**ZK Researcher + Engineer Role:**

**Question 1: Polygon Miden Research**

**● Section 1: Core Concepts**

Core Concepts of Polygon Miden are as follows:

* **Polygon Miden Architecture**:

Polygon Miden is a Layer 2 ZK-rollup built on top of Ethereum, designed to improve scalability and security through zero-knowledge proofs. Now, layers in blockchain is similar to stacking parts up to make things work faster and better.

**Layer 0:** Consists of the base layer where all hardware infrastructure and internet protocols lie such as the TCP/IP that helps communication between systems. It also has interoperability networks for interaction between systems.

**Layer 1:** This layer has the main block chain itself, like Ethereum, Bitcoin, Solana, etc. Here is where all the transactions happen. However, this processing can be delayed when many users simultaneously join, so we need another layer on top that can tackle this.

**Layer 2:** So, now on layer 2, we have this technology called Polygon Miden, which takes care of the transaction processing much faster and more efficiently. It offloads the crowd from layer 1 and does bundling or Roll-ups to speed things up. Now, without actually proving layer 1, it gives some valid proof and makes it believe that all transactions have been processed properly and correctly, which is the concept of “**Zero Knowledge Proofs**.”

It also has a **Miden VM(Virtual Machine)** at the center which allows the transactions to happen off-chain and later be bundled and sent to the main chain. It provides an isolated environment for these processes.

* **Consensus Mechanism**:

A **consensus mechanism** is like an agreement process. It’s a way for all the computers/nodes in a network to agree on the correct information, like who owns what or what transactions happened. When everyone agrees, they write it down, and it becomes part of the official record.

Miden leverages ZK proofs, particularly STARKs (Scalable Transparent Argument of Knowledge), for verification. This mechanism avoids traditional consensus algorithms, like proof of work or proof of stake, and instead focuses on cryptographic proofs for trustless and secure verification.

* **Key Features**:
  + **Privacy**: Leveraging STARKs, Polygon Miden supports private transactions and computations.
  + **Scalability**: Miden offloads computation to Layer 2, reducing the load on the Ethereum mainnet and improving throughput.
  + **Decentralization and Transparency**: Using STARKs ensures Miden doesn’t rely on trusted setups, contributing to a more transparent and decentralized ecosystem.