A PRESENTATION

Blockchain

Finance

EVOLUTION OF DEFI

Incentives

Presented by Adrian Li

Design

AGENDA

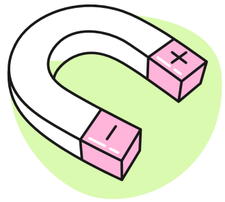
INTRODUCTION

A short introduction to myself and DeFi.

FOUNDATION

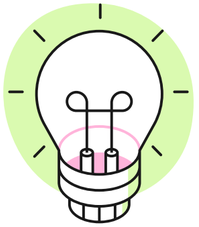
The core concepts that build up the industry.

BEYOND



Considerations of DeFi beyond the technical.

CONCLUSION



Closing out the discussion.

INTRODUCTION

WHAT IS DEFI?

1 PEER-TO-PEER

A financial system built on blockchain technology that enables peer-to-peer transactions without intermediaries such as banks or financial institutions.

2 DECENTRALIZED

DeFi protocols operate on decentralized networks and smart contracts, making them trustless, transparent, and permissionless.

3 UNIVERSAL ACCESS

DeFi has the potential to democratize finance by providing access to financial services to anyone with an internet connection, regardless of their location, identity, or credit history.

DIFFERENCES

TRAD-FI

- Intermediaries required (banks, financial institutions)
- Centralized control and authority
- Limited accessibility based on location, identity, and credit history
- High fees and long processing times
- Closed and opaque

DE-FI

- No intermediaries required
- Decentralized control and authority
- Accessible to anyone with an internet connection
- Lower fees and faster processing times
- Open and transparent

WHY DEFI MATTERS

ACCESS, FREEDOM, DEMOCRACY

FOUNDATION

STABLECOINS

FIAT-BACKED

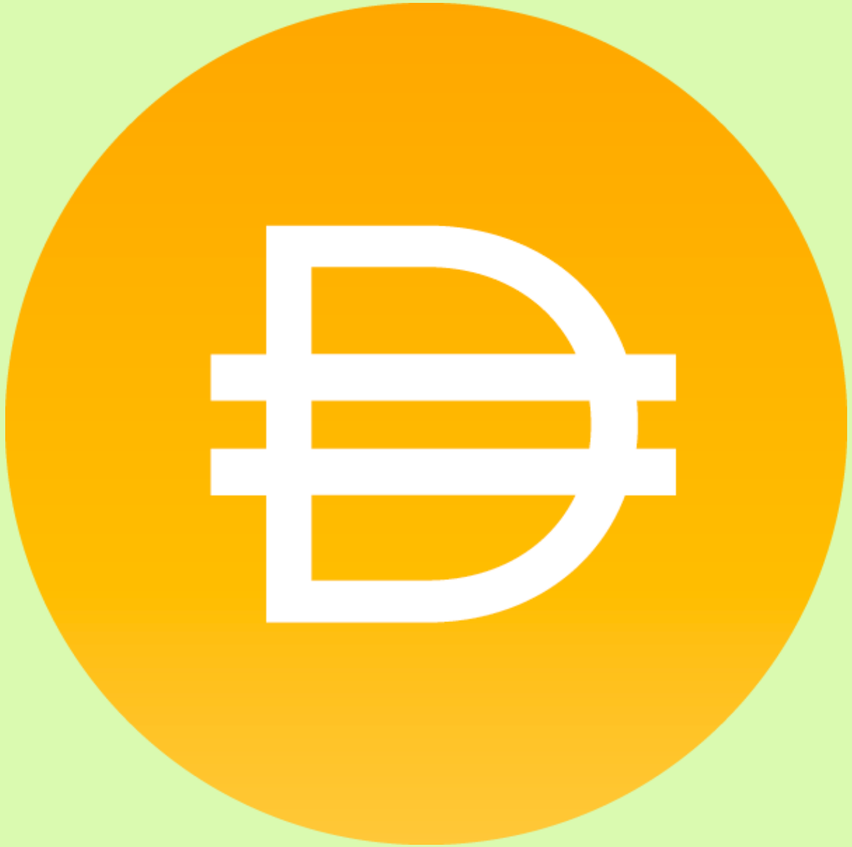
USDT (2014) and USDC (2018) are the most popular fiat-backed stablecoins on the market today.

Both claim that they have enough reserves for 1-to-1 redeem-ability should the need arise.

CRYPTO-BACKED

DAI (2017) is a USD-pegged stablecoin backed by a diverse range of crypto assets.

If the value of any collateral assets fall below a certain threshold, a liquidation is triggered so that DAI can maintain its price.



