

Decentralized Finance: Market Design and Governance Structure

Agostino Capponi

Department of Industrial Engineering and Operations Research
Columbia University

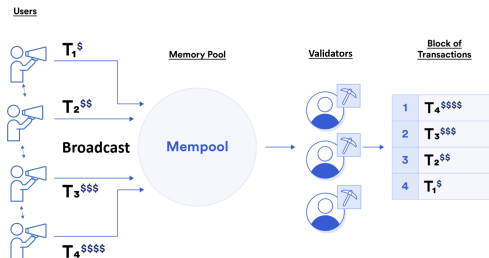
October 21, 2022

Outline

- 1 Introduction
- 2 The Pros and Cons of Transparency
- 3 Governance Risk

Public Blockchain Technologies

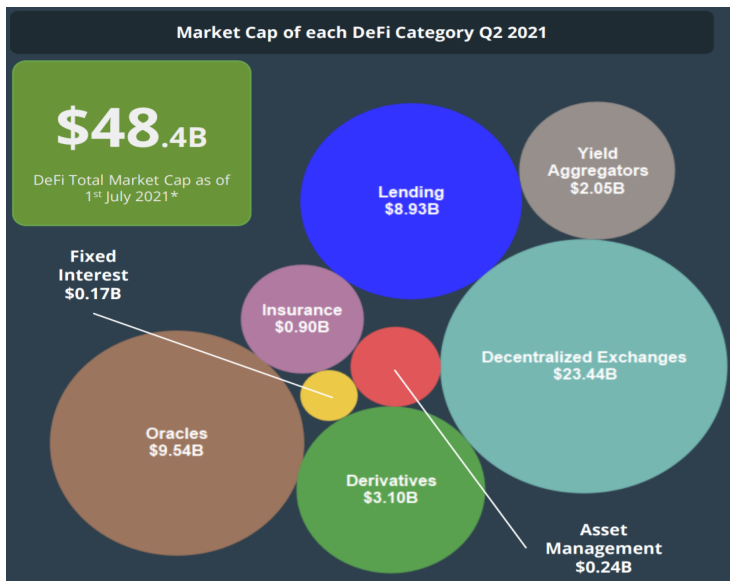
- A blockchain is a digitally distributed, decentralized, public ledger that exists across a network.
- Decentralization through validators, which process orders in batches
- Users submit **blockchain fees** to prioritize their orders.
- Orders pending in the mempools are visible to all.



Decentralized Finance

- Second-generation blockchains support **decentralized finance** (DeFi)
- DeFi is a set of of disintermediated financial services
 - Utilizes open-source smart contracts
 - Provide lending, swapping, and insurance services without any centralized financial intermediary
- DeFi is widely believed to be one of the killer applications for blockchain technologies











DeFi Ecosystem



Key Characteristics of DeFi

- Transparency:
 - Information on settled and pending transactions is publicly available
 - DeFi protocols are hard-coded, open-sourced algorithms:
 - No ambiguity in the contract
 - Settlement of transactions enforced by the smart contract.
- Decentralization:
 - Architecture: distributed ledger
 - Governance: distributed community of token holders

Transparency of Confirmed Transactions

| | |
|---|---|
| Transaction Hash: | 0x7b54d61f6e4624bb704ccd510da460fa80301428994b45ef92f74c9b7caea222  |
| Status: | ✔ Success |
| Block: | 13680579 41 Block Confirmations |
| Timestamp: | 9 mins ago (Nov-25-2021 01:21:11 AM +UTC)  Confirmed within 30 secs |
| Transaction Action: | Swap 235.998068  ALICE For 1.43229536454691122 Ether On  Uniswap V2 |
| From: | 0xbf5ae133b9a0fc1a07952a7df2afa21f7f69ef58  |
| Interacted With (To): | Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2: Router 2)   |
| Tokens Transferred:  | <ul style="list-style-type: none"> From 0xbf5ae133b9a0fc... To Uniswap V2: ALIC... For 235.998068 (\$6,114.71)  ALICE (ALICE) From Uniswap V2: ALIC... To 0xbf5ae133b9a0fc... For 1.43229536454691122 (\$6,200.86)  Wrapped Ethe... |
| Value: | 0 Ether (\$0.00) |
| Transaction Fee: | 0.01677753 Ether (\$72.64) |

