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

*ETH Zurich – Distributed Computing Group – www.disco.ethz.ch*

Tejaswi Nadahalli

# Stock Exchange


Market Makers
Purchaser's Custodian
Seller's Custodian
Stock Exchange(s)
Purchaser's Broker
Seller's Broker
Share Purchaser
Share Seller


MegaCorp
Registrar / Stock Transfer Agent
Regulator, Reporting Destinations, Taxation Authorities, ...
Central Securities Depository
Purchaser's Custodian
Market Makers
Seller's Custodian
Stock Exchange(s)
Purchaser's Broker
Clearing House(s)
Seller's Broker
Share Purchaser
Share Seller

I own 10 Apple shares*

*Share = Unit of Stock

I have 5 Apple shares
I want some Google shares

You have 20 Google shares
You want some Apple shares

# Order Book


## Ask

I want to buy X

How much Y should I give?

## Bid

I have to sell X

How much Y will I get?

Many counterparties = Matching algorithms

No counterparties?

# Market Maker

Has both assets

Always quotes a price

And has deep pockets

Specialist operator/Entry barrier

Goes out on nights/weekends

Doesn’t handle long tail assets

Uniswap
or
Automated Market Maker
or
Constant Function Market Maker

Automated

Computer Code

# Constant Function

$$GOOG * AAPL = 100^{*}$$

* Any constant will do

# Traditional Market Maker

You have 20* GOOG and 5* AAPL

* 20 * 5 = 100

You put 20 GOOG and 5 AAPL in a pool and go away to do Via-Ferrata

Pool = 20 GOOG, 5 AAPL

I want to buy 3 AAPL

How many GOOG must I give?