ALGO-BACKED

Ampleworth (2018) is a pioneering algorithmic stablecoin with automatic supply and demand adjustments via smart contracts.

While there are various other algo-backed stablecoin models, the common theme is that they are not fully backed by liquid assets, and their peg maintenance is still a research topic.

Elastic supply

- If price > $1, give everyone more
- If price < $1, take some from everyone

STABLECOINS

FIAT BACKED

- Backed by real assets in a bank account
- Subject to government oversight
- Might require KYC/AML to mint/burn

CRYPTO BACKED

- Backed by over-collateralizing crypto assets
- Can be trustless
- Requires a robust liquidation system

ALGO-BACKED

- Algorithms on smart contracts can control supply and demand in different ways
- Can be extremely dangerous
- Hybrid solutions exist

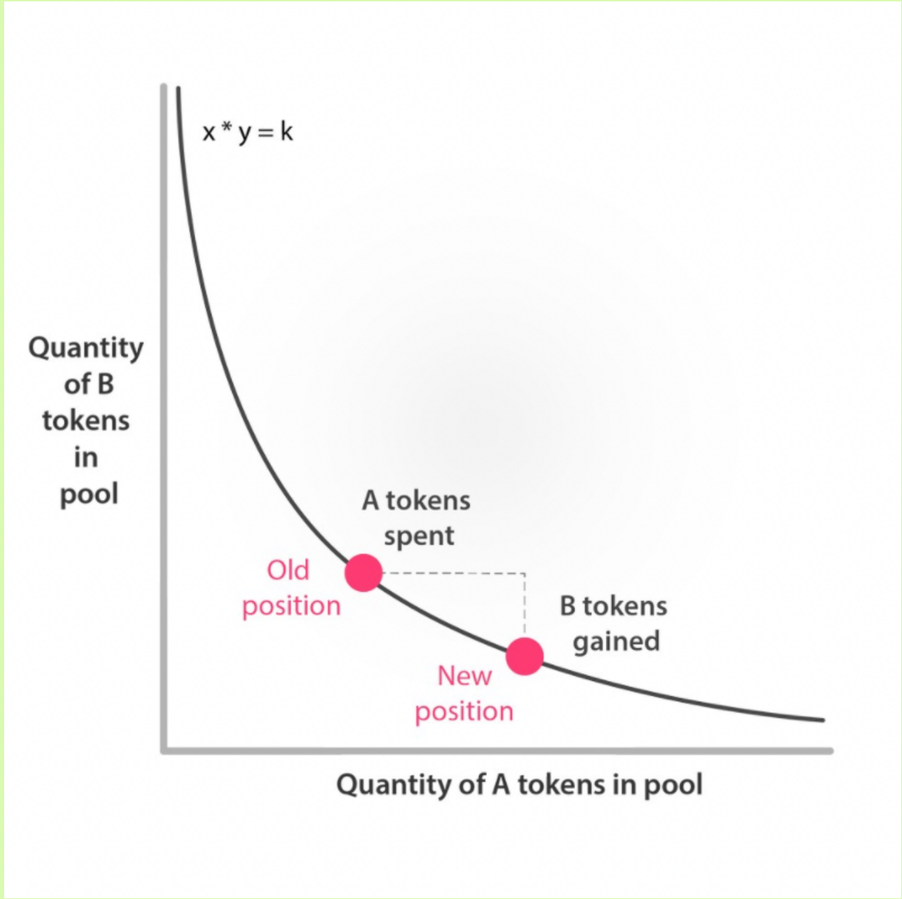
→ **MOST TO LEAST STABLE** →

AUTOMATED MARKET MAKERS

WHAT IS AN AMM?