Transparency of Pending Transactions

A total of 235,292 pending txns found
(Showing the last 10000 records)

First < Page 1 of 200 >

| Txn Hash | Nonce | Method ⓘ | Last Seen | Gas Limit | Gas Price ⓘ | From | To | Value |
|---------------------------|---------|---------------------|------------|-----------|---------------------|----------------------------|------------------------------|--------------|
| 0x424b6f1f5098b573bf8... | 31 | 0xc0468a59 | 4 secs ago | 296716 | 105.3884 1,5 Gwei | 0x04729689f219cbd549... ▼ | Uniswap V3: Router ▼ | 1,15 Ether 🟢 |
| 0x1f1a68ce3dd59685ed... | 4164316 | Transfer | 4 secs ago | 21000 | 185 2 Gwei | Coinbase 5 ▼ | 0xbcb01a53140e26947... ▼ | 0.05020473 E |
| 0x9df4927481afc763d74... | 13 | Deposit | 4 secs ago | 45038 | 121.5063 1,5 Gwei | 0x433db84f8f1944f3a5... ▼ | Wrapped Ether ▼ | 0.5 Ether 🟢 |
| 0x18059111e7b412f3f5f1... | 475 | Set Approval For... | 4 secs ago | 46747 | 110.2918 1,5 Gwei | 0xf31fc1a5bfa83452184... ▼ | Based Fish Mafia: BFM T... ▼ | 0 Ether 🟢 |
| 0xc733658c0a63c45c5f1... | 73 | Swap Exact Token... | 4 secs ago | 213798 | 105.3884 1,5 Gwei | 0xc4f565416a9034ed52... ▼ | SushiSwap: Router ▼ | 0 Ether 🟢 |

Transparency of Smart Contracts

- DeFi protocols are hard-coded, open-sourced algorithms:
 - There is no ambiguity in the contract
 - Settlement of transactions enforced by the smart contract.

UniswapV2Pair.sol

[This contract](#) [↗] implements the actual pool that exchanges tokens. It is the core Uniswap functionality.

```

1  pragma solidity =0.5.16;
2
3  import './interfaces/IUniswapV2Pair.sol';
4  import './UniswapV2ERC20.sol';
5  import './libraries/Math.sol';
6  import './libraries/UQ112x112.sol';
7  import './interfaces/IERC20.sol';
8  import './interfaces/IUniswapV2Factory.sol';

```

```

1      uint _totalSupply = totalSupply; // gas savings, must be defined here since totalSupply can
      update in _mintFee
2      if (_totalSupply == 0) {
3          liquidity = Math.sqrt(amount0.mul(amount1)).sub(MINIMUM_LIQUIDITY);
4          _mint(address(0), MINIMUM_LIQUIDITY); // permanently lock the first MINIMUM_LIQUIDITY tokens
5
6      } else {
7          liquidity = Math.min(amount0.mul(_totalSupply) / _reserve0, amount1.mul(_totalSupply) /
8          _reserve1);
9
10     }

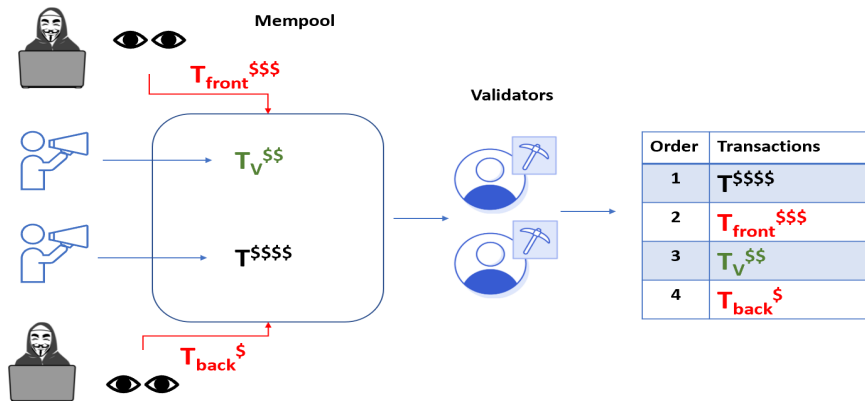
```