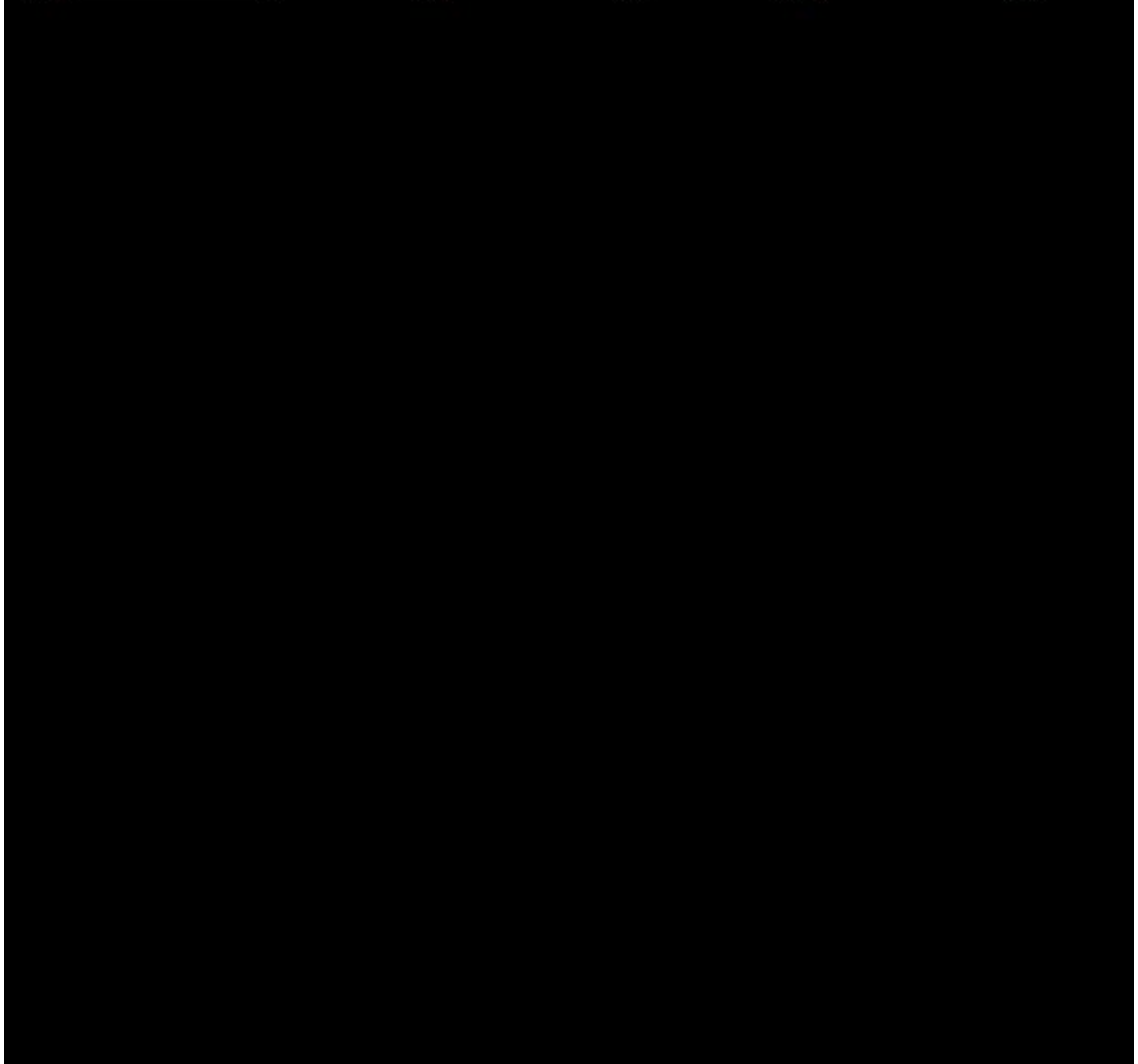
$5 * 20 = 100 = (5 - 3) * (20 + X)$

$X = 30$

Pool = 50 GOOG, 2 AAPL

# But... is the price good?

| Exchange Price | | Uniswap Pool | | Product | Trader | |
|---|---|---|---|---|---|---|
| 1 | 5 | 20.00 | 20.00 | 400 | Price/Profit | |
| 1 | 5 | 16.00 | 25.00 | 400 | 4.0 | 3.0 |
| 1 | 5 | 13.33 | 30.00 | 400 | 2.67 | 1.67 |
| 1 | 5 | 11.43 | 35.00 | 400 | 1.90 | 0.90 |
| 1 | 5 | 10.00 | 40.00 | 400 | 1.43 | 0.43 |
| 1 | 5 | 8.89 | 45.00 | 400 | 1.11 | 0.11 |



# What’s in it for you?

Liquidity Fees - 0.3% on Uniswap 😊

# Why would I do this?

Unstoppable

Permissionless (no KYC)

Always-on (fluid price)

Programmable

On what should I do this?

Not GOOG/AAPLs/Bananas

ERC-20 Tokens

What?

How?

# Ethereum Blockchain*

* World Computer

| | |
|---|---|
| Shares<br>Custodian | ERC-20 Tokens<br>(Smart Contract/Wallet) |
| Exchange (A⇔B) | Smart Contract |
| Trade | Transaction |
| Price | A * B = $K$ |
| ~~Exchange Creator~~<br>Uniswap | Smart Contract |

# Where on Ethereum?

Uniswap V2 - 0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f

Uniswap V1 - 0xc0a47dFe034B400B47bDaD5FecDa2621de6c4d95

Immutable

Forced to be simple, to be cheap

# Who else?

| | | | | |
|---|---|---|---|---|
| Uniswap | 0.3% | $2.6B/451M | X-Y (5K+ pairs) | A * B = $K$ |
| Curve | 0.04% | $716M/106M | Stable Coins | $An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$. |
| Balancer | 0.15% | $281M/9M | [X1, X2, X3…] | $\prod x_i^{w_i} = \text{const.}$ |
| SushiSwap* | 0.3% | $255M/24M | X-Y Pairs | A * B = $K$ |