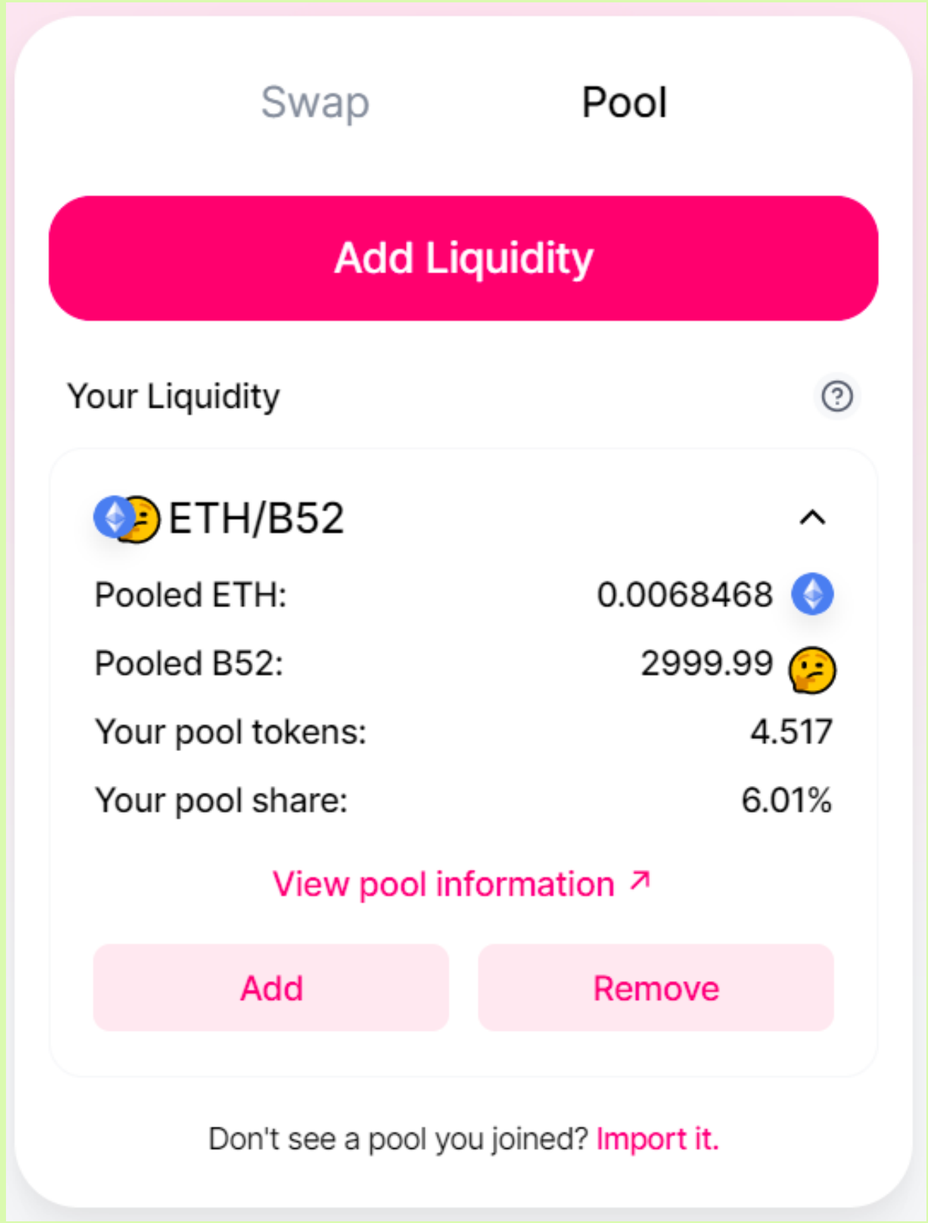
Automated Market Makers (AMMs) are decentralized exchanges (DEXs) that use a mathematical formula to determine the price of assets and facilitate trades without the need for order books.

