CESS Network

The Decentralized Data Infrastructure

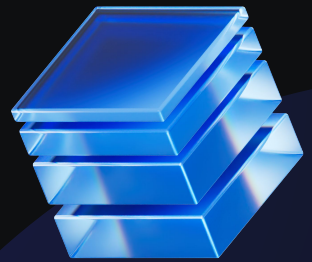
Episode 2: Blockchain Architecture & Key Technologies

https://www.cess.network

Course Logistics

Course Website: https://course.cess.network/

Episode 1	CESS Network Introduction
Episode 2	CESS Architecture & Key Technologies
Episode 3	CESS Ecosystem, Account Setup, and Applications
Episode 4	CESS Nodes & CESS Account Setup
Episode 5	Demo: Running a Consensus Node
Episode 6	Demo: Running a Storage Node
Episode 7	CESS DeOSS and DeOSS REST API
Episode 8	dApp Development using ink! Smart Contract
Episode 9	dApp Development using Solidity Smart Contract
Episode 10	Building Custom Pallet



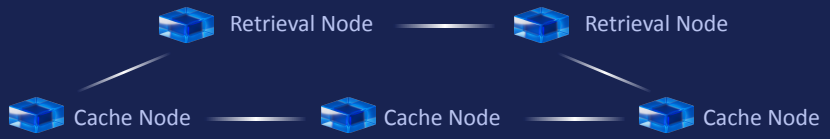
CESS Network Architecture

CESS

Interface CLI RPC API SDK

CESS Protocol Suite

Distributed Content Delivery Layer



Distributed Storage Resource Layer

CESS Blockchain

Smart Contract	Data Ownership (MDRC)	Data Availability	CESS Scan
Validator Selection (R^2S)	Consensus Algorithm (PoIS/PoDR^2)	Encryption System (PReT)	Virtual Machine

XESS AI Protocol Suite

CESS AI-LINK

And Many Others

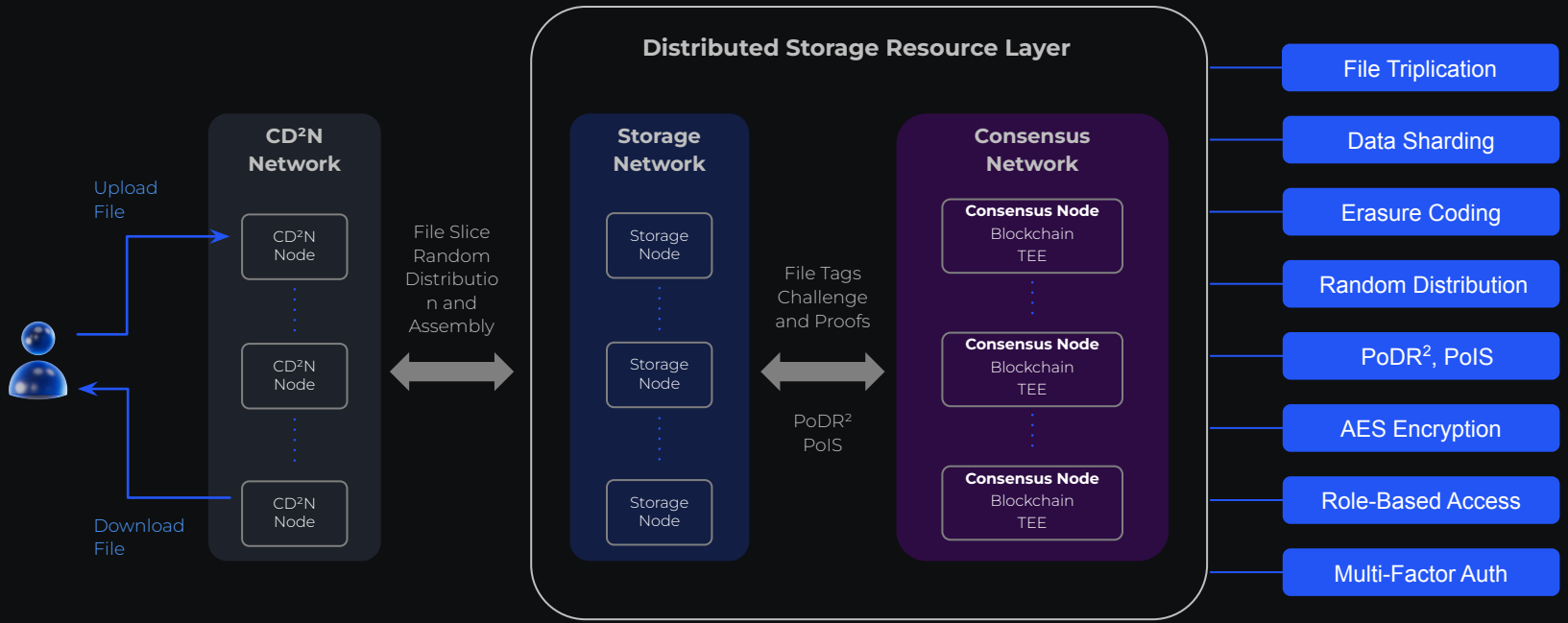
...