Data Analytics

- Does transparency provide actionable information?
 - What is the expected yield of different liquidity pools?
 - Data Analytics: Can we rate different DeFi pools or tokens, like we did for bonds or equity?
 - What is the risk of providing liquidity, or executing borrowing and lending transactions?
 - Capponi and Jia (2021) show that liquidity providers can be exploited by arbitrageurs under the current design of decentralized exchanges.
- **On-chain data analytics and frameworks are needed!**

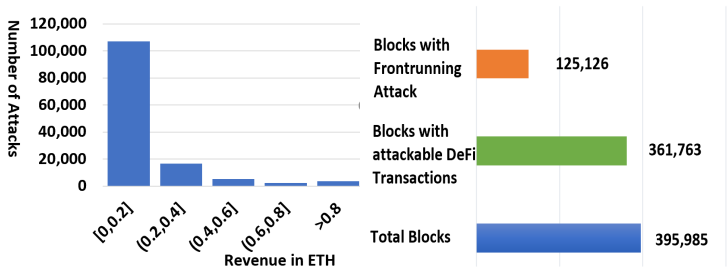
Unintended Consequences of Transparency

Users and Arbitrageurs



Mitigation of Frontrunning Risk

- Transparency may lead to **frontrunning** attacks of DeFi transactions
- Privacy preserving channels (Flashbots, Eden Network) can mitigate these risks
 - Directly route users' transactions to validators without broadcasting
 - Pending transactions are no longer public and thus cannot be frontrun



Will Private Channels be Adopted?

- Capponi, Jia, and Wang (2022) develop a dynamic game theoretical model and show that
 - If the frontrunning problem **is severe**, there exists a unique equilibrium where all validators adopt the private pool
 - if the frontrunning problem **is not too severe**, some validators do not adopt the private pool to preserve *miner extractable value*
- Privacy preserving pools do not provide enough incentives to solve the frontrunning problem.
- Perhaps the solution is at the consensus protocol level? Zero knowledge proof?

DeFi Governance

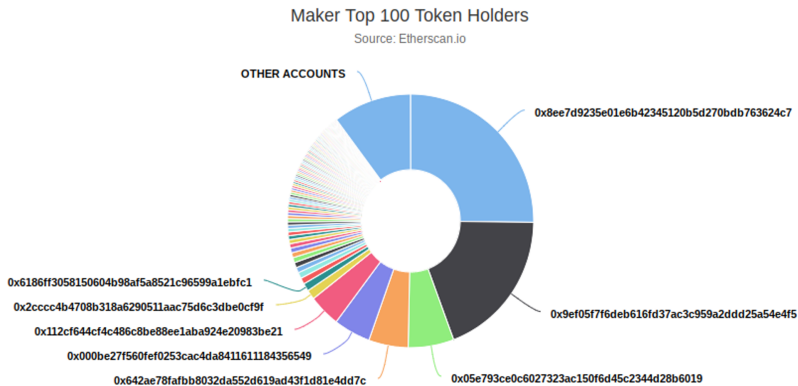
- Governance proposals:
 - Change of protocols (e.g. interest rate and collateral requirement for lending)
 - Allocation of funds, new features or interface, and change of governance system
- Anyone who holds enough governance tokens can submit and vote for governance proposals.

Potential of Governance Tokens

- Transparency and Efficiency:
 - Avoid empty-voting or over-voting problems of traditional proxy-vote systems
- Implement alternative governance structures:
 - Square root voting
 - Voting power as a function of holding time
 - Develop multiple classes of tokens (similar to class A and B shares)

Risk of Centralization

- Few accounts (early investors, developers, big whales) hold most of the tokens
- Development team typically has control of the interface, Treasury, and development of new protocols



Risk of Manipulation and Embezzlement.

- **Tradable governance token + pseudoanonymous + immutable = the best place for manipulation and embezzlement!**
- Manipulators can secretly acquire governance tokens for attacks.
 - Attacker controlled True Seigniorage Dollar (TSD) and rewarded himself with 11.8b worth of TSD in 2021.

Thank you!