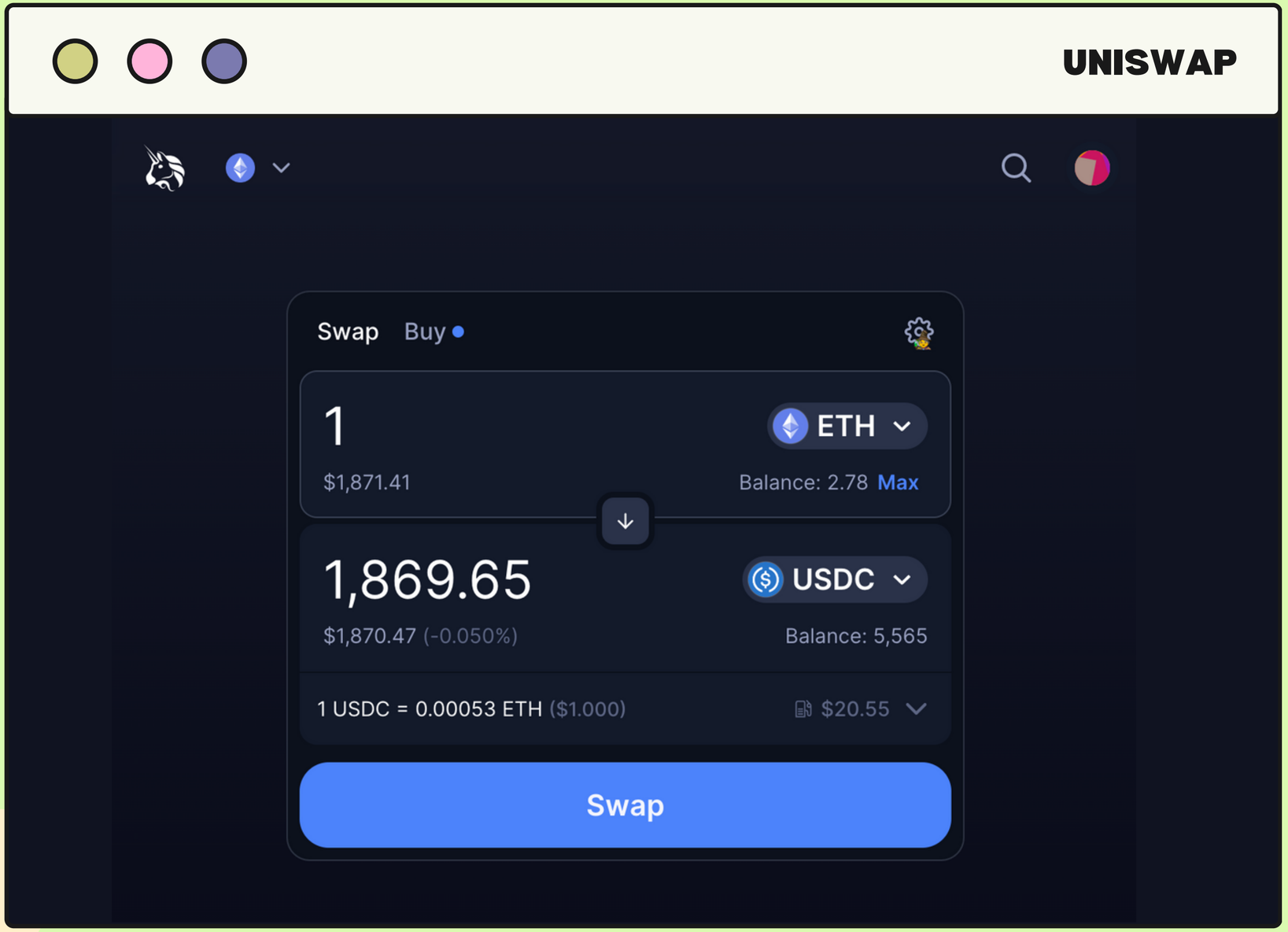
x * y = k



LIQUIDITY PROVIDERS

LPs are critical to the functioning of Automated Market Makers (AMMs) by providing the tokens necessary for trading on the platform and earning a share of the trading fees generated by the platform, while also enabling users to earn passive income and support the growth of the DeFi ecosystem.




UNISWAP
Swap
Buy
1
ETH
$1,871.41
Balance: 2.78 Max
1,869.65
USDC
$1,870.47 (-0.050%)
Balance: 5,565
1 USDC = 0.00053 ETH ($1.000)
$20.55
Swap

LENDING AND BORROWING

WHY LEND AND BORROW?

1 IMPORTANCE

One of the core building blocks of a financial system is the ability to lend and borrow. This increases the capital efficiency of an economy.

2 LENDING

People with assets can put them into a lending protocol to earn yield instead of simply letting it sit.

3 BORROWING

People who need to borrow some tokens are willing to pay lenders for this benefit.

Assets to supply

Hide —

Show assets with 0 balance

Assets	Wallet balance	APY	Can be collateral	
ETH	2.79	1.70 %	✓	Supply Details
USDC	1,565.89	2.97 %	✓	Supply Details
WETH	0.2500000	1.70 %	✓	Supply Details

Assets to borrow

Hide —

To borrow you need to supply any asset to be used as collateral.

Asset	Available	APY, variable	APY, stable	
DAI	0	3.95 %	12.68 %	Borrow Details
FRAX	0	3.88 %	—	Borrow Details
GUSD	0	3.79 %	—	Borrow Details

YIELD FARMING

WHAT IS YIELD FARMING?

- **Definition:** Earning rewards by staking or lending assets on DeFi platforms.
- **Process:** Deposit assets, receive rewards for liquidity provision or governance participation.
- **Benefits:** Additional income, increased liquidity and participation on DeFi platforms.
- **Risks:** Smart contract risk, impermanent loss, high volatility. Careful consideration is advised.