CESS Blockchain Layer

CESS

Incentive Stack	Incentive Mechanism	Economic Modeling	Weight Algorithm	DAO Governance
Consensus Stack	VRF	R^2S	PoIS	$PoDR^2$
Data Stack	Transaction Message	Blobs Sidecar Ref.	Data Fingerprint	File Tag
Network Stack	P2P Protocol	gRPC	Fault Tolerance	Route Discovery
Physical Stack	Storage Node	Consensus Node	TEE Node	High-Speed Network

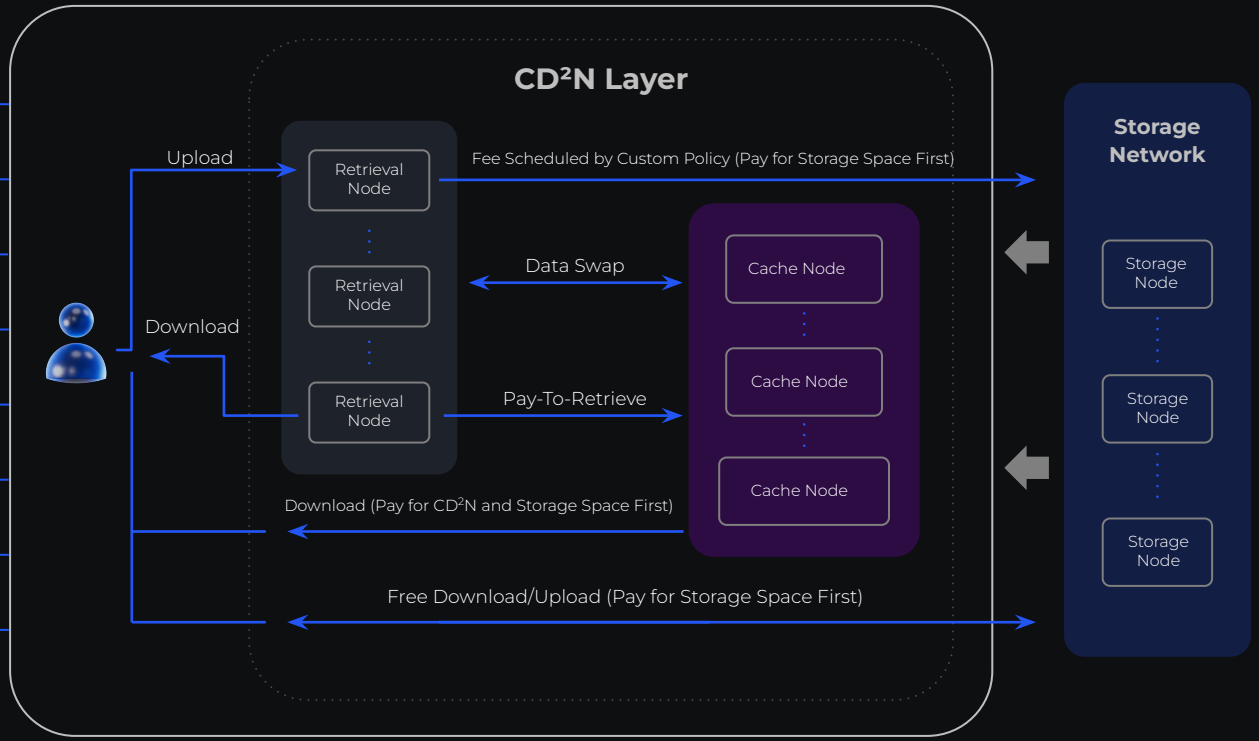
Distributed Storage Resource Layer



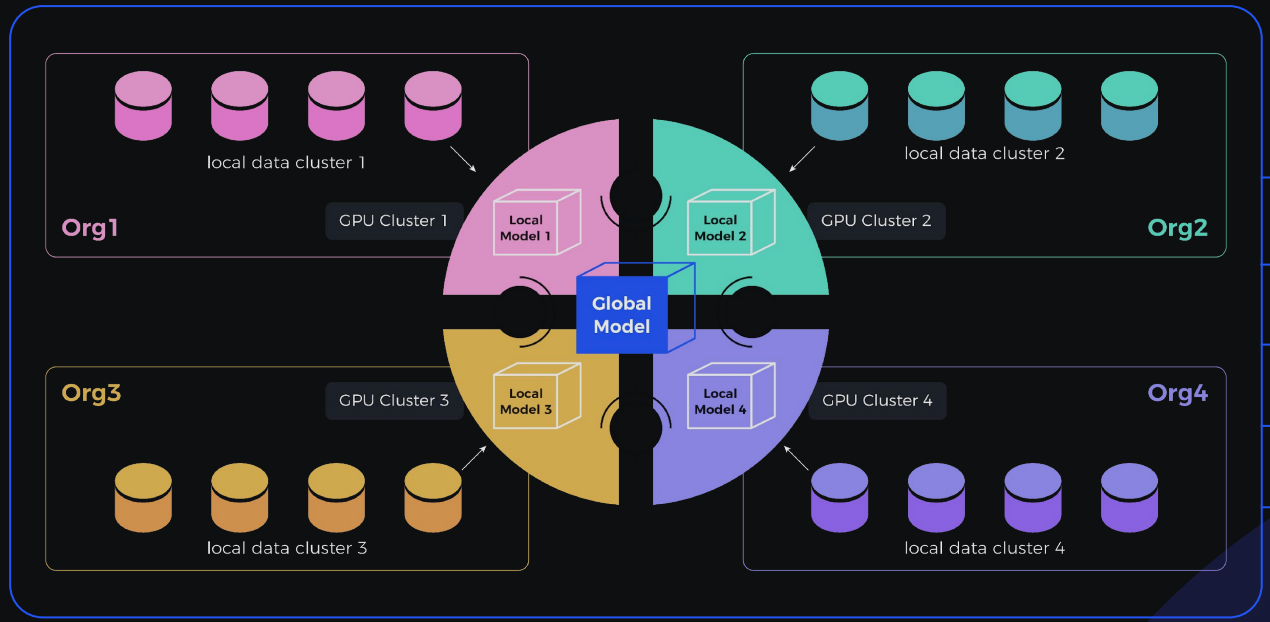
Content Distributed Delivery Network (CD²N) Layer

CESS

- Dynamic Load Balancing
- Edge Computing
- Scalability and Elasticity
- Security and Privacy
- Fault Tolerance
- Analytics and Monitoring
- Interoperability with other Networks
- Energy Efficient



CESS AI-LINK



- Byzantine-robust Circuit
- AI Model Training
- Prevents Data Leaks
- Privacy Preserving
- Eliminate Data Sharing

Industrial Challenges & CESS Solutions

CESS

Industry Challenges

- Data Vulnerability
- Ownership Rights
- Poor Economics Model
