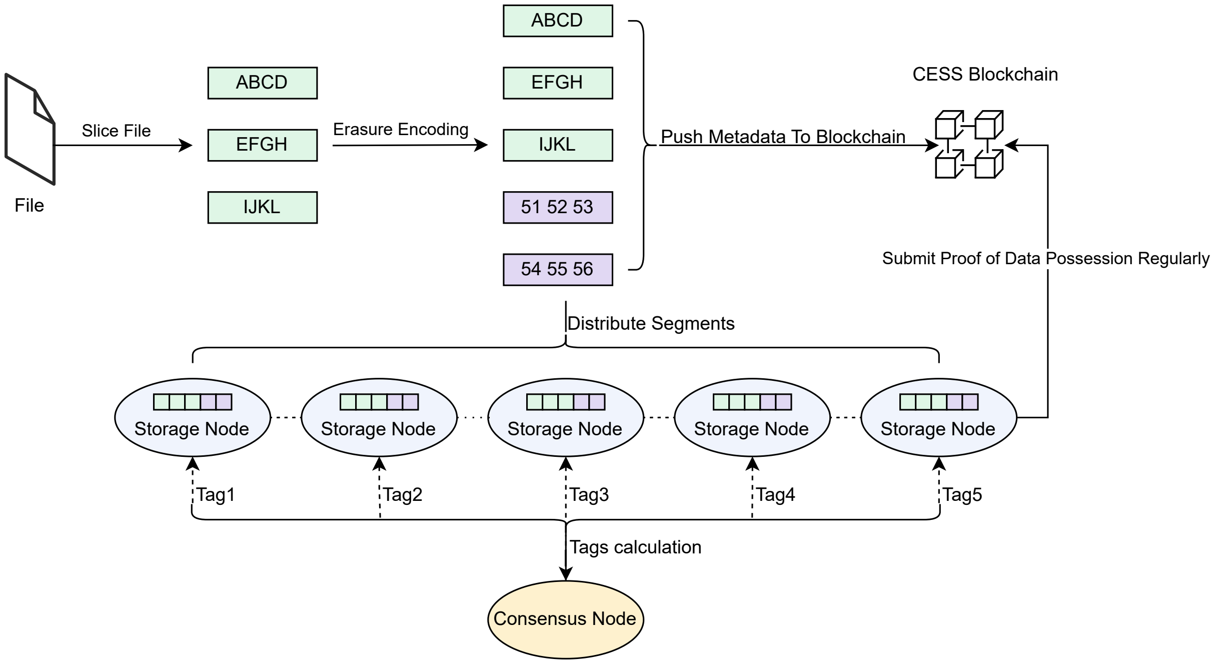


Figure 8 | *PoDR^2 Process*

The algorithm workflow (Figure 9) of PoDR^2 as follows.

- $\boldsymbol{KeyGen(\pi, k)}$: This algorithm is executed by TI and the DO. It takes the system's 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 a 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 $chal = \{(i, v_i)\}$.
- $\boldsymbol{ProofGen(chal, c)}$: 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 $Proof(\mu, \sigma)$.
- $\boldsymbol{Verify(pk, \mu, \sigma)}$: The algorithm is triggered by the smart contract on the BN, taking the pk and the $Proof(\mu, \sigma)$ as inputs, and outputs of the verification result.

Where:

- $\boldsymbol{DO}$: Data Owners,

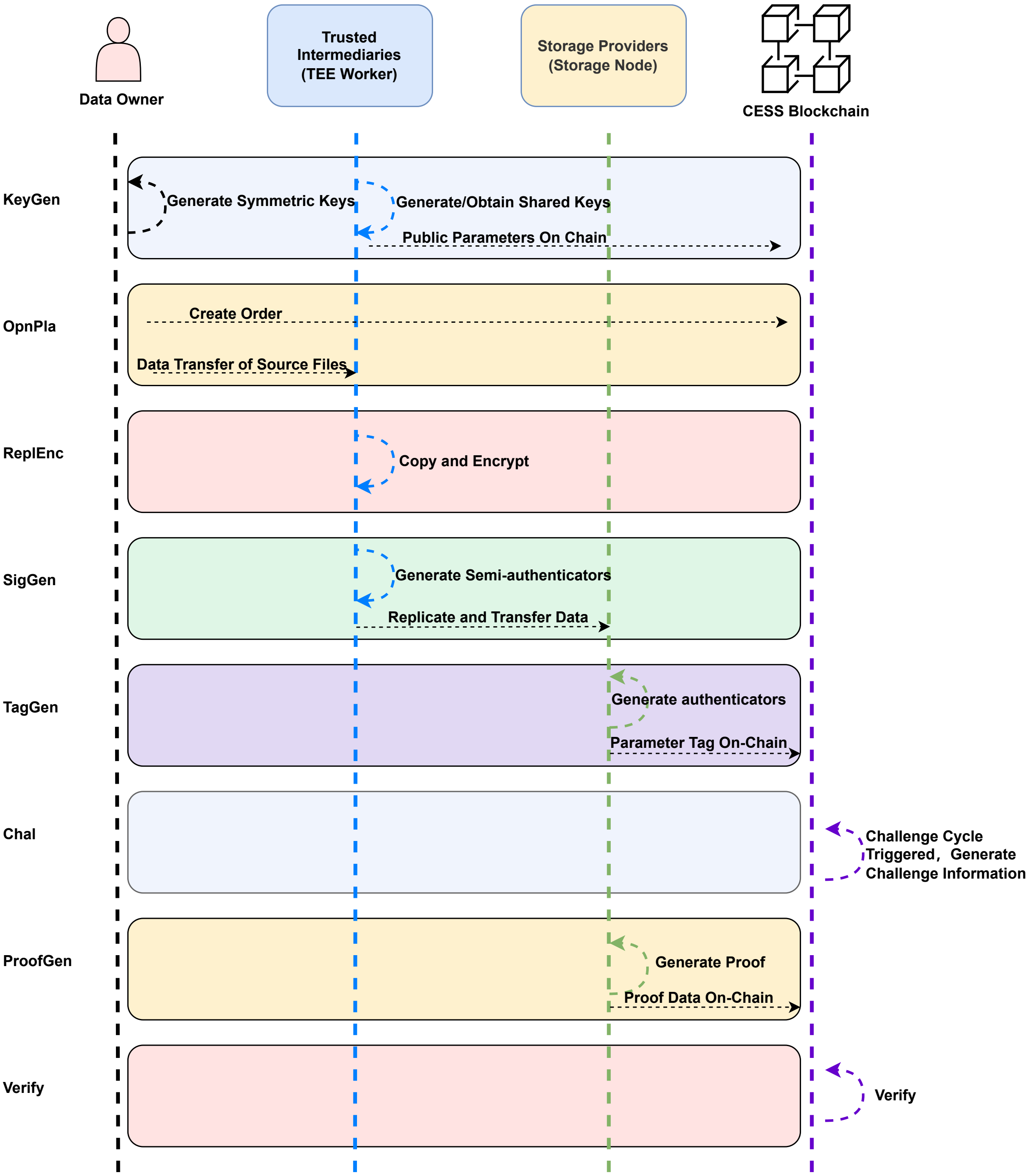

Data Owner
Trusted Intermediaries (TEE Worker)
Storage Providers (Storage Node)
CESS Blockchain
KeyGen
Generate Symmetric Keys
Generate/Obtain Shared Keys
Public Parameters On Chain
OpnPla
Create Order
Data Transfer of Source Files
ReplEnc
Copy and Encrypt
SigGen
Generate Semi-authenticators
Replicate and Transfer Data
TagGen
Generate authenticators
Parameter Tag On-Chain
Chal
Challenge Cycle Triggered, Generate Challenge Information
ProofGen
Generate Proof
Proof Data On-Chain
Verify
Verify

Figure 9 | *The algorithm workflow of PoDR*^{2}

- $\boldsymbol{TI}$: Trusted Intermediaries,
- $\boldsymbol{SP}$: Storage Providers,
- $\boldsymbol{BN}$: Blockchain Network.

PoDR^2 can identify and replace the missing file segment by replicating it to another storage node, guaranteeing the file remains accessible if a segment is lost due to a natural disaster or a node leaving the network.

Handling Large Files

Tagging large files can be time and resource-consuming, particularly in a TEE environment. Due to limited computing resources, generating tags for extensive files may not be feasible. CESS PoDR^2 overcomes this issue by dividing the data into smaller segments (Figure 10) before fragmentation supporting files of any size. This simplifies the process of computing Erasure coding and handling large files.
The CESS network, by breaking down large files into manageable segments, can maintain efficient tagging and verification processes, ensuring data integrity and availability.

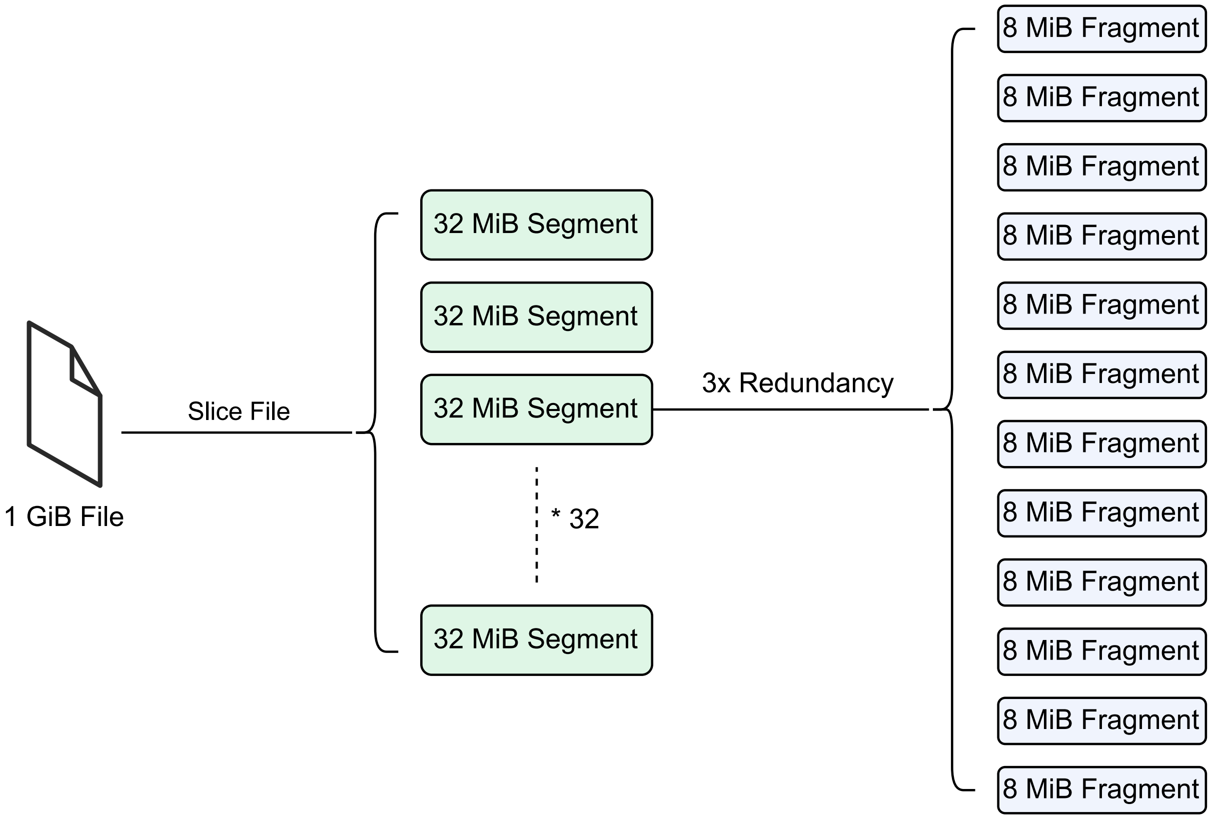


Figure 10 | *Slicing a File into Fragments*

Trusted Execution Environment (TEE)