Curve

You haven't connected a wallet. **Connect wallet**

Curve pools

C

All | **USD** | **BTC** | **ETH** | **Crypto** | **Others** | **My Dashboard**

[X] Hide very small pools

Pool	Base vAPY ? Rewards tAPR ?	Volume	TVL ▼
3pool USD DAI+USDC+USDT	0.10% +0.28% →0.69% CRV	$42m	$1.6b
stETH concentrated USD FACTORY WETH+stETH	3.76% +0.00% →0.00% CRV +4.02% LDO	$406k	$688.6m
ironbank USD cyDAI+cyUSDC+cyUSDT	1.27% +2.04% →5.09% CRV	$385.8k	$152.8m
Compound USD cDAI+cUSDC	1.20% +0.35% →0.89% CRV	$0	$101.6m
sUSD USD DAI+USDC+USDT+sUSD	0.42% +2.18% →5.46% CRV	$3.5m	$94.9m

FLASH LOANS

FLASH LOANS

1 ATOMIC

Flash loans are a type of DeFi lending that allow users to borrow funds without collateral for within a single transaction.

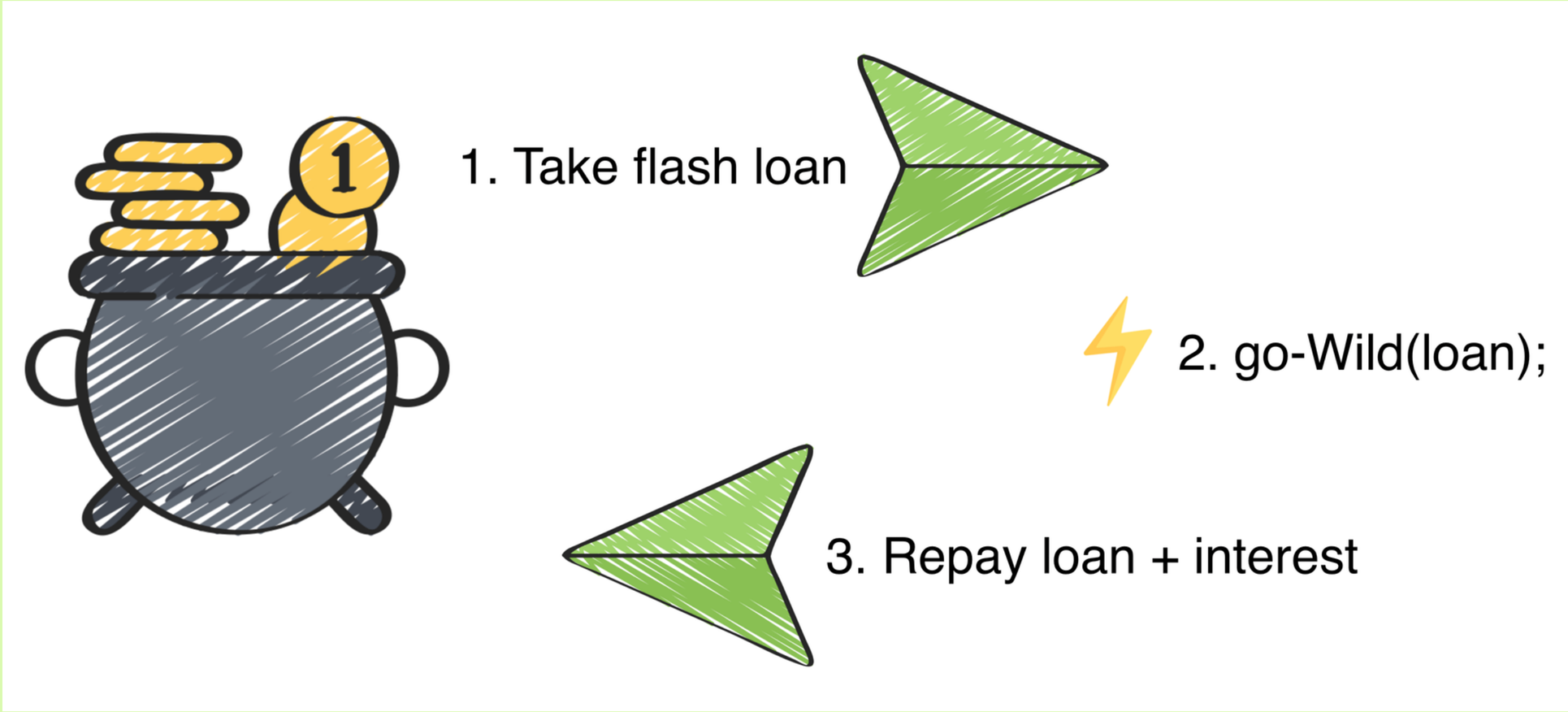
2 ACCESS

Flash loans provide universal access to massive capital for anyone, as long as their transaction is profitable.

3 USES

Can be used for arbitrage, collateral swapping, liquidation prevention, and any other profitable activity that can be executed in one transaction.

