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
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 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

Market Cap of each DeFi Category Q2 2021

$48.4B
DeFi Total Market Cap as of 1st July 2021*

- Lending $8.93B
- Yield Aggregators $2.05B
- Decentralized Exchanges $23.44B
- Oracles $9.54B
- Insurance $0.90B
- Derivatives $3.10B
- Asset Management $0.24B
- Fixed Interest $0.17B
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
<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Hash:</td>
<td>0x7b54d616e4624bb704ccd510da460fa80301428994b45ef92f74c9b7cae222</td>
</tr>
<tr>
<td>Status:</td>
<td>Success</td>
</tr>
<tr>
<td>Block:</td>
<td>13880579 - 41 Block Confirmations</td>
</tr>
<tr>
<td>Timestamp:</td>
<td>9 mins ago (Nov-25-2021 01:21:11 AM +UTC)</td>
</tr>
<tr>
<td>Transaction Action:</td>
<td>Swap 235.998068 🌟 ALICE For 1.43229536454691122 Ether On 🌟 Uniswap V2</td>
</tr>
<tr>
<td>From:</td>
<td>0xbf5ae133b9a0fc1a07952a7df2afa21f7f69ef58</td>
</tr>
<tr>
<td>Interacted With (To):</td>
<td>Contract 0x7a250d5630b4cf539739df2c5dabc4659f248dd (Uniswap V2: Router 2)</td>
</tr>
<tr>
<td>Tokens Transferred:</td>
<td>From 0xbf5ae133b9a0fc... To Uniswap V2: ALICE... For 235.998068 ($6,114.71) 🌟 ALICE (ALICE)</td>
</tr>
<tr>
<td>Value:</td>
<td>0 Ether ($0.00)</td>
</tr>
<tr>
<td>Transaction Fee:</td>
<td>0.01677753 Ether ($72.64)</td>
</tr>
</tbody>
</table>
# The Pros and Cons of Transparency

## Transparency of Pending Transactions

A total of 235,292 pending txns found

<table>
<thead>
<tr>
<th>Txn Hash</th>
<th>Nonce</th>
<th>Method</th>
<th>Last Seen</th>
<th>Gas Limit</th>
<th>Gas Price</th>
<th>From</th>
<th>To</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x424b6f1f5098b573bf8...</td>
<td>31</td>
<td>Transfer</td>
<td>4 secs ago</td>
<td>296716</td>
<td>105.3884</td>
<td>0x04729689f219cbd549...</td>
<td>Uniswap V3: Router</td>
<td>1.15 Ether</td>
</tr>
<tr>
<td>0x1f1a68ce3dd59685ed...</td>
<td>4164316</td>
<td>Transfer</td>
<td>4 secs ago</td>
<td>21000</td>
<td>185</td>
<td>Coinbase 5</td>
<td>0xbc0d01a53140e26947...</td>
<td>0.050020473 E</td>
</tr>
<tr>
<td>0x9df4927481afc763d74...</td>
<td>13</td>
<td>Deposit</td>
<td>4 secs ago</td>
<td>45038</td>
<td>121.5063</td>
<td>0x433db84f88f1944f3a5...</td>
<td>Wrapped Ether</td>
<td>0.5 Ether</td>
</tr>
<tr>
<td>0x18059111e7b412f3f55f...</td>
<td>475</td>
<td>Set Approval</td>
<td>4 secs ago</td>
<td>46747</td>
<td>110.2918</td>
<td>0xf31fc1a5bfa83452184...</td>
<td>Based Fish Mafia: BFM T...</td>
<td>0 Ether</td>
</tr>
<tr>
<td>0xc733658c0a63c45c5f1...</td>
<td>73</td>
<td>Swap Exact Token</td>
<td>4 secs ago</td>
<td>213798</td>
<td>105.3884</td>
<td>0x4f565416a9034ed52...</td>
<td>SushiSwap: Router</td>
<td>0 Ether</td>
</tr>
</tbody>
</table>
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.

```
pragma solidity =0.5.16;

import './interfaces/IUniswapV2Pair.sol';
import './UniswapV2ERC20.sol';
import './libraries/Math.sol';
import './libraries/UQ112x112.sol';
import './interfaces/IERC20.sol';
import './interfaces/IUniswapV2Factory.sol';

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

Mempool

Validators

<table>
<thead>
<tr>
<th>Order</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$T$</td>
</tr>
<tr>
<td>2</td>
<td>$T_{\text{front}}$</td>
</tr>
<tr>
<td>3</td>
<td>$T_{\text{v}}$</td>
</tr>
<tr>
<td>4</td>
<td>$T_{\text{back}}$</td>
</tr>
</tbody>
</table>
The Pros and Cons of Transparency

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
The Pros and Cons of Transparency

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!