The consensus nodes are equipped with a Trusted Execution Environment (TEE), a secure area of a processor designed to safeguard the confidentiality and integrity of the code and data it contains.
CESS TEE consists of a private key pair unknown to external applications. This key is used to

compute PoDR^2 Tags for each data fragment. The tag contains information like the fragment name and secret information encrypted by the PoDR^2 TEE's private key based on PDP [8][9]. Storage nodes compute their fragment tags in advance due to the time and resource-intensive process. Failing to do so can result in delays in producing storage proofs and being penalized.

3.3. Proxy Re-encryption

To safeguard user data, CESS applies encryption and disperses it among multiple storage nodes. 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 are developing a decentralized proxy re-encryption [10] [11] 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 nodes. Once authorized by the owner, the proxy re-encryption mechanism can grant access to specified entities by encrypting the nodes stored on the node, allowing designated parties to access others' data using their private keys.

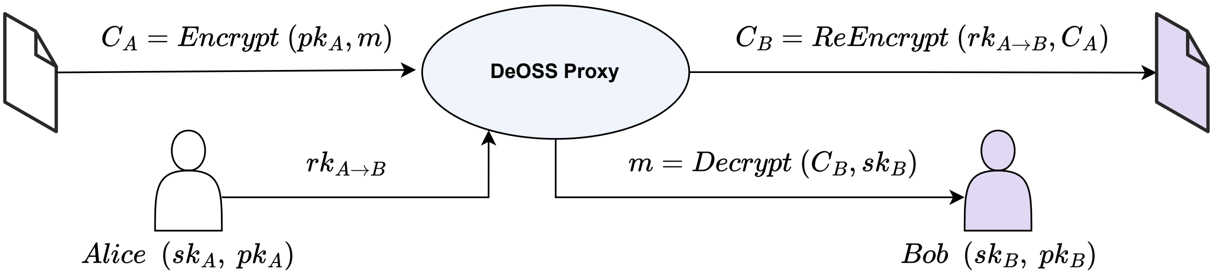

$C_A = Encrypt\ (pk_A, m)$
DeOSS Proxy
$C_B = ReEncrypt\ (rk_{A\to B}, C_A)$
$rk_{A\to B}$
$m = Decrypt\ (C_B, sk_B)$
$Alice\ \ (sk_A,\ pk_A)$
$Bob\ \ (sk_B,\ pk_B)$

Figure 11 | *Proxy Re-encryption*

As shown in Figure 11, we use DeoSS as the ReEncryption proxy:

- Alice encrypts a message $\boldsymbol{m}$, with Alice's public key $\boldsymbol{pk_A}$, resulting in ciphertext $\boldsymbol{C_A}$.
- Alice decides to delegate access to message $\boldsymbol{m}$ to Bob, who has the key pair $\boldsymbol{(sk_B, pk_B)}$.
- Alice creates a re-encryption key using her secret key and Bob's public key:

$$\boldsymbol{rk_{A\to B} = rekey\ (sk_A, pk_B)} \tag{6}$$

- DeOSS Proxy will re-encrypt $\boldsymbol{C_A}$ and which gets transformed into $\boldsymbol{C_B}$:

$$\boldsymbol{C_B = ReEncrypt(rk_{A\to B}, C_A)} \tag{7}$$

- Bob can then decrypt $\boldsymbol{C_B}$ using his secret key $\boldsymbol{sk_B}$, and get the Plaintext message $\boldsymbol{m}$:

$$\boldsymbol{m = Decrypt(C_B, sk_B)} \tag{8}$$

3.4. Multi-Format Data Rights Confirmation Mechanism (MDRC)

The data exchange market is vulnerable to cyber piracy, potentially undermining its ability to provide exclusive content to users without strong enforcement of data rights protection. The CESS advanced on-chain Multi-format Data Rights Confirmation Mechanism (MDRC) 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, protecting the premium content quality. MDRC can identify relationships between various datasets by analyzing their digital fingerprints. These authenticated fingerprints serve as proof of the data's origin, strengthening copyright protection and supporting the enforcement of data copyrights.

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 Figure 12 illustrates the overall process of MDRC.

