**Week 8 Seminar Solutions**

1. What are the disadvantages of DEXs.

As revolutionary as they are, decentralized exchanges have their fair share of drawbacks. It is important to weigh these cons before making a decision on which exchange to use.

* Transaction Speed

The processing of orders on DEXs can be slow. This is because trading calls have to first be broadcasted to the network and confirmed by miners before they are processed. This is why trades on DEXs are more likely to suffer from “price slippage,” where the transaction doesn’t execute due to changes in the values of the cryptocurrencies being swapped.

“Front-running” is also a concern with public order-books. In this scenario, users initiate trades with higher gas fees to have them executed earlier than those that are still pending.

* Liquidity Issues

Liquidity is achieved by centralized exchanges through enormous capital. DEXs often have a problem on this end because, unlike centralized exchanges, their liquidity heavily relies on the number of users actively trading on the platform. They also often do not have access to any fund which they can move around to facilitate trades.

Fortunately, the decentralized finance (DeFi) space has come up with a solution to this through liquidity pools that DEXs can tap.

2. What are the benefits of an AMM?

The major benefits of an AMM are constant availability and that a traditional counterparty is not necessary to execute a trade. These provisions are very important for smart contracts and DeFi development because of the guarantee that a user can exchange assets at any moment if necessary. A user maintains custody of her funds until she completes the trade, hence, counterparty risk is zero. An additional benefit is composable liquidity, which means any exchange contract can plug into the liquidity and exchange rates of any other exchange contract. AMMs make this particularly easy because of their guaranteed availability and their allowing one-sided trading against the contract. Composable liquidity correlates comfortably with the concept of DeFi Legos.

One drawback to an AMM is the concept of impermanent loss, the opportunity-cost dynamic between offering assets for exchange and holding the underlying assets to potentially profit from the price movement. The loss is impermanent because it can be recovered if the price reverts to its original level. To illustrate, consider two assets, A and B, each initially worth 1 ETH. The AMM contract holds identical quantities of 100 of each asset and naively offers both at a fixed exchange rate of 1:1. We use ETH as the unit of account to track the contract’s return on its holdings and any impermanent loss. At the given balances and market exchange rates, the contract has 200 ETH in escrow. Suppose asset B’s price appreciates to 4 ETH in the wider market and asset A’s price appreciates to 2 ETH. Arbitrageurs exchange all of asset B in the contract for asset A because asset B is more valuable. The contract then holds 200 of asset A worth 400 ETH. In this case, the contract’s real return is 100%.

If, however, the contract does not sell asset B, the contract’s value would be 600 ETH. The contract has an impermanent loss equal to 200 ETH, the difference between 600 ETH and 400 ETH. If the contract's holdings return to parity between assets A and B, the impermanent loss disappears. If the goal for liquidity held in the contract is profit, any fees charged must exceed the amount of the impermanent loss.

Impermanent loss occurs for any shift in price and liquidity, because the contract is structured to sell the appreciating asset and to buy the depreciating asset. An important feature of impermanent loss is path independence. In our example, it is irrelevant whether 1 or 100 traders consumed all the liquidity. The final exchange rate and contract asset ratios yield the same impermanent loss regardless of the number of trades or the direction of the trades. Because of path independence, impermanent loss is minimized on trading pairs that have correlated prices (mean-reverting pairs). Thus, stablecoin trading pairs are particularly attractive for AMMs.

3. Explain how flash loans work on the Ethereum transaction.

A thorough understanding of an Ethereum transaction is important for understanding how flash loans work. One clause in the transaction is vital: if the loan is not repaid with required interest by the end of the transaction, the whole process reverts to the state before any money ever left the lender’s account. In other words, either the user successfully employs the loan for the desired use case and completely repays it in the transaction or the transaction fails and everything resets as if the user had not borrowed any money.

Flash loans essentially have zero counterparty risk or duration risk. They allow a user to take advantage of arbitrage opportunities or refinance loans without pledging collateral. This capability allows anyone in the world to have access to opportunities that typically require very large amounts of capital investment. In time, we will see similar innovations that could not exist in the world of traditional finance.

4. Explain the three types of oracle solutions.

The first is a Schelling-point oracle. This oracle relies on the owners of a fixed-supply token to vote on the outcome of an event or report the price of an asset. Examples of this type of oracle include Augur and UMA. While Schelling-point oracles preserve the decentralization components of protocols that rely on them, they suffer from slow times to resolution.

The second type of oracle solution an API oracle. These oracles are centralized entities that respond asynchronously to requests for data or prices. Examples include Provable, Oraclize, and Chainlink. All systems relying on API-based oracles, must trust the data provider to respond accurately to all queries.

The third type of oracle is a custom, application-specific oracle service. This type of oracle is used by Maker and Compound. Its design differs based on the requirements of the protocol it was developed for. For example, Compound relies on a single data provider that the Compound team controls to provide all on-chain price data to the Compound oracle.

5. How do I make money with DeFi?

The value locked up in Ethereum DeFi projects has been exploding, with many users reportedly making a lot of money.

Using Ethereum-based lending apps, as mentioned above, users can generate “passive income” by loaning out their money and generating interest from the loans. Yield farming, described above, has the potential for even larger returns, but with larger risk. It allows for users to leverage the lending aspect of DeFi to put their crypto assets to work generating the best possible returns. However, these systems tend to be complex and often lack transparency.

6. Is investing in DeFi safe?

No, it’s risky. Many believe DeFi is the future of finance and that investing in the disruptive technology early could lead to massive gains.

But it’s difficult for newcomers to separate the good projects from the bad. And, there has been plenty of bad.

As DeFi has increased in activity and popularity through 2020, many DeFi applications, such as meme coin YAM, have crashed and burned, sending the market capitalization from $60 million to $0 in 35 minutes. Other DeFi projects, including Hotdog and Pizza, faced the same fate, and many investors lost a lot of money.

In addition, DeFi bugs are unfortunately still very common. Smart contracts are powerful, but they can’t be changed once the rules are baked into the protocol, which often makes bugs permanent and thus increasing risk.