Decentralized Finance

MGT 4074 Fintech & Crypto Tokens, Section A, Spring 2025

Joseph Hall

Georgia Institute of Technology

September 29, 2025

Welcome! Today is Monday 9/29/25

Thank you for submitting Homework #2.
For Wednesday: Please read:
"Don't Trust, Verify"
by Marthe Naudts on Medium

Verification of Completion for HW2

- Anyone with an internet connection can verify that *someone* did your homework
- Anyone (e.g. Nnadozie and me) who knows the mapping of wallets to names can verify who

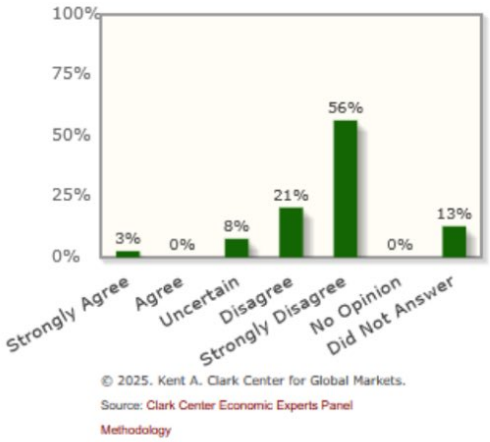
The contract

The token

In the News: Economists Remain Crypto Bears

The US economy would benefit substantially by borrowing money to form a strategic crypto asset reserve fund.

Responses



Responses weighted by each expert's confidence

CHICAGO BOOTH | Kent A. Clark Center for Global Markets

2013 Nobel Laureate Eugene Fama: Crypto "will go to zero within 10 years".

In the News: CFPB to Pause All Enforcement

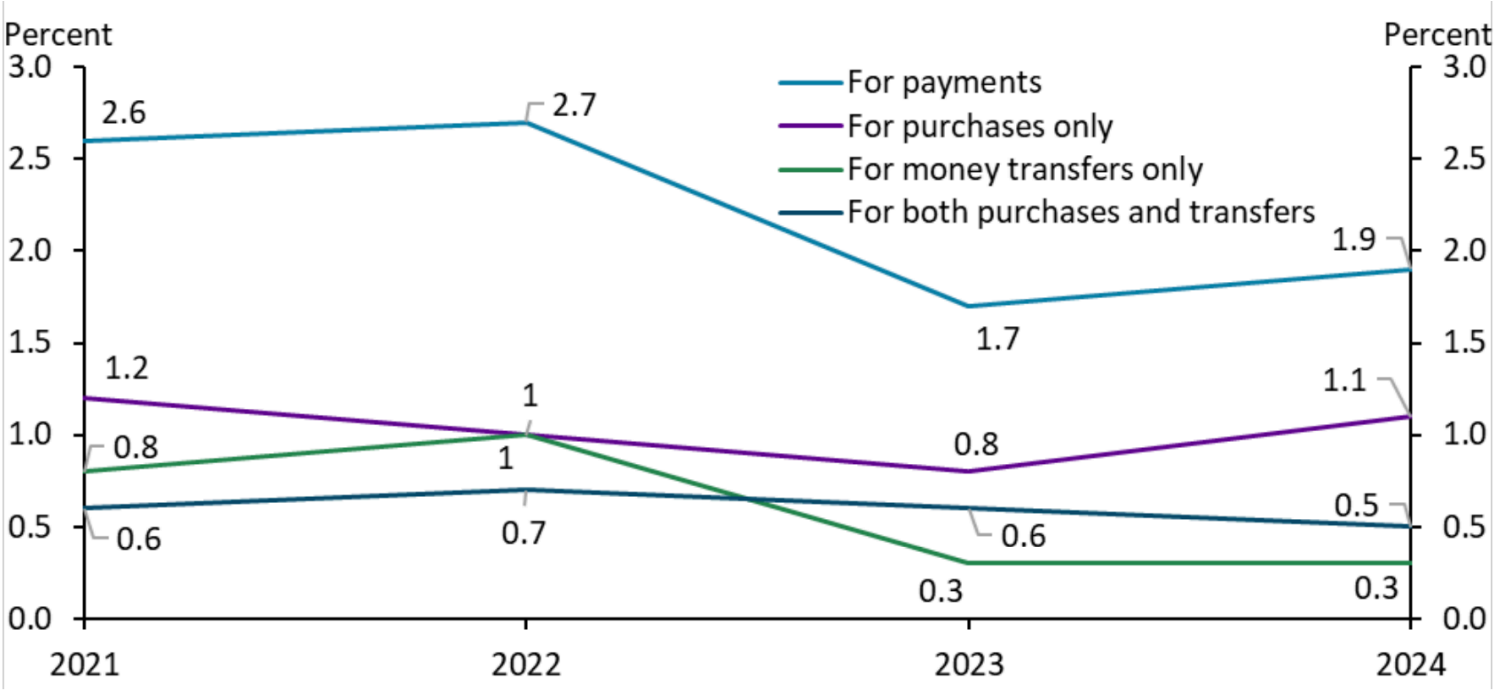
Employees expect CFPB to terminate all enforcement actions

The embattled regulator has dropped more than half its Biden-era docket, including cases against Apple and U.S. Bank. But insiders at the bureau say that's just the beginning.

