**ZK Researcher + Engineer Role:**

**Question 1: Polygon Miden Research**

**● Section 1: Core Concepts**

**How does Miden differ from other ZK-rollup solutions like zkSync and StarkNet?**

Polygon Miden, zkSync, and StarkNet are all Layer 2 ZK-rollup solutions. They bundle multiple off-chain transactions into a single proof to post on Ethereum, increasing speed and lowering costs. But they differ in their underlying technologies used, design goals and how they work:

(i) Differences based on ZK proof methods used:

* **Polygon Miden** uses **STARKs (Scalable Transparent Argument of Knowledge)** for ZK proofs. STARKs are transparent, as they don’t need a secure initial setup phase. This transparency makes them more secure and auditable since they’re free of third-party trust requirements.
* zkSync uses SNARK (Succinct Non-interactive Argument of Knowledge) for ZK proofs but require an initial setup phase which may pose some security issues. StarkNet also uses STARK but it differs in the way of working and applications areas where its used.

(ii) Difference based on the VM used:

* Polygon Miden uses Miden VM specifically made for the ZK-proof methodology. But its not directly compatible with the underlying layer 1, Ethereum Virtual Machine (EVM). It is flexible and suitable for complex computations.
* zkSync is compatible with EVM and hence helps easy migration of Ethereum dApps to layer 2.
* **StarkNet** runs on the **Cairo VM**, which is built for STARK and designed to maximize the efficiency of proof generation. Like Miden, Cairo is not EVM-compatible, so developers write contracts using Cairo’s custom language.

(iii) Privacy and Focus on User Experience:

* **Polygon Miden** focuses heavily on **privacy** by using STARKs, it allows private transactions and computations by default.
* **zkSync** is designed with scalability and simplicity in mind but focuses a bit less on privacy, as it prioritizes easy migration and minimal costs.
* **StarkNet** is geared toward scalable applications that require high throughput, such as gaming and DeFi, but it also enables privacy via its STARK proofs.

**What are the potential advantages and disadvantages of Miden compared to other solutions?**

Advantages of Polygon Miden:

* Miden provides strong privacy features as it uses STARK which helps in easy transacation processing without revealing the details of the transactions. This is used where security and confidentiality is very important.
* STARK doesn’t require a secure initial setup phase which makes them transparent. So it does not rely on any third party applications and hence is very secure.
* It is highly flexible as it is a general purpose computation platform which allows the development of any type of application such as finance, game apps etc. It can be used for complex transaction operations and is highly customizable.
* Finally, Miden is highly scalable as it can handle and verify numerous transactions at once without congestion.

Disadvantages of Polygon Miden:

* Miden lacks compatibility with EVM and hence requires extra effort for dApps that wish to migrate to L2. This causes potential delay and is difficult for developers.
* Miden is quite computationally expensive as it generally has a large proof size and focuses more on privacy. But sometimes for small-scale applications people may prefer to choose zkSync as it is compatible with EVM and also less expensive computationally.
* Miden is relatively new in the market so it has a less mature tooling and ecosystem. Since the developer community and available resources are less, it is difficult for the developers to start working with it right away.

Thus Polygon Miden has a lots of advantages but relatively a few disadvantages as it’s a new and upcoming technology but this can be overcome in the coming years.