**ZK Researcher + Engineer Role:**

**Question 1: Polygon Miden Research**

**● Section 2: Technical Deep Dive**

**Describe the underlying cryptographic primitives used in Miden, such as STARKs and FRI.**

**STARKs (Scalable Transparent Argument of Knowledge)**

* STARKs are a type of **zero-knowledge proof** that allows a prover to convince a verifier that a computation is correct without revealing the computation’s actual inputs. STARKs are especially useful for proving large computations in a way that is secure and scalable, meaning they can handle high transaction volumes and complex logic efficiently.

**How it works**:

* STARKs transform computational problems into mathematical ones. They break down the computation into polynomials and prove that these polynomials satisfy certain properties.
* Unlike some other zero-knowledge proofs, STARKs use randomness from the verifier without requiring a “trusted setup,” a special process that generates secret parameters for security. This makes STARKs **transparent**, so they don’t rely on any third-party trust assumptions.
* STARKs are designed to work on large data sets. As the size of the computation grows, the size of the proof grows more slowly, making them scalable for systems handling a high number of transactions.
* STARKs are well-suited to applications that require both privacy and highsecurity. Their transparency and scalability make them an ideal choice for Polygon Miden, where privacy and efficiency are top priorities.

**FRI (Fast Reed-Solomon Interactive Oracle Proofs of Proximity)**

* FRI is a **proof-of-proximity** protocol used within STARKs to verify that a function (like the polynomial in STARKs) is close to what it’s supposed to be, meaning it checks if the data aligns closely with the properties we expect. FRI is specifically designed to make STARKs faster and more efficient by improving the process of verifying polynomials.

**How it works**:

* FRI uses **Reed-Solomon codes**, a type of error-correcting code that helps in verifying the properties of polynomials without needing to check every point. This makes the process faster and more efficient.
* Instead of checking the entire polynomial, FRI randomly samples parts of it, significantly speeding up verification. This randomness ensures that even with a few samples, we can be highly confident in the polynomial’s correctness without evaluating each detail.
* **Reducing Proof Size**: FRI helps keep the proof size relatively small, reducing the data that needs to be transmitted and stored on-chain.
* FRI makes the STARK-based proofs in Miden more efficientand practical by reducing the time and computational resources required to verify proofs. It keeps the proof sizes manageable, which is crucial for maintaining low fees and quick verification times.

**How does Miden achieve scalability and security while maintaining privacy?**

Polygon Miden achieves scalability, security, and privacy by combining ZK-rollup architecture with STARK-based cryptography and a custom virtual machine (VM), Miden VM.

* **Scalability**: Miden processes transactions off-chain by “rolling up” batches of transactions, creating a single proof for each batch instead of individual transactions. This setup reduces on-chain storage and gas fees (a small fee that you pay for processing the transactions on the chain), enabling higher transaction volumes. Using STARKhelps keep proof sizes small and verification fast, while FRI speeds up the proof verification process by sampling only parts of the computation.
* **Security**: Miden uses **transparent STARKs**, which don’t require a trusted setup phase, enhancing security by eliminating reliance on third-party initializations. This transparency makes Miden’s security depend solely on mathematics, which can be trusted and verified by anyone.
* **Privacy**: Zero-knowledge proofs let Miden verify that transactions are correct without revealing sensitive details like amounts or participants. The Miden VM (Virtual Machine) enables complex applications that can maintain this privacy by hiding transaction details. This makes Miden suitable for private applications like finance or identity management.

**What is the role of the Miden VM in executing smart contracts?**

Smart contracts:

Smart contracts are self-executing programs on a blockchain that automatically carry out actions when certain conditions are met. They work like a traditional contract but without the need for middlemen or enforcement agencies. Once it is created, it will run based on the flow and no one can alter it while running.

**Supports Complex Computations**:

* Miden VM is built to handle more advanced and complex operations, allowing developers to create detailed and powerful applications. This flexibility is ideal for applications that require heavy computations, like private financial transactions, gaming, or complex algorithms.

**Privacy and Efficiency with Zero-Knowledge Proofs**:

* It uses **zero-knowledge (ZK) technology** to keep transaction details private while still proving to the network that the smart contract’s rules were followed correctly. This ensures both privacy and security for users, as only the necessary information is revealed.

**Optimized for Off-Chain Execution**:

* Miden VM runs computations off the main Ethereum chain, then submits a **proof** (using STARKs) to verify that everything was executed correctly. This setup reduces the load on Ethereum and keeps gas fees low.