In the News: Downward Trend in Crypto Payments

From Hayashi & Routh:

Chart 1: The share of U.S. consumers who use cryptocurrency for payments has declined slightly



Sources: Board of Governors of the Federal Reserve System and authors' calculations.

Matt Levine's Commentary

"I suppose it is often the case that a technology is introduced with great hype to solve one particular problem, and then turns out to be more or less irrelevant to that problem but quite useful for some other problem. Here Bitcoin was introduced to allow for peer-to-peer permissionless payments, for which it has turned out to be a dud. But Bitcoin is very good at an unrelated thing, which is "going up in price." (You can see why that would make it bad as a payments medium!) So it has caught on and become widely adopted, even though its original premise was kind of wrong."

Matt Levine's Commentary, Contd.

"Incidentally the point of that Kansas City Fed research note appears to be to express skepticism about stablecoins as a payments mechanism, in the face of growing optimism elsewhere. I don't know if that follows. Crypto is not widely used for payments for a number of reasons, including (1) prices are volatile, (2) you can't reverse payments and (3) you can't send crypto from your bank's app. Stablecoins fix the first problem and, with a certain amount of pushing to become part of the financial mainstream, could solve the other two as well."

Backtracking: Bremmerman's Limit

In our unit on Cryptography and Blockchains, I forgot to mention the very important **Bremmerman's Limit**.

Bremmerman's Limit gives an upper bound to computation speed in the physical universe. It is 1.4×10^{50} **bits per second per kilogram**.

A Bremmerman computer the mass of Earth could theoretically crack a 256-bit hash in about 2 minutes, or a 512-bit hash in 10^{75} years.

Problems which require more than 10^{93} bits of computation are called **transcomputational**, meaning a Bremmerman computer the size of Earth would not solve the problem within the current estimated age of Earth.

In practice, of course, engineering considerations restrict feasible computers far, far below this limit. Suffice it to say, your on-chain assets are safe from a brute force attack for the forseeable future.

Roadmap

1. Pain Points of TradFi
2. Promise of DeFi
3. Lending Protocols
4. Derivatives

Roadmap

1. Pain Points of TradFi
2. Promise of DeFi
3. Lending Protocols
4. Derivatives

The Traditional Financial System

- The traditional financial system allows people and institutions to trade time and risk, using promises
- The purpose of the system is to enable agents to smooth consumption and share risk

The Traditional Financial System

- The traditional financial system allows people and institutions to trade time and risk, using promises
- The purpose of the system is to enable agents to smooth consumption and share risk
  - Essential functions for a society!
  - When thinking about defi, remember the purpose of finance!

The Traditional Financial System

- The traditional financial system allows people and institutions to trade time and risk, using promises
- The purpose of the system is to enable agents to smooth consumption and share risk
  - Essential functions for a society!
  - When thinking about defi, remember the purpose of finance!
- But not all is good with tradfi:
  - Complexity
  - Rents
  - Justice
  - Access

A Promise in Tradfi

ISDA®

International Swaps and Derivatives Association, Inc.

2002 MASTER AGREEMENT

dated as of .....

..... and .....

have entered and/or anticipate entering into one or more transactions (each a "Transaction") that are or will be governed by this 2002 Master Agreement, which includes the schedule (the "Schedule"), and the documents and other confirming evidence (each a "Confirmation") exchanged between the parties or otherwise effective for the purpose of confirming or evidencing those Transactions. This 2002 Master Agreement and the Schedule are together referred to as this "Master Agreement".

Accordingly, the parties agree as follows:—

Source

A Promise in Tradfi

ISDA®

International Swaps and Derivatives Association, Inc.

2002 MASTER AGREEMENT

dated as of .....

..... and .....

have entered and/or anticipate entering into one or more transactions (each a "Transaction") that are or will be governed by this 2002 Master Agreement, which includes the schedule (the "Schedule"), and the documents and other confirming evidence (each a "Confirmation") exchanged between the parties or otherwise effective for the purpose of confirming or evidencing those Transactions. This 2002 Master Agreement and the Schedule are together referred to as this "Master Agreement".

Accordingly, the parties agree as follows:—

1. Interpretation

(a) ***Definitions.*** The terms defined in Section 14 and elsewhere in this Master Agreement will have the meanings therein specified for the purpose of this Master Agreement.

(b) ***Inconsistency.*** In the event of any inconsistency between the provisions of the Schedule and the other provisions of this Master Agreement, the Schedule will prevail. In the event of any inconsistency between the provisions of any Confirmation and this Master Agreement, such Confirmation will prevail for the purpose of the relevant Transaction.

(c) ***Single Agreement.*** All Transactions are entered into in reliance on the fact that this Master Agreement and all Confirmations form a single agreement between the parties (collectively referred to as this "Agreement"), and the parties would not otherwise enter into any Transactions.