# Who loses?

Liquidity Provider suffers

*Impermanent Loss*

# Impermanent Loss

| Exchange Price | | Uniswap Pool | | Trader | | Pool Value |
|---|---|---|---|---|---|---|
| 1 | 5 | 20.00 | 20.00 | Price/Profit | | 120 |
| 1 | 5 | 16.00 | 25.00 | 4.0 | 3.0 | 105 |
| 1 | 5 | 13.33 | 30.00 | 2.67 | 1.67 | 96.65 |
| 1 | 5 | 11.43 | 35.00 | 1.90 | 0.90 | 92.15 |
| 1 | 5 | 10.00 | 40.00 | 1.43 | 0.43 | 90 |
| 1 | 5 | 8.89 | 45.00 | 1.11 | 0.11 | 89.45 |

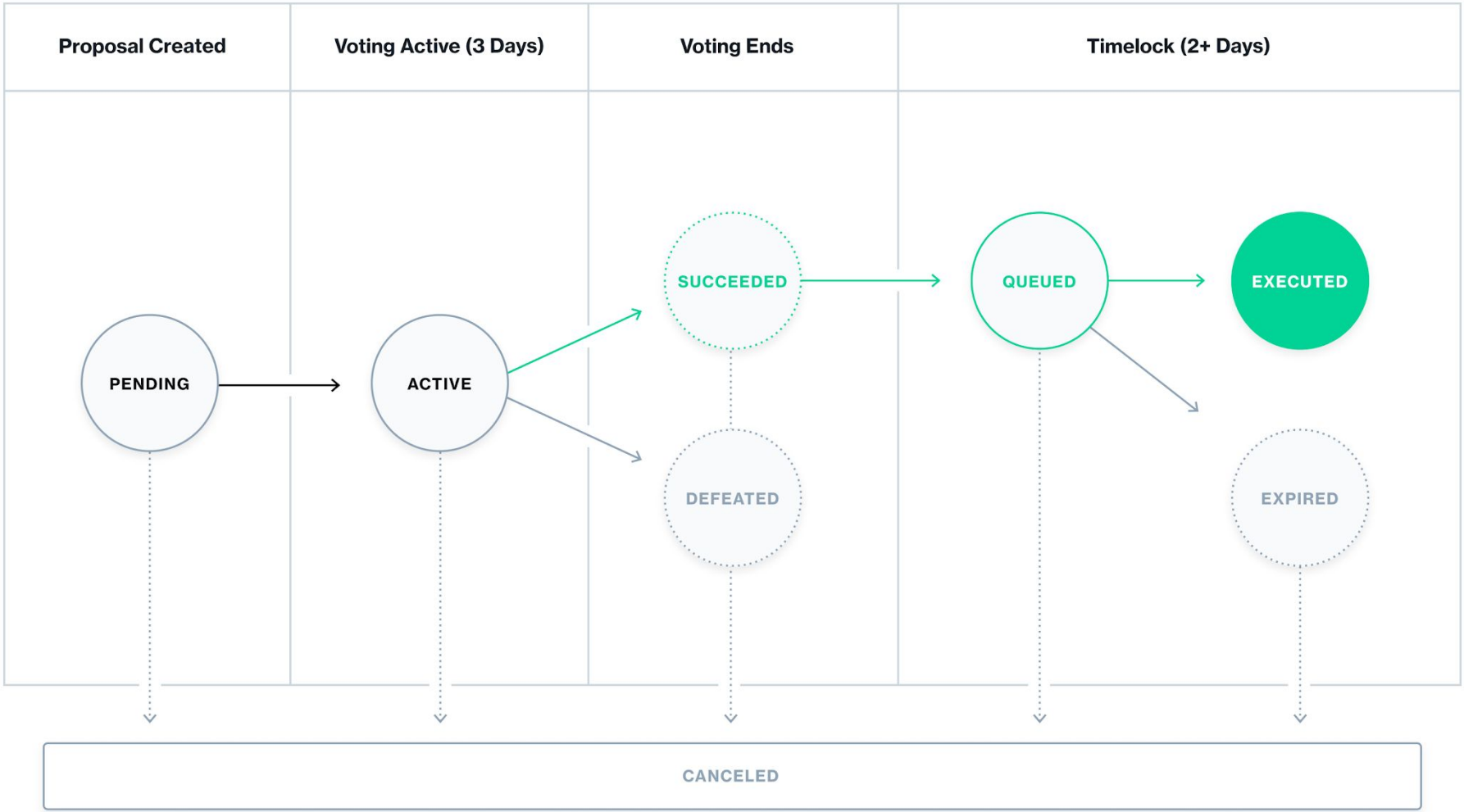
# Two Other Tokens

# Liquidity Provider (LP) Token

Bookkeeping for LP’s

How much of the pool do you own?

# Governance Tokens


Proposal Created
Voting Active (3 Days)
Voting Ends
Timelock (2+ Days)
PENDING
ACTIVE
SUCCEEDED
DEFEATED
QUEUED
EXECUTED
EXPIRED
CANCELED

# Vampire Attacks

# SushiSwap

Copy (open source) Code of Uniswap

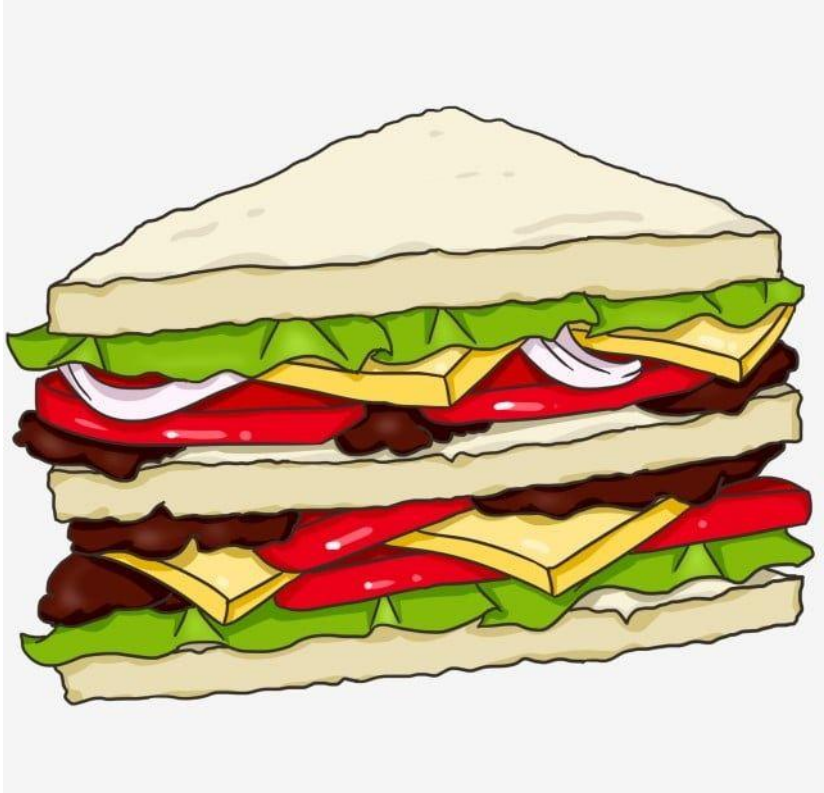
Add Governance Token (Sushi)

