Part 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 <u>*externally owned account*</u> (EOA) or by using smart contract code (<u>*contract account*</u>).
- 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 <u>revert all previous steps</u> 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.

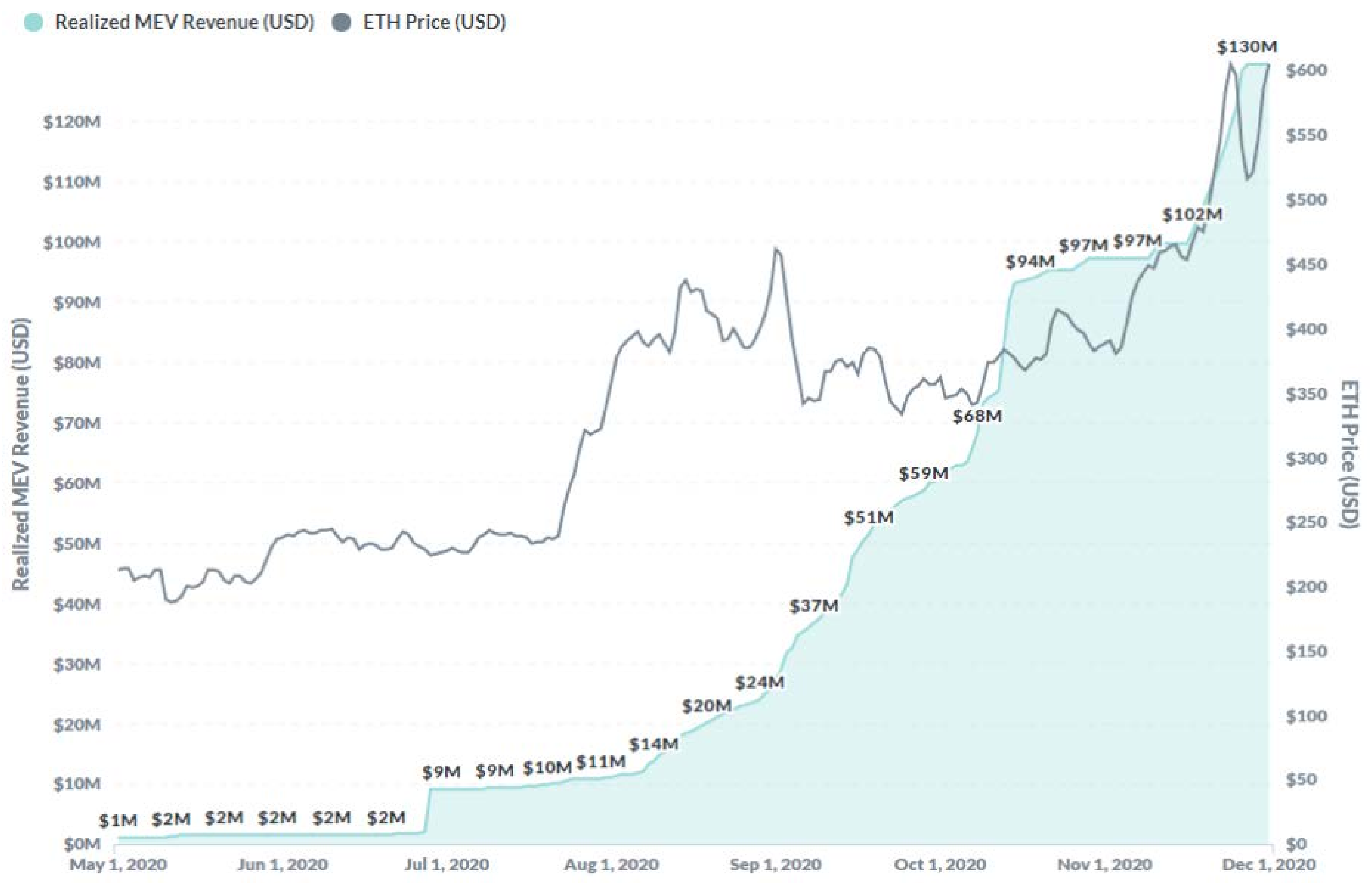
Transaction mechanics

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

Part II:

DeFi Primitives

1. The Mechanics of Modern Decentralized Finance

(ii) Fungible Tokens

Fungible tokens

ERC-20 functionality

- When a token implements the ERC-20 interface, any application that generically handles the defined functionality can instantly and seamlessly integrate with the token.
- Using ERC-20 and similar interfaces, application developers can confidently support tokens that do not yet exist.

