Zero-Knowledge Proof (ZKP)

Finally, Zero-Knowledge Proofs (ZKP) is a foundational core cryptographic technique employed in DNA Layer's AIVM, complimenting the above security implementations. ZKP enables one party, the prover, to demonstrate to another party, the verifier, that a certain statement is true without revealing any information beyond the validity of the statement itself.

There are some notable examples of ZKP adopted in blockchain applications. Zcash, for instance, utilizes ZKP to enable private transactions on a public blockchain. By using zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge), Zcash allows users to conceal transaction details such as the sender, receiver, and amount, while still verifying the transaction's legitimacy.

Ethereum is also exploring the implementation of ZKPs to enhance scalability and privacy on the platform. Other projects like zkSync and Hermez use ZKP to batch transactions off-chain and then settle them on-chain, providing scalability solutions without compromising on security.

On DNA Layer, ZKP plays a pivotal role in several key areas:

- **Interfacing with Smart Contracts:** Drawing inspiration from projects like Chainlink but applying it to small and large-scale AI inference requests, we leverage ZKP to build secure protocols that enable the feeding of off-chain data into on-chain smart contracts. This mechanism ensures that smart contracts can access the necessary data for AI model execution while maintaining the confidentiality of the off-chain data sources.
- **Privacy-Preserving Computation:** We implement ZKP to perform computations on private models and data without revealing any underlying sensitive information. This approach is crucial for preserving the privacy of user data and proprietary AI models throughout the inference process. By employing ZKP, we can provide cryptographic assurance that the computation was executed correctly, without exposing the data to external parties.

The integration of ZKP in our system architecture enables private on-chain interactions and confidential computing while providing an easy and accessible channel where users and

enterprises can confidently engage with blockchain technology. This alignment of transparency with confidentiality paves the way for broader adoption and trust in DNA Layer's decentralized system as it evangelizes AI on-chain around the world.

Split-Flow harmonizes the sometimes simultaneous need for these privacy technologies above through its automated evaluation system that analyzes factors such as input sensitivity, workload, model specifics, and consensus criteria to ascertain whether hardware-based secure enclaves, cryptographic techniques, or a combination of the composites should primarily handle data processing.

The adaptability of the Split-Flow protocol allocates processes between a confidentiality-preserving stream and a verifiability-focused one, with security measures tailored to match the dynamic demands of varying data models and inference goals, as well as the model's size and computational intensity, creating a balanced and secure operational state across these heavy security technologies.

Previous
Verifiable Random Function (VRF)

Next
Definitions