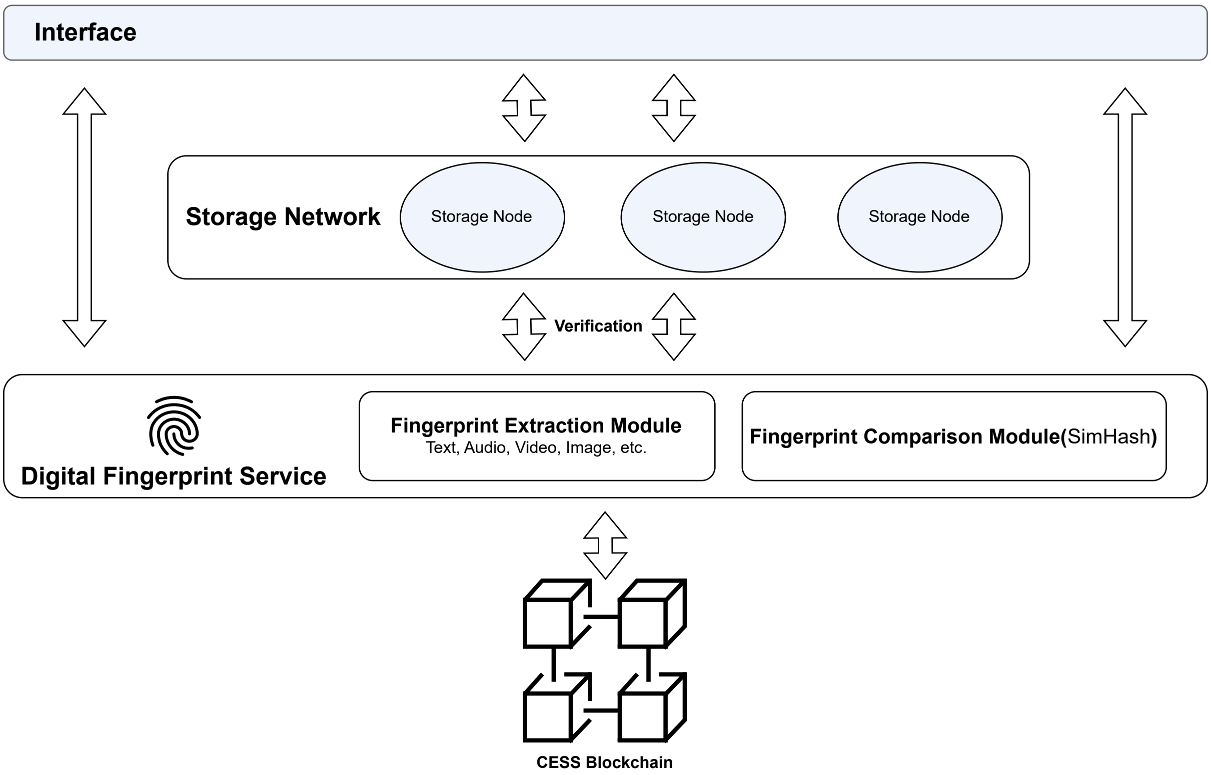

Interface
Storage Network
Storage Node
Storage Node
Storage Node
Verification
Digital Fingerprint Service
Fingerprint Extraction Module
Text, Audio, Video, Image, etc.
Fingerprint Comparison Module(SimHash)
CESS Blockchain

Figure 12 | *Multi-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**: Text data 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 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 technologies.

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. Simple MD5 or SHA values are used as their respective digital fingerprints for specific technology implementations of these data types.

Simhash algorithm [12] calculation occurs after obtaining the data fingerprint. 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.

The hamming distance detection technology compares 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. Location-Based Storage Selection (LBSS)

AI systems depend significantly on data for both their development and operation. However, the management of this data is complicated by various regulations, geographic restrictions (geo-fencing), concerns about national security, and differing privacy requirements—all of which make effective data management challenging.

3.5.1. Design principle

The LBSS feature of the CESS Network employs advanced algorithms and decentralized data storage to determine the optimal geographic location for data storage, considering several factors:

- **Compliance with Regulatory Frameworks**: Confirming that data is housed in the appropriate jurisdiction aligned with local data sovereignty laws.
- **Latency**: Minimizing the time required for AI systems to retrieve data, ensuring real-time or near-real-time access.
- **Cost Efficiency**: Reducing operational expenses such as storage and transaction fees by choosing the most cost-effective regions.

1) **Compliance Factor**
   The compliance factor in LBSS ensures that data storage choices meet legal standards. Data residency laws differ by region, the algorithm evaluates these regulations to ensure data storage complies with national and international data protection laws.
   The compliance score $C_{compliance}(L, D)$ serves as a crucial parameter in the LBSS decision-making process, reflecting the legal alignment of a storage location with the applicable jurisdiction's laws. The algorithm dynamically adjusts its compliance checks based on the dataset's relevant legal framework, guiding the selection of the most suitable storage region.
2) **Latency Factor**
   AI applications typically need access to real-time data for effective decision-making, reducing data retrieval times. The LBSS algorithm assesses the latency linked to each possible storage location.

The latency function, denoted as $T_{latency}(L, D))$, measures the round-trip time for data to travel between the storage location $\boldsymbol{L}$ and the user or AI model requesting the data $\boldsymbol{D}$, In the context of AI applications.
The LBSS system assesses the proximity of data centers to users or applications to minimize latency. Priority is given to storage locations closest to the user. This approach allows AI models to process real-time data more quickly and efficiently, thus enhancing both performance and the overall user experience.

3) **Cost Factor**
The cost of storing data in certain geographic areas can be higher than in others because of factors like energy prices, infrastructure costs, and transaction fees. The cost function $C_{cost}(L, D)$ estimates the total expense of storing data $\boldsymbol{D}$ at a specific location $\boldsymbol{L}$.

3.5.2. The LBSS Algorithm

The LBSS system utilizes a multi-factor optimization algorithm that assesses compliance, latency, and cost concurrently to identify the most suitable storage location. The primary goal is to determine the optimal storage location $\boldsymbol{L}$ for a dataset $\boldsymbol{D}$, as expressed by the following objective function:

$$L_{optimal} = \arg\min_{L \in \mathbb{L}} \left(\alpha \cdot C_{compliance}(L, D) + \beta \cdot T_{latency}(L, D) + \gamma \cdot C_{cost}(L, D)\right) \tag{9}$$

where:

- $\mathbb{L}$ is the set of all possible storage locations,
- α, β, γ are weighting factors that define the relative importance of the compliance, latency and cost. These factors can be dynamically adjusted based on the specific needs of the application (e.g., an AI-powered medical diagnostic tool may prioritize compliance over cost),
- $C_{compliance}(L, D)$, $T_{latency}(L, D)$, $C_{cost}(L, D)$ are the compliance, latency and cost factors, respectively, as described above.