- No Private Data Sharing
- No Privacy-Preserving AI Model Training
- Inefficient use of Storage Space

Key Technologies

- Proof of Data Reduplication and Recovery(PoDR^2)
- Multiple-Format Data Rights Confirmation Mechanism (MDRC)
- Random Rotational Selection (R^{2}S) Consensus Mechanism
- Proxy Re-encryption
- CESS AI-LINK
- Smart Space Management System

Challenge 1: Data Vulnerability

CESS

Unexpected Node Failure

- Impact on data availability and integrity
- Need for robust redundancy and recovery mechanisms

Storage Nodes Quit

- Loss of storage capacity and increased risk of data loss
- Importance of incentivizing long-term participation

Hack Attempts

- Persistent threat to data security
- Necessity for advanced encryption and security protocols

CESS Solution

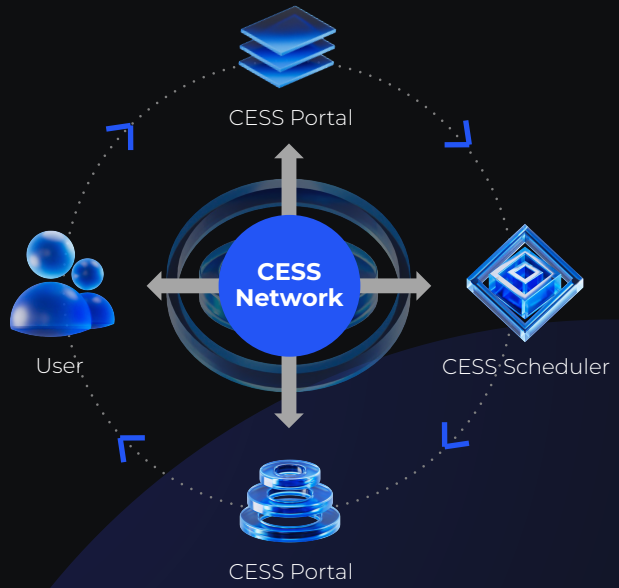
Proof of Data Reduplication and Recovery (PoDR^2)
Proof of Idle Space (PoIS)

Challenge 1 - CESS Solution: PoDR²

How to ensure that these files are stored safely and correctly on the hard disk?

