zku.one Assignment 7

Question 1.

> **Question 1**: [**Both streams**] Celestia is set out to be the consensus and data availability layer for blockchains. Chains built on top of Celestia can concentrate on execution. Do you think data availability is the true bottleneck to scale blockchain? Argue for and against the need for the data availability layer for blockchain.

I argue for the availability layer for blockchain. Why? increasing block size, sharding and rollups would mark the endless growth of blockchain's size. Let us see the case of Solana. It has taken a distinctive path for scaling, which is of a monolithic blockchain. It has its plan on building more validating nodes indefinitely to operate the network as they require more increasing computing power. However, this approach is not feasible and would end up centralization as the node validators are forced to purchase cutting-edge hardware to constantly keep up with the performance requirements. This implies the fact that storing transaction data and validating them in a single node is not feasible.
It is better to have another layer to handle the data availability issue. A modular blockchain is a good approach for tackling this issue to scale up to millions of TPS. As rollups and data shards become the feasible idea for scaling blockchain performance, the data availability issue should be tackled by an independent but separable layer. From this angle, I love the case of Celestia since it has its ambitions to build transaction storage for Rollups. In addition, Celestia eliminates the bootstrapping efforts to build validators which is burdensome for the starting project. Celestia does the work instead of projects. This approach is similar to Layer 0 chains like Cosmos. The main blockchain called Layer 0 works as a communication and data availability layer, it serves the same benefits to Celestia. I believe that Celestia might need to focus on EVM blockchains as the project on the EVM ecosystem builds their scalability solutions based on Rollups and shardings.

Question 2.

> **Question 2**: [**Both streams**] Another popular zero knowledge technology in the market today is zk-STARKs. Starkware uses this technology to power dApps such as DiversiFi, ImmutableX, dYdX, etc.. List some advantages of zk-Starks over zk-Snarks. In your opinion, which one is better and why?

- When it comes to the advantages of zk-STARKs, it does not require a trusted setup phase as it uses publicly verified random entropies to create verifiable computational systems. It is also claimed that zk-STARKs are quantum-computing resistant as zk-STARKs are blamed for their vulnerability to quantum computing.
- However, the proof size of zk-STARKs is over 10x bigger than zk-SNARKs, which makes it difficult to upload the proof and execute the operation on-chain. Thus, to utilize zero-knowledge technology in a more decentralized fashion including a mobile environment, Celo's Plonk selects zk-SNARKs technology.
- Last but not least, although the fact that zk-STARKs are more advanced at technical levels, it seems that zk-SNARKs are more advanced and practical today in building real-world applications like bridges and light clients.
- Thus, as I am a high-level application developer, there is no option but to choose zk-SNARKs for hands-on building own application experience.

Question 3.

> **Question 3**: [**Both streams**] Write in brief (1- 2 line for each) about the polygon's product stack. Refer this Polygons ZK Product Overview

1. Polygon PoS: A layer-1 compatible EVM sidechain that saves gas costs, without shared security. It was the first product and took full advantage since May 2021.
2. Polygon Hermez: zk-based rollup that does not support zk EVM while focusing on decentralization. It is now available to use since March 2021. It can process up to 2000 transactions per second.
3. Polygon Zero: It began as Mir protocol powered by recursive ZK proofs. Unlike Polygon Hermez, it devotes to speed rather than focusing on decentralization. The protocol uses Plonky 2, which is a recursive ZK proof generator capable of generating a SNARK proof every 0.17 seconds, making Plonky 2 the world's fastest recursive ZK prover.
4. Polygon Miden: MidenVM utilizes a proof called zk-STARKs that stands for the scalable transparent argument of knowledge. zk-STARKs do not require an initial setup process between the prover and validator. In addition, the advantage lies in the creation of MidenVM, a zk-STARK compatible with EVM. MidenVM is a general-purpose ZK Virtual Machine, which lets developers utilize the full Turing completeness capability of the platform. The languages like Solidity, Move, and Vyper is compiled into Miden Assembly Languages to be ready by the VM. The current iteration of MidenVM, a public v0.1 prototype, combines features from both Distaff VM and Winterfell and was launched in November 2021. A v0.2 prototype is anticipated to be released in Q2 2022, and the mainnet deployment is expected to occur sometime in 2023.
5. Polygon Nightfall: Nightfall is an Optimistic rollup enhanced by the privacy benefits of ZK cryptography. The type of ZK cryptography used in Nightfall differs slightly from generic ZK Rollups; it pairs the ZK cryptography with a fraud-proof rollup originated from the need to service enterprises with a differentiated product. It kept the privacy elements of ZK cryptography while maintaining low transaction costs. Thus, the corporate-focused tools benefit the most from privacy features. It also legally supports KYC-compliant features that serve as a whitelist of companies that can access the network. EY has collaborated with Polygon to render the Polygon Nightfall protocol. It is now in production.
6. Polygon Avail: It is a data availability-specific blockchain like Celestia, which is designed for standalone blockchains. It works for all blockchains all across the Ethereum ecosystem and is purposed to store Ethereum calldata tracking changes to the Ethereum state machine. The entire purpose of Avail's existence is to sequence and store data to ensure data remains accessible by a sampling process conducted by light client nodes. Light nodes prioritize sampling a random group of data from each block to evaluate for completeness, which is a process called a data availability check. The process can be completed at a constant resource cost. It is now at the development level.
7. Polygon Edge: Edge is an open-source modular blockchain development framework built for engineers who want to create their blockchains. The framework allows for the creation of both secured Layer 2 chains and standalone Ethereum sidechains. The rollout of Edge for the standalone chain framework began in May 2021, and the second iteration of the framework for secured chains is expected to follow shortly.

Question 4.

> **Question 4:** Write in brief (at least 4 -5 lines) about your learnings throughout the course.

I believe that zero-knowledge proof would be the future in terms of the following: 1) All layer 1 is inevitable to have a zk-Rollup arsenal while having security/consensus solution like utilizing light clients or independent data availability chains. 2) Multi-chain environment is now looming so bridging each other trustlessly is important, which means that zero-knowledge technology would be actively used for that. I believe that creating bridges and connecting among other chains could be the product-as-a-service so that any L1/L2 chain creators can easily adapt it by utilizing BaaS (Blockchain-as-a-service) product. 3) Lastly but not least, a product utilizing zero-knowledge technology would be the next mass adoption for the Web3 scene. Considering the importance of privacy and people's concentration on the issue, I strongly affirm that those product lines would be valuable in the future as the high-level implementation of zero-knowledge proof advances more. I would like to serve as TA and contribute to the Harmony Protocol's effort to educate for zero-knowledge proof since helping more Web2 developers to onboard the Web3 scene is the key to attracting more consumers. As more feasible products are released, more consumers to massively adopt crypto and Web3 into their lives. Let our parents use Web3 and crypto products without the need to appreciate any sophisticated concepts of Web3 and crypto stuff.

Question 5.

> [**Stream A**] Provide 2 - 3 ideas for your final project. Explain the pros and cons of each idea. Also, provide a draft proposal for the idea of your liking. Refer here for samples.

- Please refer to the following link. GitHub Link