By adjusting the weights of these factors, businesses and developers can customize the LBSS system to address their specific use case needs, whether they prioritize data security, performance, or cost.

3.6. CESS AI Agent Hub

One of the biggest bottlenecks in the AI industry is the lack of seamless interoperability between AI agents across different domains. Each sector—medical, finance, education, or autonomous driving—has its set of specialized agents, models, and data systems.
These agents may be homogenous or heterogeneous. They often operate in silos, making it challenging to integrate them or have them work together effectively. Their interactions are critical for the system to solve complex tasks collectively.
As in the web era, Yahoo became the portal for various sites, the **CESS AI Agent Hub** is designed to act as a decentralized entry point, bringing together thousands of specialized AI agents across industries like medical, financial, autonomous driving, and education.

3.6.1. Coordination and Cooperation Models

Cooperation refers to agents working together towards a common goal, while coordination involves agents managing their actions to avoid conflict or inefficiency.

1) **Information Flow Function**: The information shared between two agents represents an information flow function. Let the information flow between two agents $\boldsymbol{i}$ and $\boldsymbol{j}$ be denoted by $\boldsymbol{F_{ij}(t)}$, where t is the time step. This function could represent the transfer of messages, the sensor data exchange, or updates on tasks and goals.

$$\boldsymbol{F_{ij} = \alpha \cdot I_{ij}(t) \cdot D_{ij}(t)} \tag{10}$$

Where:

- $\boldsymbol{I_{ij}(t)}$ is the information content (such as the amount of data or messages exchanged),
- $\boldsymbol{D_{ij}(t)}$ is the distance in the communication channel, which could represent latency or security processing time,
- $\boldsymbol{\alpha}$ is a constant that factors in the efficiency or reliability of communication.

2) **Utility Function for Cooperation**: Each agent $\boldsymbol{i}$ in the system may have a utility function $\boldsymbol{U_i}$ that measures its benefit from a given interaction. The goal of each agent is to maximize its utility while also considering the utility of other agents for cooperation.
The utility function for the agent $\boldsymbol{i}$, in a cooperative setting with agents $\boldsymbol{j_1, j_1, \ldots, j_n}$ can be written as:

$$\boldsymbol{U_i = \sum_{j=1}^{n} \beta_{ij}(t) \cdot f_{ij}(t)} \tag{11}$$

where:

- $\boldsymbol{\beta_{ij}(t)}$ is the weight or importance of the communication with the agent $\boldsymbol{j}$,
- $\boldsymbol{f_{ij}(t)}$ is the performance function based on the communication and cooperation between $\boldsymbol{i}$ and $\boldsymbol{j}$ agents.
- $\boldsymbol{\alpha}$ is a constant that factors in the efficiency or reliability of communication.

3) **Coordination Strategy**: Coordination strategies ensure that agents do not perform conflicting actions. One common strategy is task allocation, where tasks are distributed among agents based on their capabilities and available resources. This can be modeled as an optimization problem:

$$\boldsymbol{max \sum_{i=1}^{n} R_i \cdot x_i \quad s.t. \quad \sum_{i=1}^{n} x_i = 1} \tag{12}$$

where:

- $\boldsymbol{R_i}$ is the resource or reward function for the agent $\boldsymbol{i}$,
- $\boldsymbol{x_i}$ is the binary allocation variable that determines whether the agent $\boldsymbol{i}$ takes on the task.

The solution to this optimization problem determines how tasks are assigned to agents to minimize conflict and maximize efficiency.

3.6.2. Technical Features

At the core of the CESS AI Agent Hub is CESS Network's decentralized infrastructure and XESS AI Protocol Suite, which leverages distributed storage, computing, and blockchain-based security to aggregate and serve AI agents. What truly sets CESS AI Agent Hub apart is its decentralized architecture. Powered by Blockchain and distributed computing, the platform allows for the decentralized deployment and orchestration of AI agents.

- **Scalability**: The CESS AI Agent Hub is designed for scalability. As demand grows across sectors like healthcare, finance, and autonomous driving, the decentralized nature of the system ensures that it can scale without compromising performance or security.
- **Fault Tolerance**: Decentralized systems are naturally more resilient to failures. If one node in the system goes down, the network can seamlessly reroute requests to other available nodes, ensuring uninterrupted service.
- **Enhanced Security**: By leveraging blockchain technology, CESS ensures that all AI interactions are secure, tamper-proof, and auditable. This is crucial, particularly in industries like finance and healthcare, where data privacy and integrity are paramount.
- **The Simplicity of Service Interfaces**: One of the standout features of CESS AI Agent Hub is its ease of use. Instead of managing complex configurations and integrating separate systems, users can access multiple AI agents through a single API call.

3.7. CESS AI-LINK

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 AI module generation.

In traditional federated learning (FL) [13], a central aggregator is typically required to maintain and update the global model. CESS AI-LINK offers a unique approach by operating as an aggregator-free FL system on a blockchain network, making it completely decentralized. With smart contracts, CESS AI-LINK can perform 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, reassuring privacy and data integrity through the Proof of Data Reduplication and Recovery (PoDR^2) mechanism.

CESS AI-LINK (Figure 13), a Byzantine-Robus Circuit from the CESS network, is designed to resist Byzantine attacks. 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 Decentralized GPU Computation Web3 DePINs. CESS AI-LINK revolutionizes secure and efficient machine learning processes in decentralized environments by enabling collaborative AI training without compromising data integrity.