The storage proof mechanism of **CESS** is **Proof of Data Reduplication and Recovery (PoDR²)**, which with:

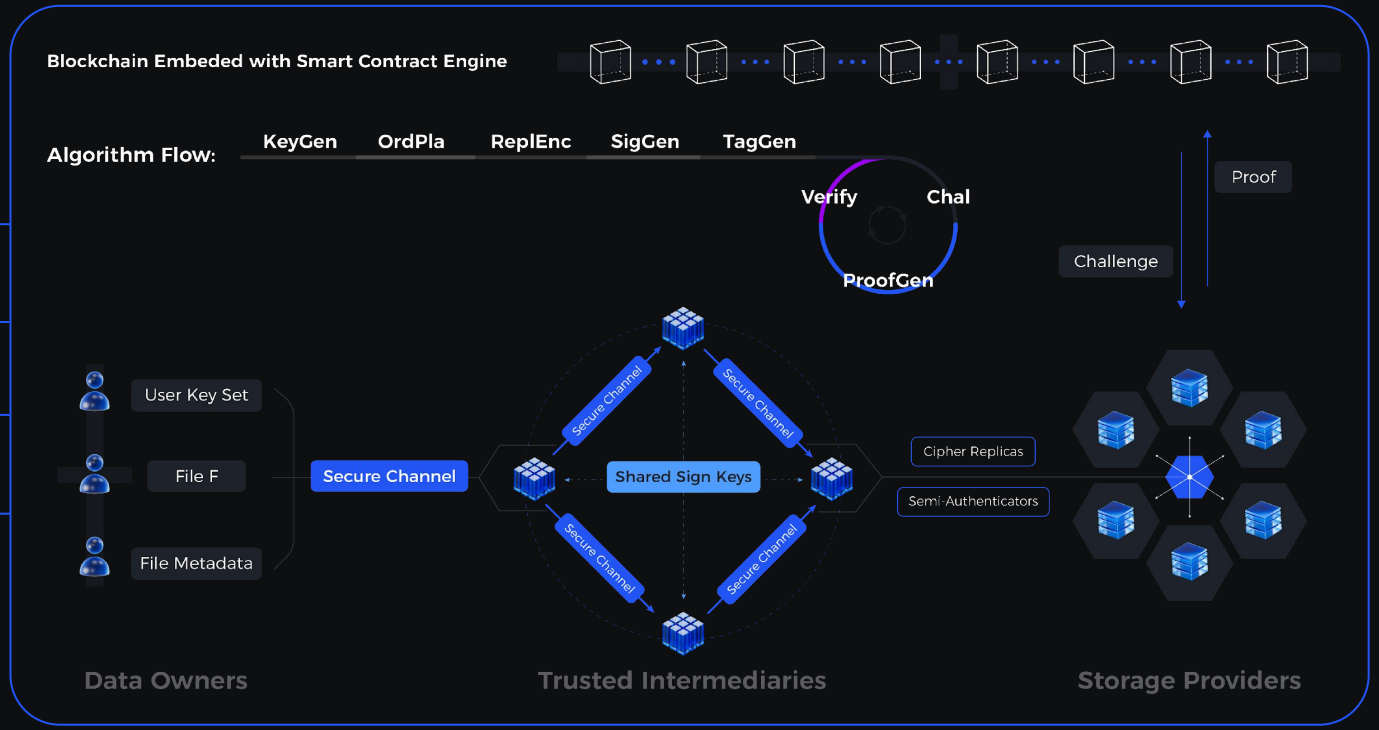
- Publicly verifiable managed continuous proofs.
- Storage proofs based on data copies.
- data integrity rapid recovery mechanism.
- Ultra-compressed aggregated proofs and batch verification.
- Rapid verification and error localization.
- Key revocation and updating.



Challenge 1 - PoDR² Workflow

CESS

- Data Owners (DO)
- Trusted Intermediaries (TI)
- Storage Providers (SP)
- Blockchain Network (BN)



Challenge 1 - Proof of Idle Space (PoIS)

CESS

How to ensure that these files are stored safely and correctly on the hard disk?