IN ONE TRANSACTION



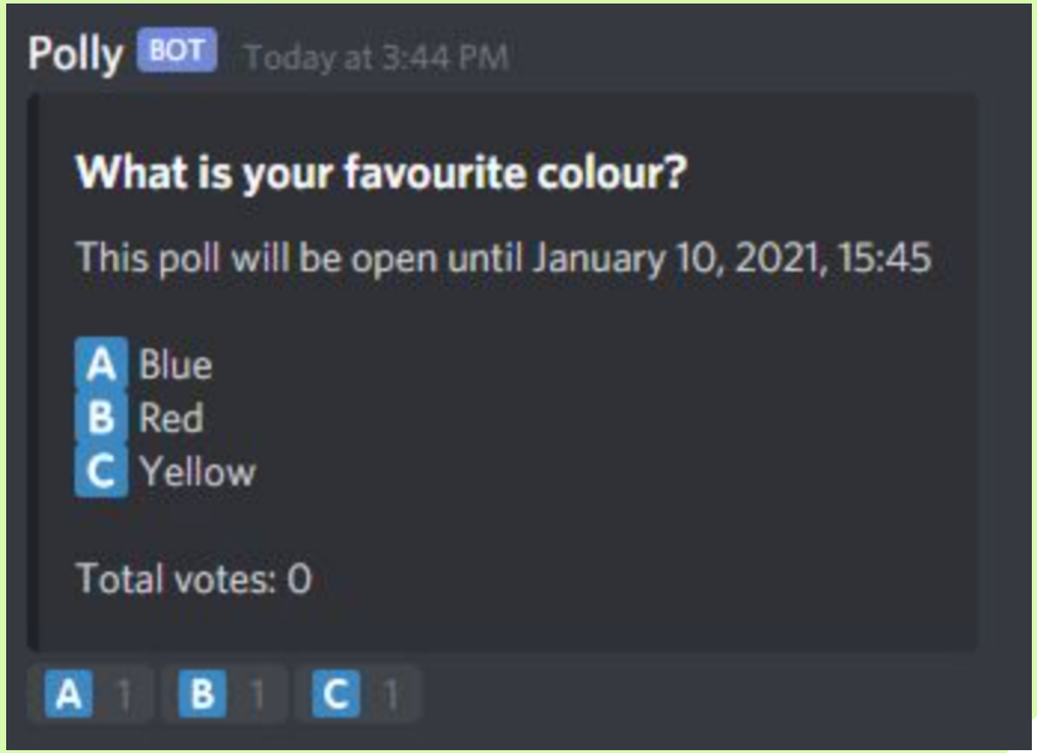
https://hackingdistributed.com/2020/03/11/flash-loans/