Using the CESS network presents a sophisticated avenue for sharing parameters and models among various entities in organizational data exchange and model development. By utilizing CESS AI-LINK, which features a Byzantine-robust encryption system designed to preserve data privacy, organizations can safely conduct iterative procedures to improve and optimize their models. 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 reinforces the 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.

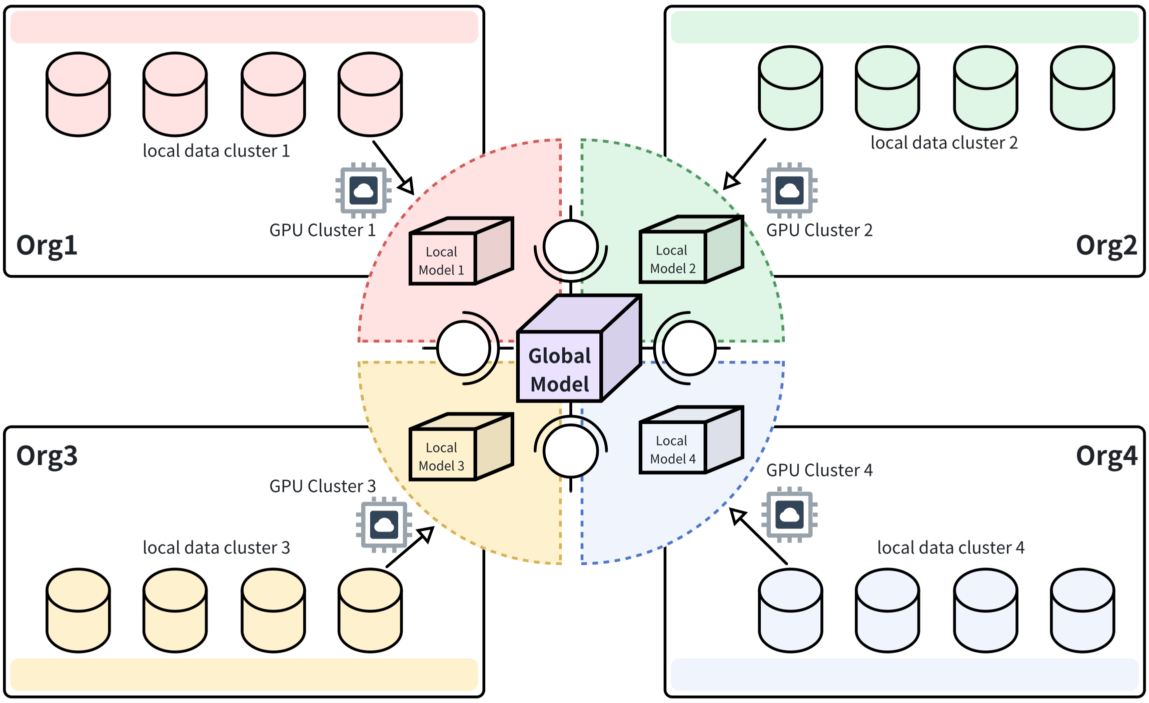


Figure 13 | *CESS AI-LINK*

4. Economic Model

4.1. Overview

The incentive framework of the CESS network is designed to encourage nodes to offer dependable and high-quality storage solutions, strengthening the network's ongoing performance. This system utilizes advanced mathematical algorithms to evaluate each node's activities and responsibilities within the ecosystem for a fair reward distribution.
Central to CESS is its economic model, which establishes the amount of storage each node contributes, assesses their value to the network, and allocates compensation correspondingly. This financial architecture is fundamental to the CESS operation.

4.2. Roles and Operational Structure

CESS relies on the collaboration of various node types, each vital to the network's health and function. There are **four** principal node categories within CESS: **Consensus Nodes**, **Storage Nodes**, **CDN Nodes**, and **TEE Nodes**.

4.2.1. Consensus Nodes

Consensus Nodes form the backbone of CESS's blockchain, assembling and publishing blocks via the proprietary **R^{2}S** consensus mechanism. R^{2}S builds upon traditional PoS systems by employing a dynamic process that randomly selects **11** validators per cycle, factoring in node workload, staked tokens, and an element of chance. Validators are instrumental in generating and confirming blocks and are compensated with CESS tokens.
Key functions of consensus nodes include:

- Record transaction outcomes and update system state.
- Facilitate decentralized peer-to-peer communication.
- Run the consensus algorithm to uphold data security and support the chain's expansion.
- Employ cryptographic tools for authentication and transaction validation.

Participants can either operate their consensus node to serve as **Validator**s or stake tokens to act as **Nominator**s, backing Validators and sharing in block rewards.

Validator

A Validator is a consensus node elected by the protocol during a specified timeframe. Their responsibilities include creating new blocks and verifying consistency within the blockchain during that period. Successful block creators earn rewards.

Nominator

Nominators are token holders who indirectly engage in consensus by staking their assets to support Validators, earning a portion of the Validators' rewards.

4.2.2. Storage Nodes

Storage Nodes form the foundational storage layer in CESS, protecting user data while effectively utilizing idle storage capacity via the **PoIS** mechanism. This mechanism identifies unused storage, allowing it to be converted for reliable persistent data storage through innovative management technologies.
To further protect data, CESS utilizes **PoDR**^{2}—a redundancy mechanism that allows swift recovery in case of data loss. When data is compromised, Storage Nodes automatically initiate restoration processes to maintain redundancy and high availability.
The network checks to verify available space and data integrity on Storage Nodes. Those who pass these verifications receive rewards. Thanks to simple command-line deployment tools, setting up a storage node is straightforward, allowing users to monetize spare storage resources with minimal setup.
Storage Nodes manage disk space, enforce overall storage quotas, and provide services such as storing data, retrieving files, and generating proofs. The more storage space a node contributes, the more incentive it receives.