PoIS utilizes specific randomly generated data to fill idle storage spaces. By determining the size of this filled data, the true idle space of each node can be ascertained.

The Algorithm of Idle File Generation

- Generate the *layer0* for *file1*, then sequentially generate *layer0* for *file2* ... *file4*.
- Calculate *layer(N)* nodes label, make *layer(N-1)*'s Merkle Hash Tree Root (MHTR) as input.
- Each idle file in the *layerN*, depends on $\sum_{0}^{(N-1)}$(MHTR)

Challenge 2: Ownership Rights

CESS

Lack of Data Origin Verification

- Inability to accurately determine the original creator of the data
- Challenges in establishing authenticity and provenance

Cyber Piracy

- Unauthorized copying and distribution of digital content
- Significant threat to intellectual property rights

Negative Impact On Content Creators

- Loss of revenue and recognition for creators
- Erosion of trust and discouragement from producing original content

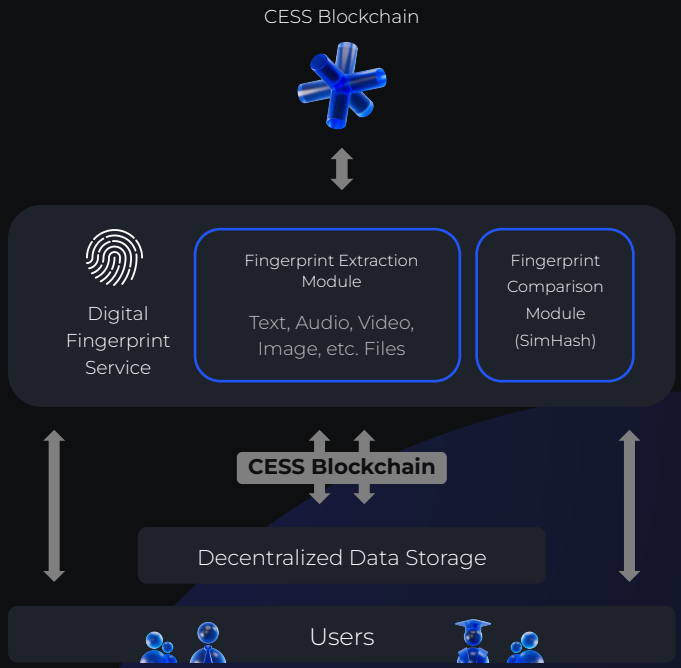
CESS Solution

Multiple Formats Data Rights Confirmation (MDRC)

Challenge 2 - CESS Solution: MDRC

Multiple-Format Data Rights Confirmation Mechanism (MDRC) assigns a unique data certificate ID to each file by extracting a data fingerprint.

- Fingerprints are extracted using advanced word segmentation (Texts). Colors, textures, shapes, space etc. (Photos) etc..
- Performs fingerprints comparison for Data Rights Protection using SimHash.
- Generates Certificate ID to store it on Blockchain for Data Rights Confirmation.



Challenge 3: Inefficient Network

CESS

Low Transactions Per Second

- Limited scalability affecting network performance
- Inability to handle high volumes of transactions efficiently

High Transaction Fees

- Increased costs for users and developers
- Barrier to entry for widespread adoption and everyday use

Lack of Average Nodes Incentives

- Insufficient rewards for nodes leading to low participation
- Difficulty in maintaining a robust and secure network

CESS Solution

Random Rotational Selection Mechanism R^2S

Challenge 3 - CESS Solution: R^2S

CESS

Random Rotational Selection Consensus Mechanism

Open Participation

All nodes have equal opportunities to become candidate consensus nodes

Energy Efficiency

Low computational requirements for consensus nodes.

On-duty Nodes

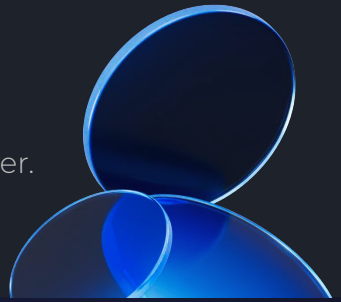
Selection of 11 nodes as on-duty consensus nodes every two weeks - VRF.

Trusted Execution Environment (TEE)

Credible process. Generates file tags, space holder files, and $PoDR^2$ Proof Verification.

Credit Rating

Nodes with poor performance are replaced and credit ratings get lower.