BEYOND

GOVERNANCE

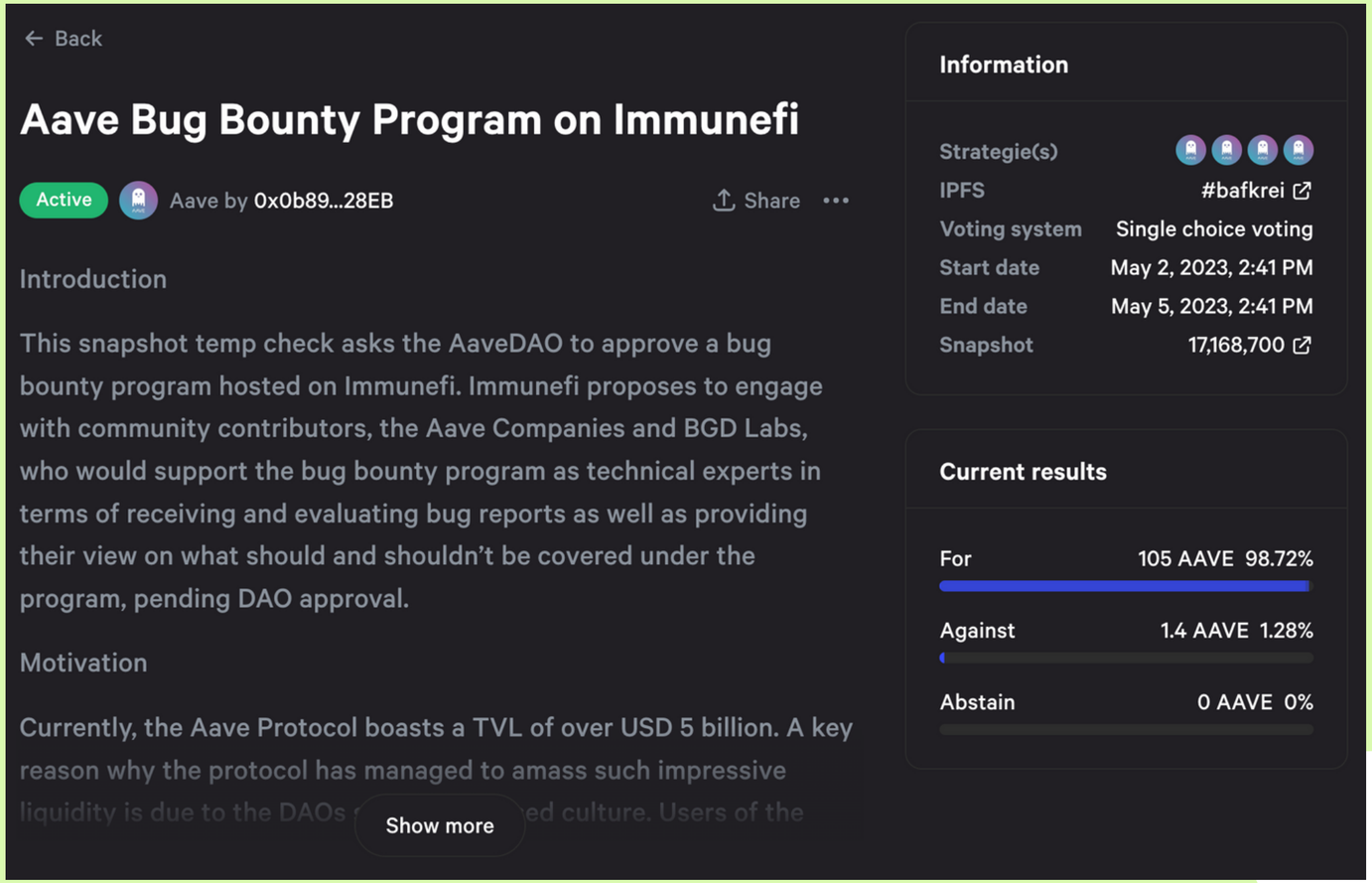
FORUM & CHAT VOTING

- Done through online forums or chat groups.
- Non-binding, and results may not be accurate or secure.
- May not require holding specific tokens or having a minimum threshold of tokens to participate.
- Very fast and convenient.