4.2.3. CDN Nodes

In the CESS **CD**^{2}**N** system, CDN Nodes improve data access efficiency, evenly distribute network load, mitigate DDoS threats, and enable two-way data transfer between users and CESS. These nodes provide quick, seamless delivery both ways and support AI-related tasks such as datasets and models, which are essential for AI integration into CESS.
CDN Nodes are split into two main roles:

Retriever

Retrievers handle:

- Prompt the user for data fetching.
- Temporary caching of popular content for lower latency.

- Data processing (e.g., transformation or analytics).
- Load balancing across the network.
- Verifying traffic associated with cached data.

Retrievers share cached information throughout CESS for optimal data exchange and earn rewards for their computational efforts and bandwidth contributions.

Cacher

Cachers concentrate on light caching tasks and operate on energy-efficient DePIN devices. Their primary role is to store files accessed frequently, enhancing responsiveness. By leveraging multiple low-cost devices, Cachers contribute to scaling edge infrastructure. Their compensation depends on the quantity of data served.

The proliferation of Cachers enables virtually limitless scaling of edge caches by incorporating caching nodes into the network's data distribution framework.

4.2.4. TEE Nodes

Within the CESS network, TEE Nodes function inside the trusted execution environment (TEE), playing an essential part in upholding the security and reliability of the system. Their main responsibilities include verifying the authenticity of unused storage space and overseeing the initialization of user data, ensuring that all related processes occur in a highly secure and tamper-resistant setting.

Deploying a TEE Node is designed to be user-friendly—supported devices can be quickly set up using straightforward installation scripts. Once operational, these nodes help bolster the efficiency and effectiveness of both storage and consensus nodes by facilitating verification tasks. This enhances the network's scalability and security, allowing users to actively engage in and optimize consensus operations, strengthening the broader ecosystem.

TEE Nodes can operate under three distinct configurations: **Full Mode**, **Marker Mode**, and **Verifier Mode**. Each mode is tailored to specific functions within the trusted execution environment, offering users flexibility based on their needs and roles within the CESS infrastructure.

Full Mode

In Full Mode, TEE Nodes are fully engaged, executing all primary functions such as:

- **User Data Initialization**: Setting up and preparing active user data.
- **Idle Space Authentication and Replacement**: Checking and repurposing unused storage areas for new data.
- **Random Challenge Verification**: Validating random challenges related to idle storage and active data to maintain integrity and accessibility.

Nodes in Full Mode handle every critical operation required to maintain data integrity and availability across the CESS network.

Marker Mode

Marker Mode restricts the node's activities to specialized tasks that **exclude** random challenge verifications. In this configuration, TEE Nodes focus solely on authenticating and managing data without being tied to any consensus node or participating in challenge-based validations. This mode is ideal for scenarios where only basic data management is necessary.

Verifier Mode

Verifier Mode dedicates the TEE Node's resources exclusively to random challenges verification associated with idle and in-service data. The node in this mode must be linked to a consensus node to ensure its validation processes are properly synchronized with the consensus mechanism. This mode can also be incorporated as part of Full Mode for nodes that require comprehensive functionality.

Each operational mode allows TEE Nodes to specialize in different aspects of network maintenance, whether through complete oversight, focused data management, or dedicated integrity checks, to optimize performance and resource allocation according to the demands of the CESS network.

4.3. Incentive Mechanism

4.3.1. Consensus Node Incentive

Consensus nodes are selected at random via a rotation protocol known as R^{2}S. For each "**Era**", **11** nodes are drawn from a pool of qualified candidates by this algorithm to serve as block producers within the blockchain system. These selected nodes assemble blocks, verify transactions, and store essential blockchain data on the network. These nodes are motivated to receive mining rewards for fulfilling their duties.

Participants must stake a designated amount of tokens to become a consensus node within the CESS storage platform. The distribution of rewards is tied to each node's workload during consensus activities; specifically, rewards correspond to "**Era points**" which are accrued through various qualifying actions during each Era.

At the end of every Era, rewards are allocated among validators. All participating validators share block production rewards equally, regardless of their staked amounts; however, individual payouts may vary depending on how many Era points each validator has earned. While there is an element of randomness in earning these points, factors such as network connectivity can influence outcomes. Validators who consistently perform well should see their Era point totals converge over time.

Additionally, validators may receive optional transaction tips from senders as further incentive to include those transactions in newly created blocks.

If a consensus node chooses to leave the network, it enters a mandatory cooling-off period during which its staked deposit is temporarily locked. The deposit becomes available for withdrawal only after this period ends.

R^{2}S Score Formula

Upon joining the CESS network, every consensus node maintains the network state and carries out data storage audits. A credit system has been implemented to incentivize active participation. 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 or replacement idle space.
- Verify the total number of bytes of in-service data and idle space in random challenges.

In each round of Era, validators are rotated based on their credit scores. According to the R^{2}S mechanism, the 11 nodes with the highest scores are selected as validators for the Era.

The R^{2}S score is calculated by the formula:

$$\boldsymbol{CreditScore \times 0.5 + StakingScore \times 0.3 + VRFScore \times 0.2} \tag{13}$$

4.3.2. Storage Node Incentive

Storage nodes in the CESS network offer 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 merely allocating 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 in-service data by completing random challenges. These validated storage capabilities will be the foundation for contribution to the CESS network. Once a random challenge is completed, storage nodes can ger rewards in proportion to their storage capacity within 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 in-service 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:

$$\boldsymbol{Inservice\ data(in\ bytes) \times 0.7 + idle\ space(in\ bytes) \times 0.3} \tag{14}$$

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:

$$\boldsymbol{\frac{(Total\ reward\ of\ this\ Era) \times (hash\ power\ of\ the\ storage\ nodes)}{Total\ hash\ power\ of\ CESS\ network\ at\ the\ end\ of\ this\ Era}} \tag{15}$$

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.