Give Sushi for Uniswap LP Token

Sweep Uniswap Pools to SushiSwap

# Frontrunning

# Sandwich Attack



Trader submits transaction TX - in the open

Attacker is watching

Attacker constructs TX1, bids high fee

← TX1 is confirmed

TX is confirmed

Attacker constructs TX2

← TX2 is confirmed

# Composability

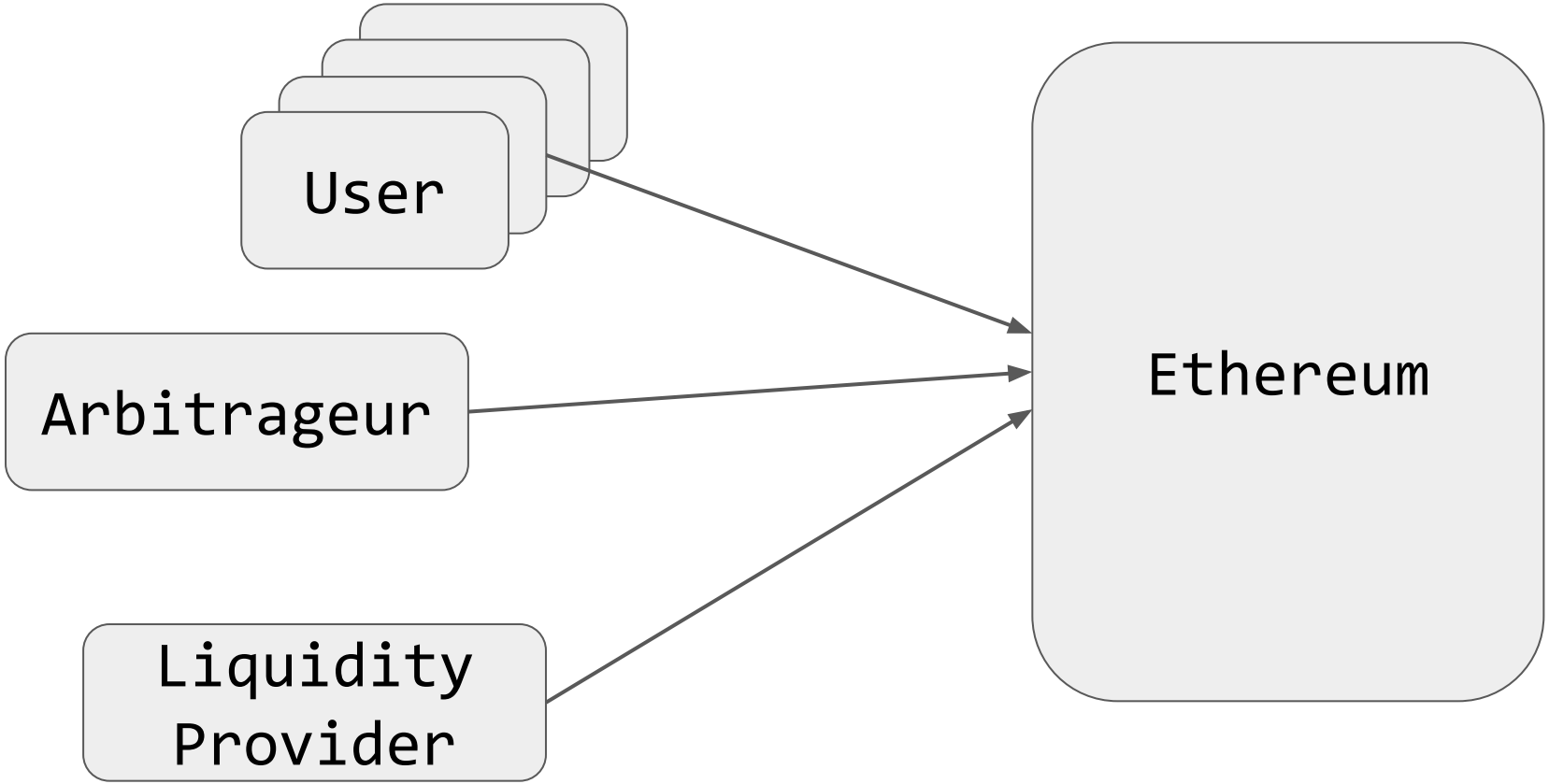
# 2021 is the new 2008?

Stablecoin

Smart Contract API


Lending Platforms

Uniswap/DEX


User
Arbitrageur
Liquidity Provider
Ethereum