Question 1

Polygon Miden Research

Section 1: Core Concepts

Architecture and Key Features

Polygon Miden is a Layer 2 scaling solution using STARK-based ZK-rollups for secure, scalable, and private Ethereum transactions. Unlike zkSync and StarkNet, which use zk-SNARKs, Miden's STARKs avoid the need for a trusted setup, enhancing transparency. By anchoring proofs on Ethereum, Miden leverages Ethereum's security.

Differences and Comparison

- **Privacy**: Miden's STARK-based verification offers privacy without a trusted setup, unlike zk-SNARKs.
- **Compatibility**: Miden VM supports Ethereum-compatible smart contracts.
- **Advantages**: High transparency, scalability, and quantum resistance.
- **Disadvantages**: Computationally intensive proof generation.

Section 2: Technical Deep Dive

Cryptographic Primitives: STARKs and FRI

STARKs ensure transparency and quantum resistance, while FRI reduces on-chain data requirements, improving efficiency.

Scalability, Security, and Privacy

Off-chain computation and only posting proofs on-chain allow Miden to scale while maintaining Ethereum's security and user privacy.

Role of the Miden VM

The Miden VM executes Ethereum-compatible smart contracts efficiently, supporting general-purpose applications.

Section 3: Future Potential and Challenges

Future Applications and Use Cases

Miden could enable scalable and private DeFi, gaming, and identity management solutions on Ethereum.

Challenges

- Computational load for proof generation.
- Establishing broader interoperability standards with other blockchains.

Contribution to the ZK Ecosystem

Miden could bolster the ZK ecosystem by advancing interoperability and contributing to Ethereum's scalability framework.