On-Chain Model and AIVM Repository

The on-chain model and AIVM repository represent the decentralized storage and management system for AI models and their associated virtual machine configurations on DNA Layer. This repository acts as a global library, enabling users to access and deploy pre-existing AI models and developers to contribute new models and AIVMs.

In this section, we outline how DNA Layer leverages decentralized storage technologies and encryption to maintain a secure, transparent, and persistent repository of AI models and execution environments.

Decentralized Storage Solutions

To facilitate the storage of AIVM kernels — comprising model parameters, configuration files, and inference code—we utilize the InterPlanetary File System (IPFS) and Arweave.

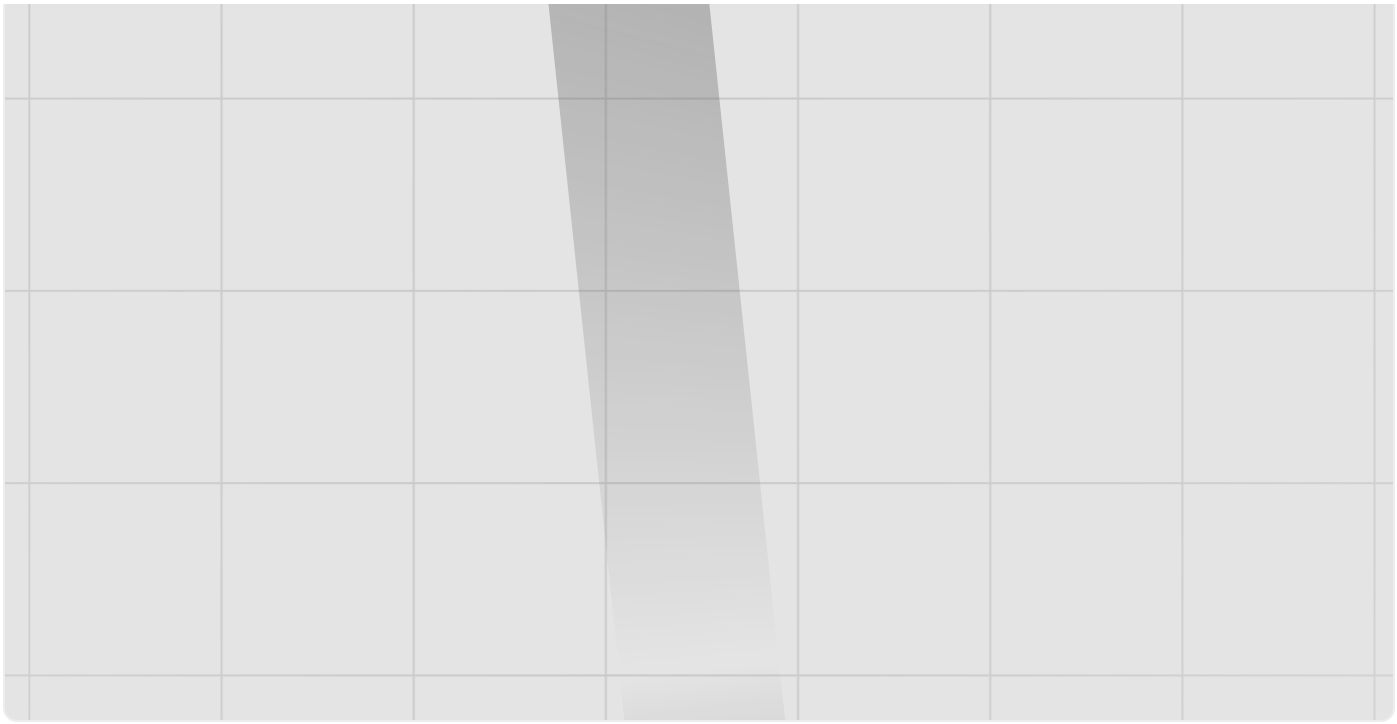
IPFS offers a peer-to-peer network for storing and sharing data in a distributed file system, ensuring that AIVM kernels are accessible across the network without relying on centralized servers. Arweave provides a platform for permanent storage with its blockweave technology, ensuring that once an AIVM kernel is uploaded, it remains available indefinitely.

By combining these decentralized storage solutions, we achieve resilience against data loss and censorship, as well as enhanced accessibility for model deployment.

Integration with the Blockchain

The blockchain maintains a registry of the AIVM kernels, storing metadata such as model descriptions, versioning information, and pointers to the actual data on decentralized storage.

This registry allows for the discovery and verification of models, as DNA Layer's immutability and transparency provide a reliable source of truth for the available kernels.



Privacy for Proprietary Models:

For models that are private or proprietary, encryption is employed before uploading the kernel to the decentralized storage. The model owner is responsible for managing the encryption keys and can distribute them to authorized parties who have the necessary permissions to execute the model. This ensures that private models remain confidential and secure, while still benefiting from the decentralized infrastructure of the platform.

Encryption and Key Distribution

When a private model is uploaded, the model owner uses robust encryption algorithms to secure the data. The corresponding decryption keys are not stored on the blockchain or in the decentralized storage.

Instead, the model owner maintains control over the key distribution, which can be facilitated through secure channels, ensuring that only authorized nodes can execute the private model.

The repository supports updates and version control for AIVM kernels. When a model is updated, the new version is uploaded to decentralized storage, and the blockchain registry is updated to point to the latest version.

This versioning system allows users to access both historical and current versions of models, fostering model evolution while preserving the lineage of development.

Verification and Quality Assurance: Before a model is added to the on-chain repository, it undergoes a verification process to ensure compatibility with the AIVM execution standards. This process includes checks for correctness, consistency, and compliance with the platform's security protocols.

By enforcing a rigorous verification process, we maintain high-quality standards for the models available in the repository.

Through the on-chain model and AIVM repository, we provide a stable and scalable infrastructure for the storage and deployment of AI models.

This infrastructure results in persistent model security, consistency, and accessibility to all users and contributors, whether they are engaging with public models or managing proprietary ones.

Previous
Model Consistency and Inference Reliability

Next
AIVM Interface for Model Interaction

Last updated 1 month ago