Research Answers

**Section 2: Technical Deep Dive**

**Underlying Cryptographic Primitives**

Miden leverages the following cryptographic primitives to achieve its goals:

* **STARKs (Scalable Transparent ARguments of Knowledge):** STARKs are a type of ZK proof system that allows for efficient verification of complex computations. They are highly scalable and secure, making them ideal for use in blockchain scaling solutions.
* **FRI (Fast Reed-Solomon IOPP):** FRI is a cryptographic protocol used to reduce the size of ZK proofs. It is a key component of the STARK proof system.

**Scalability and Security**

Miden achieves scalability and security through the following mechanisms:

* **ZK Proofs:** By using ZK proofs, Miden can verify the correctness of computations without revealing the underlying data. This allows for efficient processing of a large number of transactions.
* **Distributed Network:** Miden's distributed network of verifiers ensures that the network is resilient to attacks.
* **Security Audits:** Miden undergoes rigorous security audits to identify and address potential vulnerabilities.

**Miden VM and Smart Contracts**

The Miden VM is a virtual machine designed to execute smart contracts in a ZK-friendly manner. It is optimized for efficient computation and proof generation. The Miden VM supports a variety of programming languages and can be used to build a wide range of decentralized applications.