Challenge 4: No Private Data Sharing

CESS

Lack of Support for Private Data

- Inadequate infrastructure for handling sensitive information
- Users unable to control who accesses their data

No Encryption Mechanism

- Data transmitted and stored without encryption
- Increased risk of unauthorized access and data breaches

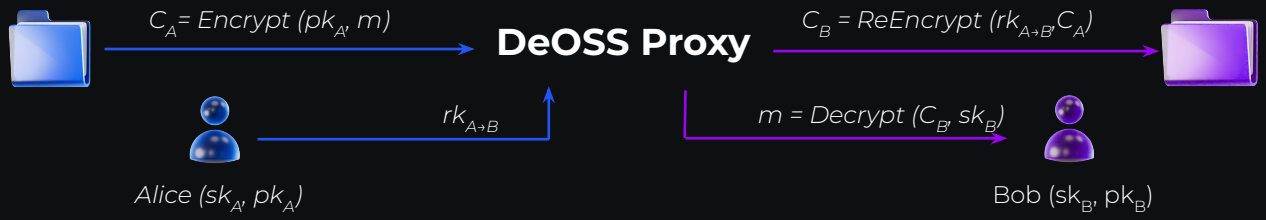
Data Leaks

- Frequent incidents of data exposure
- Loss of trust among users and potential legal implications

CESS Solution

Proxy Re-Encryption

Challenge 4 - CESS Solution: Proxy Re-Encryption



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

$$rk_{A→B} = rekey(sk_A, pk_B)$$

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

$$C_B = ReEncrypt(rk_{A→B}, C_A)$$

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

$$m = Decrypt(C_B, sk_B)$$

Challenge 5: Training AI Models Without Exposing Original Data

CESS

AI Data Privacy Issues

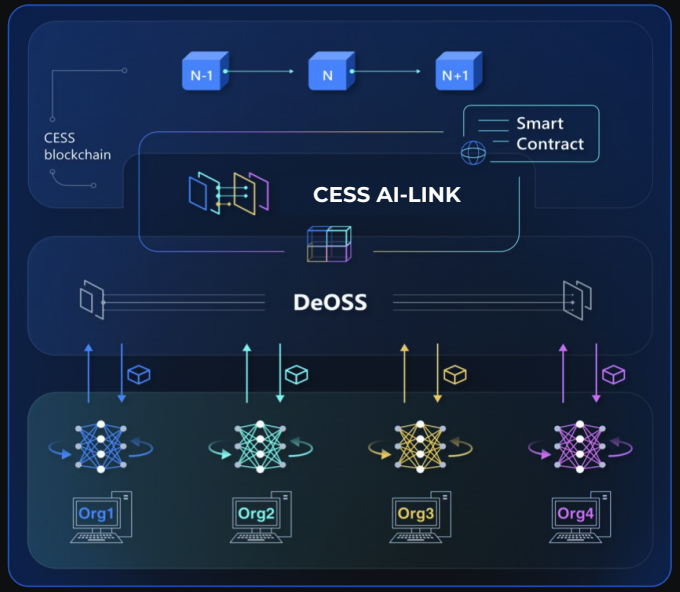
- AI algorithms require large datasets, often containing sensitive information
- Lack of robust privacy measures lead to potential misuse of data and breaches of ethical standards.
- Training Data Without Sharing the Content itself.

CESS Solution

CESS AI-LINK

Challenge 5 - CESS Solution: CESS AI-LINK

A Byzantine-Robust circuit with data privacy.



Train AI models without exposing the original data in a decentralized network.

Key advantages

- Decentralized computing.
- Coordinate training round division by smart contracts.
- Easy integration with other GPU networks
- Can be accelerated by hardware.

Challenge 6: Inefficient use of Storage Space

CESS

No Cloud Pooling Functionality

- Lack of mechanisms for aggregating and efficiently utilizing storage resources
- Individual storage nodes operate in isolation, leading to underutilization

Wastage of Resources

- Unused storage space remains idle and unproductive
- Increased costs and inefficiencies in storage management

CESS Solution

Smart Space Management System

Challenge 6 - CESS Solution: Smart Space Management System

Manages Whole Network Space

- Nodes with unequal storage and computing power
- Space management mechanism to prevent malicious acts

Space Classification

Unverified Space:

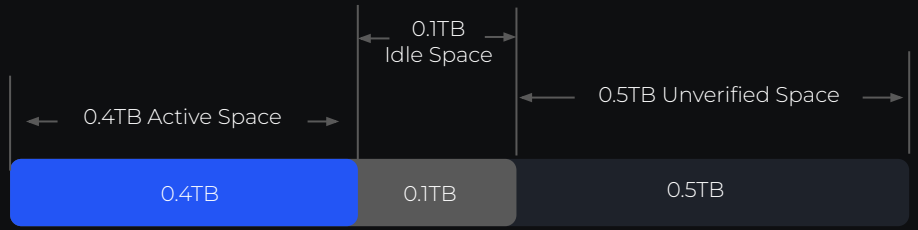
- Reported by storage node
- Specified in configuration
- Larger space staked with more CESS tokens
- No rewards for this space

