ZKU - Assignment 7

```
Email - stanleychiu@protonmail.com
Discord - HKerStanley#4125
GitHub - https://github.com/HKerStanley/zk-uni (./asset/week_7)
```

Question 1

Yes I think data availability is the true bottleneck. Recalling the blockchain trilemma: Decentralization, Scalability and Security, I think each of them touching a different aspect of data availability. Decentralization is about how open is the network to public to access, store, process and provide data. Scalability is about how much effort needed to distribute the data. Security is about how much trust we can put to data provider. I think the need of data availability layer exist as it can still help a blockchain to scale up by taking data off-chain. But this is not solving the trilemma as the degree of decentralization will be comprimised if settlement and consensus solely rely on data provided by the protocol.

Question 2

zk-STARK does not require a trusted setup and it is post-quantum secure. At the current stage I would prefer zk-SNARK because it has a much smaller proof size and shorter verification time. As we already seen solution on the market to solve the requirement on trusted setup of zk-SNARK, and we are not getting into the quantum computing era soon. ZK-SNARK has a larger community and better support which makes it more mature for production and friendly to new learner. Smaller proof size and faster verification time are also big plus to make zk-SNARK as scaling solution.

Question 3

Polygon Hermez - An open-source decentralized ZK rollup to operate on top of Ethereum's mainnet

Polygon Zero - An ZK rollup utilized recursive ZK proof generation to specifically speed up transactions

Polygon Miden - A general-purpose zero knowledge virtual machine with zk-STARK which provide full Turing complete capability to developers

Polygon Nightfall - An Optimistic rollup enhanced by zero knowledge proof to conduct private transactions while maintaining low transaction costs

Polygon Avail - A data availability-specific blockchain to store Ethereum 'calldata' tracking changes to the Ethereum state machine

Polygon Edge - An open-source modular blockchain development framework built for engineers who want to create their own blockchains

Question 4

I think this course is comprehensive about blockchain and zero-knowledge. I learnt about blockchain fundamentals and existing problems like the blockchain trilemma and interoperability trilemma. Also learnt about zero knowledge application and infrastructure from examples like bridges and games. The course also help me learn deeper about some popular products like Tornado Cash which is really inspiring.

Question 5

My final project is a zkAutoChess game and I am approaching the final stage of it before deploying to testnet. I have implemented the game matching logic in smart contract, the circuit to prove player input, the basic frontend to interact with the game. I am now and will keep working on proof generation that will be committed on-chain, the reveal and verify logic of players move, and the battle result evaluation logic.