4.3.3. CDN Node Incentive

Users are incentivized to ensure high availability and performance, as CDN nodes within this globally distributed network will receive rewards.

4.3.4. TEE Node Incentive

The TEE Node acts as a bridge for consensus nodes, streamlining the process of validating random challenges that verify both idle storage capacity and the integrity of active data. Although it does not earn rewards directly, the TEE Node's activities improve the effectiveness of storage nodes. As a result, this indirectly increases the chances for connected consensus nodes to be chosen as validators.

4.4. Tokenomics

CESS methodically arranges how to allocate CESS tokens among early adopters, nodes, and partners. CESS plans to publish a total of **10 billion** $CESS tokens, with the following allocation (Figure 14) plan:

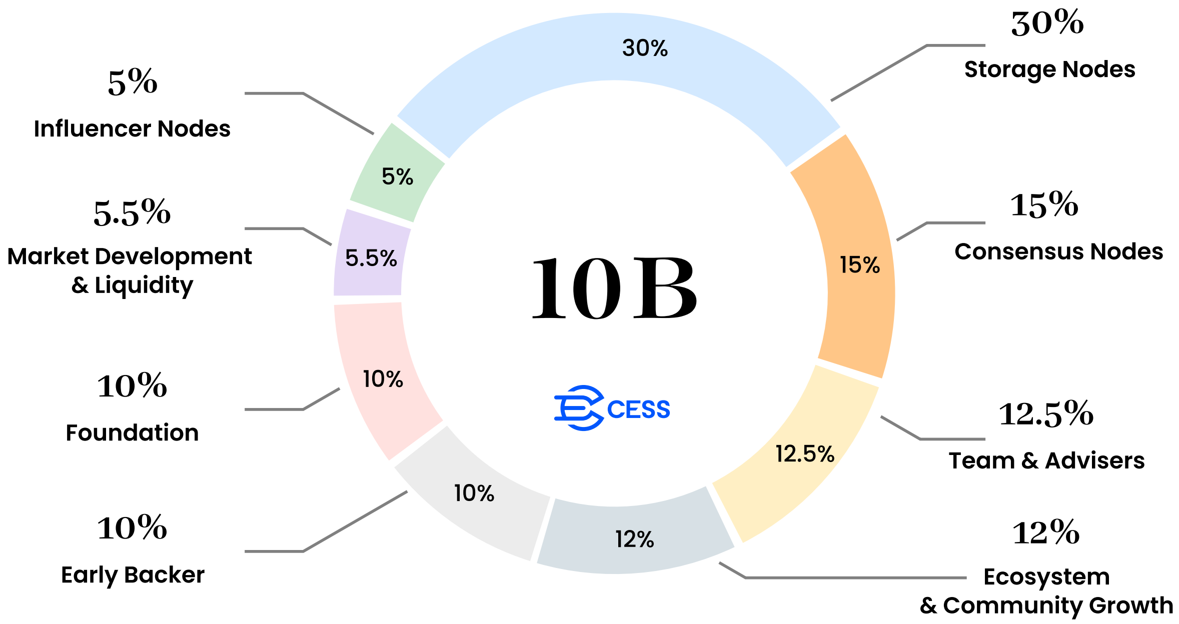


Figure 14 | *CESS Token Distribution Plan*

5. 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.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In OsDI, volume 99, pages 173–186, 1999.

[3] Geoffrey G Parker, Marshall W Van Alstyne, and Sangeet Paul Choudary. Platform revolution: How networked markets are transforming the economy and how to make them work for you. WW Norton & Company, 2016.

[4] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. white paper, 3(37):2–1, 2014.

[5] Sean Rhea, Dennis Geels, Timothy Roscoe, John Kubiatowicz, et al. Handling churn in a dht. In Proceedings of the USENIX annual technical conference, volume 6, pages 127–140. Boston, MA, USA, 2004.

[6] Thomas Karagiannis, Andre Broido, Michalis Faloutsos, and KC Claffy. Transport layer identification of p2p traffic. In Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, pages 121–134, 2004.

[7] Silvio Micali, Michael Rabin, and Salil Vadhan. Verifiable random functions. In 40th annual symposium on foundations of computer science (cat. No. 99CB37039), pages 120–130. IEEE, 1999.

[8] David E Rumelhart, Paul Smolensky, James L McClelland, and G Hinton. Sequential thought processes in pdp models. Parallel distributed processing: explorations in the microstructures of cognition, 2:3–57, 1986.

[9] Reza Curtmola, Osama Khan, Randal Burns, and Giuseppe Ateniese. Mr-pdp: Multiple-replica provable data possession. In 2008 the 28th international conference on distributed computing systems, pages 411–420. IEEE, 2008.

[10] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security (TISSEC), 9(1):1–30, 2006.

[11] Matthew Green and Giuseppe Ateniese. Identity-based proxy re-encryption. In Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007. Proceedings 5, pages 288–306. Springer, 2007.

[12] Md Sharif Uddin, Chanchal K Roy, Kevin A Schneider, and Abram Hindle. On the effectiveness of simhash for detecting near-miss clones in large scale software systems. In 2011 18th Working Conference on Reverse Engineering, pages 13–22. IEEE, 2011.

[13] Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. Advances and open problems in federated learning. Foundations and trends® in machine learning, 14(1–2):1–210, 2021.