Idle Space:

- Verified and purchasable space
- Can store data and earn rewards

Active Space:

- Verified space storing user data
- Earns higher rewards for storage nodes



Challenge 6 - Smart Space Management System - Stages

Stage 1: Filling Idle Space

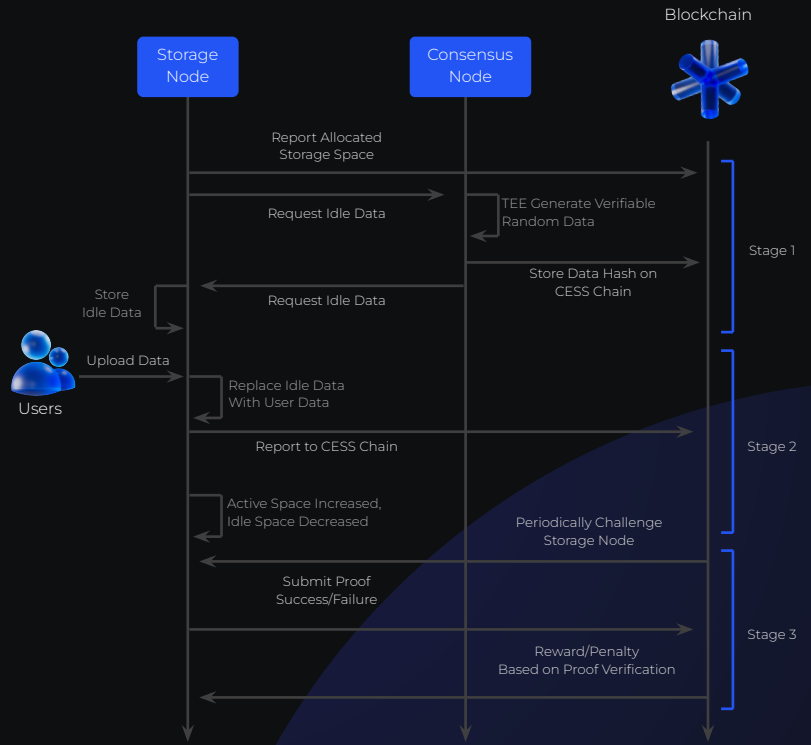
- TEE worker generates verifiable random data for storage node
- Data hash reported to CESS chain
- Idle space added to storage node

Stage 2: Storing User's Data

- User data stored, idle space deleted
- Action reported to CESS chain
- Active space increased, idle space decreased

Stage 3: Challenge and Reward

- Periodic data challenges by CESS chain
- Storage nodes must complete proof of data calculation
- Rewards for successful verification, penalties for failures



Challenge 6 - Smart Space Management System

CESS

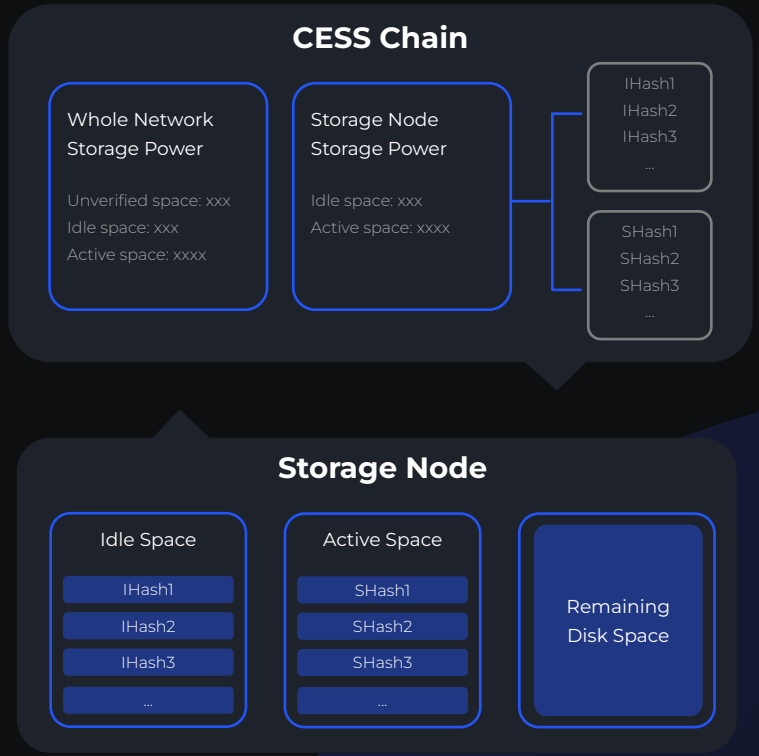
Storage Node Space Management

Regular Checks:

