DeFi: or How I Learned to Stop Worrying and Love the Blockchain

Tejaswi Nadahalli
Finance
Finance

Money

Banks

Stocks

(Stock / Currency) Exchanges

PE / VC / Hedge-Funds
## Decentralized Finance

<table>
<thead>
<tr>
<th>Money</th>
<th>Cryptocurrencies/Tokens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>Blockchains/Lending Protocols/Vaults</td>
</tr>
<tr>
<td>Stocks</td>
<td>Tokens / Synths</td>
</tr>
<tr>
<td>(Stock / Currency) Exchanges</td>
<td>Automated Market Makers</td>
</tr>
<tr>
<td>PE / VC / Hedge-Funds</td>
<td>Decentralized Autonomous Organizations</td>
</tr>
</tbody>
</table>
Decentralized Finance

- Money
- Cryptocurrencies/Tokens
- Banks
- Blockchains/
  Lending Protocols/
  Vaults
- Stocks
  Tokens / Synths
- (Stock / Currency) Exchanges
- Automated Market Makers
- PE / VC / Hedge-Funds
- Decentralized Autonomous Organizations

Expensive
Inefficient
Complex
So, why?
Decentralized Finance
Permission-less
But where exactly?
But where exactly?

The Blockchain!!!
But where exactly?

The Blockchain!!!

No, seriously
But where exactly?

Uniswap V2 - 0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f
But where exactly?

Uniswap V2 - 0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f

0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f = Hash Key
But where exactly?

Uniswap V2 - 0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f

0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f = Hash Key

Hash Value = Contract Code
But where exactly?

Uniswap V2 - 0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f

0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f = Hash Key

Hash Value = Contract Code

Hashmap = Blockchain, which is everywhere
Money

Native to the Blockchain (first level hashmap)
Money

Native to the Blockchain (first level hashmap)

Token on the Blockchain == Nested Hashmaps

Key1 = map1, Key2 = map2,...

Key1 = value1, Key2 = value2,...
Money

Native to the Blockchain

Token on the Blockchain

Example: ERC-20 Token Standard
Money

Native to the Blockchain

Token on the Blockchain

Example: ERC-20 Token Standard

Stable-coins (tokens)
Money

Native to the Blockchain

Token on the Blockchain

Example: ERC-20 Token Standard

Stable-coins (tokens)

Algorithmic

Custodial
Banks

Blockchain/Smart Contract
or
Hashmaps/Nested Hashmaps
Root Hashmap

- Roger’s Key
  - Roger’s Savings Account Balance (CHF 1000)
- Trump’s Key
  - Trump’s Tax Returns
- Compound’s Address
  - ??? (Next slide)
- Cryptopunk’s Address
  - An image with 10000 faces
- Your key
  - 0
Lending Protocol

Smart Contract (code/logic) + Storage (hashmaps = pools of capital)

Depositor

Capital

Interest

Borrower

Collateral

Loan

Liquidator

Loan

Collateral

Loan/Collateral Price Ratio

Oracle
Constant Function Market Maker (Uniswap)

$$A \times B = 2500$$
<table>
<thead>
<tr>
<th>Proposal Created</th>
<th>Voting Active (3 Days)</th>
<th>Voting Ends</th>
<th>Timelock (2+ Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PENDING</strong></td>
<td><strong>ACTIVE</strong></td>
<td><strong>SUCCEEDED</strong></td>
<td><strong>EXECUTED</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>QUEUED</strong></td>
<td><strong>EXPIRED</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>DEFEATED</strong></td>
<td></td>
</tr>
</tbody>
</table>

**CANCELED**
What can go wrong?

Trusted Third Party = ☠ ☠ ☠

- Oracles
- Stablecoins
- Contract Deployer
2021 is the new 2008?

Stablecoin

Smart Contract API

Lending Platforms

Uniswap/DEX
Public Mempool

MEV