Fungible tokens

ERC-20 interface

- **totalSupply()**—read the token’s total supply;
- **balanceOf(address)**—read the balance of the token for a particular user;
- **transferFrom(from address, to address, amount)—**send “amount” tokens from the balance of tokens held at “from address” to “to address”; and
- **approve(owner, spender, amount)—**allows “spender” to spend “amount” tokens of “owner” on behalf of owner.

Fungible tokens

Equity tokens

- An equity token (not traditional stocks) is simply a token that represents ownership of an underlying asset or pool of assets.
- The units must be fungible so that each corresponds to an identical share in the pool. For example, suppose a token, TKN, has a total <u>fixed supply of 10,000</u>, and TKN corresponds to an ETH pool of 100 ETH held in a smart contract.
- The smart contract stipulates that for every unit of TKN it receives, it will return a pro rata amount of ETH, fixing the exchange ratio at 100 TKN/1 ETH.

Fungible tokens

Equity tokens

- We can extend the example so the pool has a variable amount of ETH. Suppose the ETH in the pool increases at 5% per year by some other mechanism.
- Now 100 TKN would represent 1 ETH plus a 5% perpetual cash flow of ETH. The market can use this information to accurately price the value of TKN.

Fungible tokens

Equity tokens

- In actual equity tokens, the pools of assets can contain much more complex mechanics.
  - Variable interest-rate mechanics (Compound)
  - Contract that owns a multi-asset pool with a complex fee structure (Uniswap).
  - A standard interface for creating equity tokens with static or dynamic holdings (Set Protocol).

Fungible tokens

Utility tokens

- Utility tokens are fungible tokens that are required to utilize some functionality of a smart contract system or that have an intrinsic value proposition defined by its respective smart contract system.
- Examples of use cases for utility tokens:
    - To be collateral (e.g., SNX)
    - To represent reputation or stake (e.g., REP, LINK)
    - To maintain stable value relative to underlying or peg (e.g., DAI, Synthetix Synth)
    - To pay application-specific fees (e.g., ZRX, DAI, LINK)

Fungible tokens

Utility tokens

- The last example includes all stablecoins, regardless of whether the stablecoin is fiat collateralized, crypto-collateralized, or algorithmic.
- In the case of USDC, a fiat-collateralized stablecoin, the utility token operates as its own system without any additional smart-contract infrastructure to support its value.
- The value of USDC arises from the promise of redemption for USD by its backing companies, including Coinbase.

Fungible tokens

Governance tokens

- Governance tokens are similar to equity tokens in the sense they represent percentage ownership<u>. Instead of asset ownership, governance token ownership applies to voting rights</u>
- Many smart contracts have embedded clauses stipulating how the system can change; for instance, allowed changes could include adjusting parameters, adding new components, or even altering the functionality of existing components.

Fungible tokens

Governance tokens

- Any platform with admin-controlled functionality is <u>not truly DeFi</u> because of the admins' centralized control.
- A contract without the capacity for change is necessarily rigid, however, and has no way to adapt to bugs in the code or changing economic or technical conditions.
- For this reason, many platforms strive for a decentralized upgrade process, often mediated by a governance token.

Fungible tokens

Governance tokens

- A governance token can be implemented in many ways—with a static supply, an inflationary supply, or even a deflationary supply.
- A static supply is straightforward: purchased shares would correspond directly to a certain percentage control of the vote.
- MKR is an example of a static supply
- COMP is an example of inflationary supply to incentive use of the platform

Part II:

DeFi Primitives

1. The Mechanics of Modern Decentralized Finance

(iii) Non-Fungible Tokens

Non-fungible tokens

ERC-721

- [Switch to draft NFT presentation]

I. DeFi Infrastructure

Modules

1. Mechanics
2. **Supply and Ownership**
   i. Custody
   ii. Supply Adjustment
   iii. Incentives
3. Swaps and Loans
4. Joining the World of DeFi