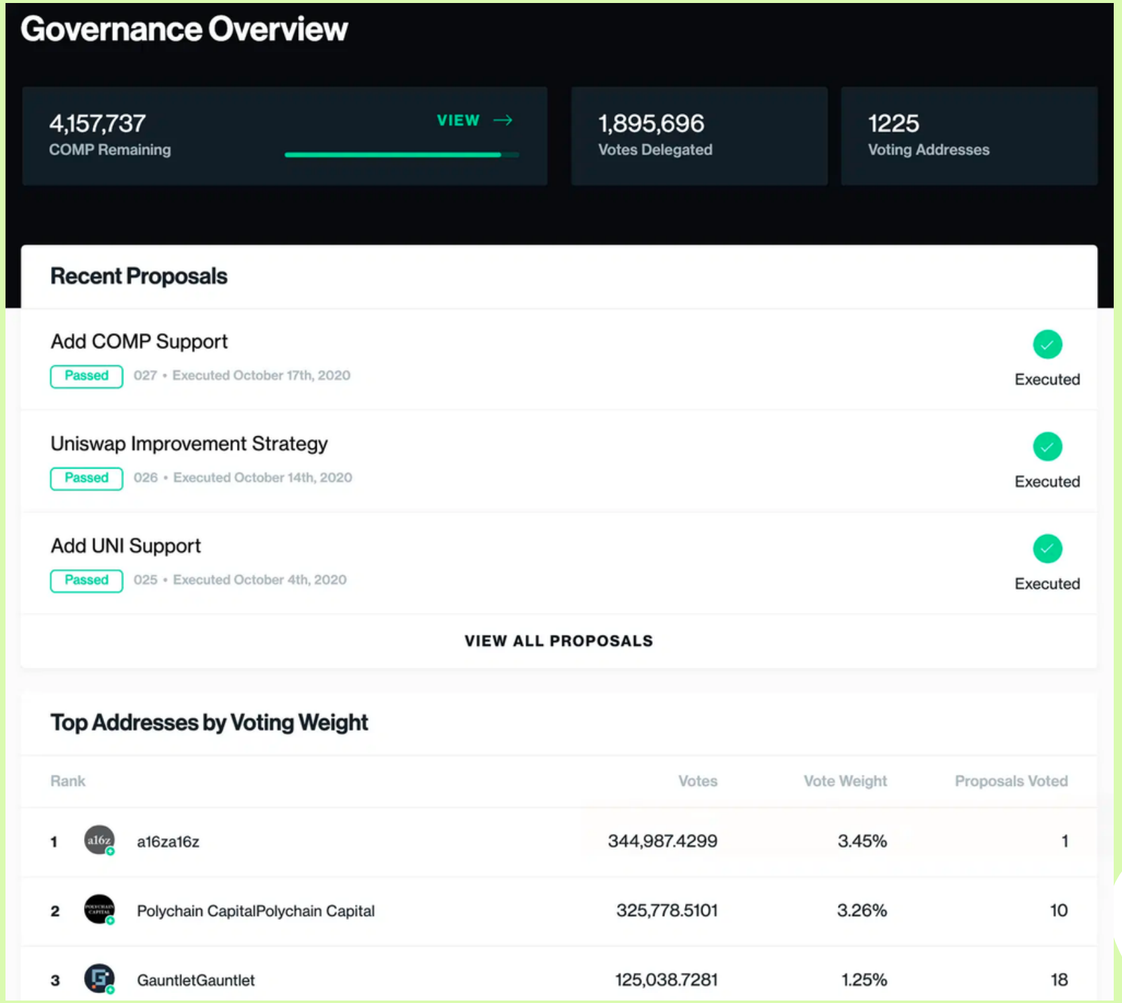
SNAPSHOT VOTING

- Uses a snapshot at a certain block number to capture token balances (i.e. voting power)
- Votes are signed with user's wallets and stored off-chain with snapshot, eliminating gas fees
- Snapshot tallies the votes (on IPFS) and records the result on-chain in a single transaction, reducing costs
- Snapshot voting is decentralized and cost-effective, while maintaining the integrity of votes



ON-CHAIN VOTING

- Votes are recorded directly on the blockchain
- Every vote is a separate transaction that requires gas fees
- More expensive and slower than snapshot voting, but it is fully on-chain and fully decentralized
- Usually used for high-stakes votes where security is a top priority



TYPES OF VOTING

FORUM VOTES

- Uses online forums or chat groups
- Results may not be accurate or secure
- Super easy

SNAPSHOT VOTES

- Off-chain votes
- Proposals and votes stored on IPFS
- Only the result is posted to the blockchain

ON-CHAIN VOTES

- Everything is done on-chain
- Execution of the decision is also done on-chain
- Highest security but also the most costly

LEAST TO MOST IMMUTABLE

SECURITY RISKS

SMART CONTRACT RISK

1 FLAWS IN THE CODE

Smart contracts can have flaws that can be exploited. Flaws like rounding errors can lead to large exploits.

2 EXTERNAL DEPENDENCY

If a smart contract depends on values external from itself. There is a possibility of an economic attack.

One such example is **oracle manipulation**:

- For example, someone can flash loan a large amount of money,
- Use the money to change the price of a token briefly, and
- Manipulate the smart contract that depends on the external token price

SOCIAL ATTACKS

1 PONZI SCHEMES

Some protocols use new users' money to pay older users. The protocol will keep succeeding until there are no more new entrants. At which point there will be a sudden collapse.

2 PHISHING

By pretending to be a reputable website or a trusted wallet, hackers can trick users into entering their passphrases or secret keys.

3 EXIT SCAMS

Leadership of the project can simply leave the project. Or in some cases, there is a hidden function allowing them to print unlimited tokens to dilute the supply.

REGULATORY RISK

1 GREY ZONE

The regulatory risks of DeFi arise from the fact that there is currently little to no regulation of DeFi platforms and their associated tokens. It is not clear whether some assets are securities or not.

2 SUDDEN CHANGES

Regulatory changes could occur suddenly, making DeFi platforms illegal or subject to new rules and regulations that may be burdensome and expensive to comply with.

3 SANCTIONS

A platform may inadvertently violate economic sanctions and face regulatory consequences. One such recent example is **TornadoCash** and **OFAC compliance.**

CONCLUSION

CONCLUSION

- DeFi is an evolving ecosystem that offers financial services and products to users around the world, with a focus on transparency, efficiency, and accessibility.
- Key concepts and innovations in DeFi include automated market makers, yield farming, flash loans, and lending and borrowing.
- DeFi has unique features that differentiate it from traditional finance, such as its decentralized governance model and open-source nature.
- Users should carefully consider the risks and potential drawbacks before participating in DeFi activities.
- Overall, DeFi represents a paradigm shift in the way that financial services are provided, and it will continue to grow and evolve in the coming years.

DEFI EVOLVED

THANK YOU

Feel free to contact me @adrianmcli