Course II:

DeFi Primitives

Campbell R. Harvey
Duke University and NBER

Learning Experience Outline

Four courses in **DeFi and the Future of Finance:**

I. DeFi Infrastructure

II. DeFi Primitives

1. Mechanics
2. Supply and Ownership
3. Loans and Swaps
4. Joining the World of DeFi

III. DeFi Deep Dive

IV. DeFi Risks and Opportunities

II. DeFi Primitives

Modules

1. **Mechanics**
   i. Transaction mechanics
   ii. Fungible tokens
   iii. Non-fungible tokens
2. Supply and Ownership
3. Loans and Swaps
4. Joining the World of DeFi

Course II:

DeFi Primitives

1. The Mechanics of Modern Decentralized Finance

(i) Transaction mechanics

Transaction mechanics

How do transactions work?

- Transactions involve sending data and/or ETH (or other tokens) from one address to another.
- An Ethereum user can control addresses through an *externally owned account* (EOA) or by using smart contract code (*contract account*).
- When sending data to a contract account, the data are used to execute code in that contract. The transaction may or may not have an accompanying ETH payment for use by the contract.
- Transactions sent to an EOA can only transfer ETH.

Transaction mechanics

How do transactions work?

- A single transaction starts with an end-user from an EOA, but can interact with a large number of dApps (or any Ethereum smart contract) before completing.
- The transaction starts by interacting with a single contract, which will enumerate all of the intermediate steps in the transaction required within the contract body.

Transaction mechanics

Atomicity

- Clauses in a smart contract can cause a transaction to fail and thereby revert all previous steps of the transaction; as a result, transactions are *atomic*.
- Atomicity is a critical feature of transactions because funds can move between many contracts (i.e., “exchange hands”) with the knowledge and security that if one of the conditions is not met, the contract terms reset as if the money never left the starting point.

Transaction mechanics

Gas

- Transactions have a gas fee, which varies based on the complexity of the transaction. E.g., low gas fee is used to compensate a miner for including and executing a transaction, and high gas fee for more data-intensive transactions
- If a transaction reverts for any reason, or runs out of gas, the miner forfeits all gas used until that point. Forfeiture protects the miners who, without this provision, could fall prey to large volumes of failed transactions for which they would not receive payment.

Transaction mechanics

Gas fees

- The gas price is determined by the market and effectively creates an auction for inclusion in the next Ethereum block.
- Higher gas fees signal higher demand and therefore generally receive higher priority for inclusion.

Transaction mechanics

Mempool

- Transactions are posted to a *memory pool*, or *mempool*, before they are added to a block.
- Miners monitor these posted transactions, add them to their own mempool, and share the transaction with other miners to be included in the next available block.
- If the gas price offered by the transaction is uncompetitive relative to other transactions in the mempool, the transaction is deferred to a future block.

Transaction mechanics

Miner extractible value

- Any actor can see transactions in the mempool by running or communicating with mining nodes.
- This visibility can even allow for advanced “front-running”. This is not to be confused with the illegal front-running in centralized finance. If a miner sees a transaction in the mempool (and all transactions are public information), she could profit from by either executing herself or front-running it, the miner is incentivized to do so if lucky enough to win the block.

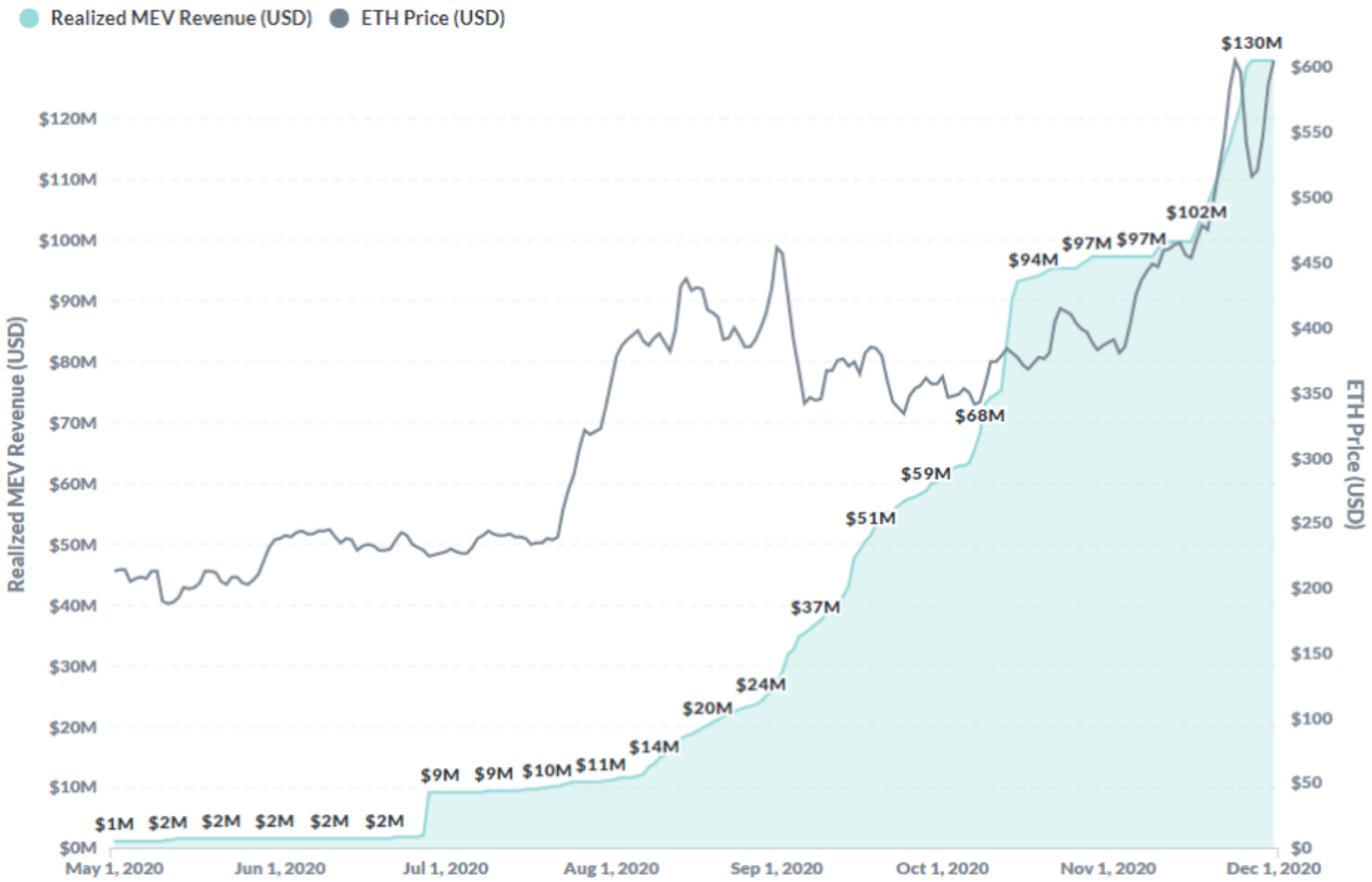
Transaction mechanics

Miner extractible value

- *Miner extractable value* (MEV) is a measure of the profit that the miner could make by including, excluding or re-ordering transactions.
- MEV is a drawback to the proof-of-work model.
- Certain strategies, such as obfuscating transactions, can mitigate MEV, thus hiding from miners how they might profit from the transactions.

https://research.paradigm.xyz/MEV

Transaction mechanics



https://research.paradigm.xyz/MEV