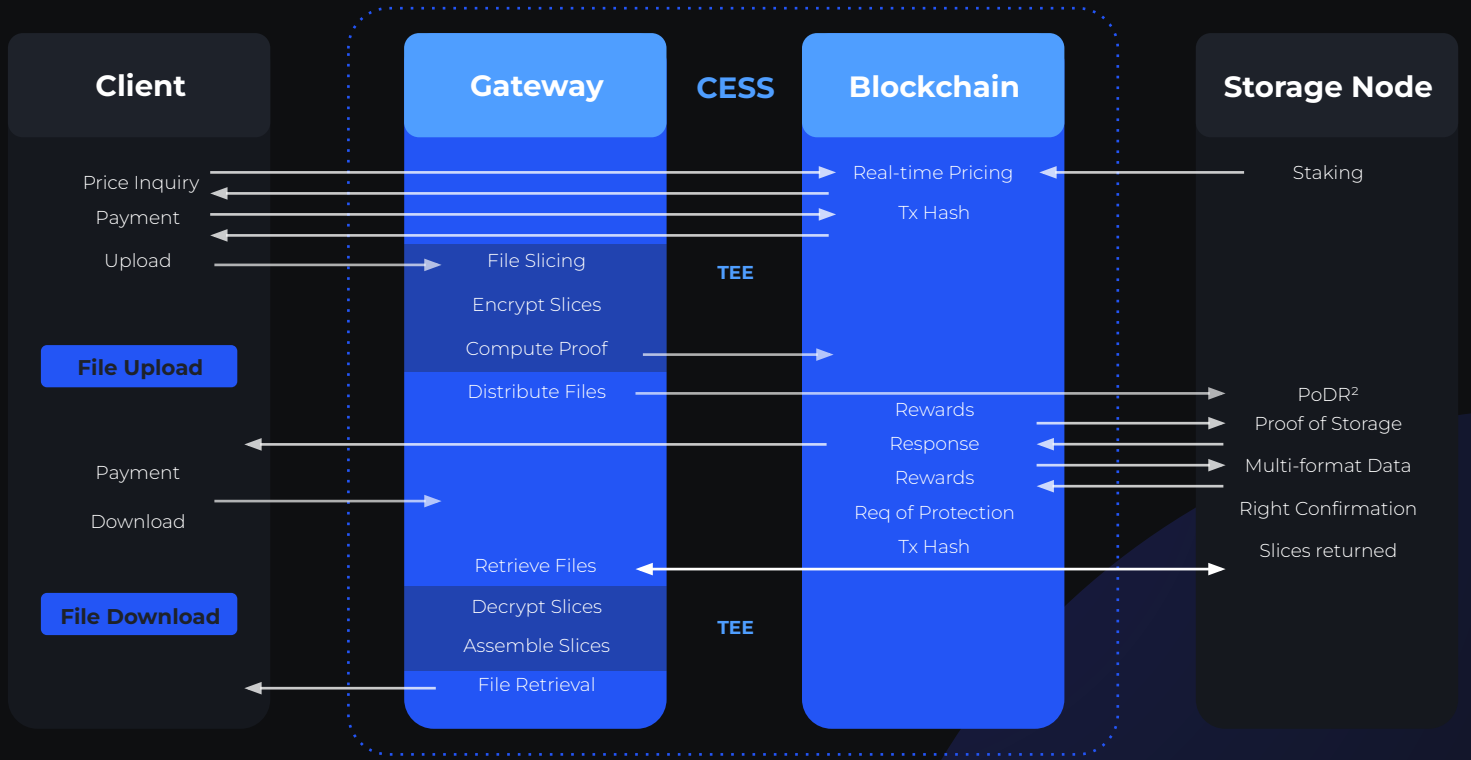
- User data stored, idle space deleted
- Action reported to CESS chain
- Active space increased, idle space decreased

Cleanup:

- Regularly remove invalid data
- Maintain valid data storage
- Command for manual cleanup: bucket tidy



CESS Client Interaction Model



CESS

Thank you for watching

Please Join Our Community

CESS Network - Episode 2

Blockchain Architecture & Key Technologies

https://www.cess.network