2. Obligations

(a) ***General Conditions.***

(i) Each party will make each payment or delivery specified in each Confirmation to be made by it, subject to the other provisions of this Agreement.

(ii) Payments under this Agreement will be made on the due date for value on that date in the place of the account specified in the relevant Confirmation or otherwise pursuant to this Agreement, in freely transferable funds and in the manner customary for payments in the required currency. Where settlement is by delivery (that is, other than by payment), such delivery will be made for receipt on the due date in the manner customary for the relevant obligation unless otherwise specified in the relevant Confirmation or elsewhere in this Agreement.

Source

A Promise in Tradfi

(iii) Each obligation of each party under Section 2(a)(i) is subject to (1) the condition precedent that no Event of Default or Potential Event of Default with respect to the other party has occurred and is continuing, (2) the condition precedent that no Early Termination Date in respect of the relevant Transaction has occurred or been effectively designated and (3) each other condition specified in this Agreement to be a condition precedent for the purpose of this Section 2(a)(iii).

(b) ***Change of Account.*** Either party may change its account for receiving a payment or delivery by giving notice to the other party at least five Local Business Days prior to the Scheduled Settlement Date for the payment or delivery to which such change applies unless such other party gives timely notice of a reasonable objection to such change.

(c) ***Netting of Payments.*** If on any date amounts would otherwise be payable:—

(i) in the same currency; and

(ii) in respect of the same Transaction,

by each party to the other, then, on such date, each party's obligation to make payment of any such amount will be automatically satisfied and discharged and, if the aggregate amount that would otherwise have been payable by one party exceeds the aggregate amount that would otherwise have been payable by the other party, replaced by an obligation upon the party by which the larger aggregate amount would have been payable to pay to the other party the excess of the larger aggregate amount over the smaller aggregate amount.

The parties may elect in respect of two or more Transactions that a net amount and payment obligation will be determined in respect of all amounts payable on the same date in the same currency in respect of those Transactions, regardless of whether such amounts are payable in respect of the same Transaction. The election may be made in the Schedule or any Confirmation by specifying that "Multiple Transaction Payment Netting" applies to the Transactions identified as being subject to the election (in which case clause (ii) above will not apply to such Transactions). If Multiple Transaction Payment Netting is applicable to Transactions, it will apply to those Transactions with effect from the starting date specified in the Schedule or such Confirmation, or, if a starting date is not specified in the Schedule or such Confirmation, the starting date otherwise agreed by the parties in writing. This election may be made separately for different groups of Transactions and will apply separately to each pairing of Offices through which the parties make and receive payments or deliveries.

(d) ***Deduction or Withholding for Tax.***

(i) ***Gross-Up.*** All payments under this Agreement will be made without any deduction or withholding for or on account of any Tax unless such deduction or withholding is required by any applicable law, as modified by the practice of any relevant governmental revenue authority, then in effect. If a party is so required to deduct or withhold, then that party ("X") will:—

(1) promptly notify the other party ("Y") of such requirement;

(2) pay to the relevant authorities the full amount required to be deducted or withheld (including the full amount required to be deducted or withheld from any additional amount paid by X to Y under this Section 2(d)) promptly upon the earlier of determining that such deduction or withholding is required or receiving notice that such amount has been assessed against Y;

(3) promptly forward to Y an official receipt (or a certified copy), or other documentation reasonably acceptable to Y, evidencing such payment to such authorities; and

2 **ISDA® 2002**

Source

A Promise in Tradfi

(iii) upon reasonable demand by such other party, any form or document that may be required or reasonably requested in writing in order to allow such other party or its Credit Support Provider to make a payment under this Agreement or any applicable Credit Support Document without any deduction or withholding for or on account of any Tax or with such deduction or withholding at a reduced rate (so long as the completion, execution or submission of such form or document would not materially prejudice the legal or commercial position of the party in receipt of such demand), with any such form or document to be accurate and completed in a manner reasonably satisfactory to such other party and to be executed and to be delivered with any reasonably required certification,

in each case by the date specified in the Schedule or such Confirmation or, if none is specified, as soon as reasonably practicable.

(b) ***Maintain Authorisations.*** It will use all reasonable efforts to maintain in full force and effect all consents of any governmental or other authority that are required to be obtained by it with respect to this Agreement or any Credit Support Document to which it is a party and will use all reasonable efforts to obtain any that may become necessary in the future.

(c) ***Comply With Laws.*** It will comply in all material respects with all applicable laws and orders to which it may be subject if failure so to comply would materially impair its ability to perform its obligations under this Agreement or any Credit Support Document to which it is a party.

(d) ***Tax Agreement.*** It will give notice of any failure of a representation made by it under Section 3(f) to be accurate and true promptly upon learning of such failure.

(e) ***Payment of Stamp Tax.*** Subject to Section 11, it will pay any Stamp Tax levied or imposed upon it or in respect of its execution or performance of this Agreement by a jurisdiction in which it is incorporated, organised, managed and controlled or considered to have its seat, or where an Office through which it is acting for the purpose of this Agreement is located ("Stamp Tax Jurisdiction"), and will indemnify the other party against any Stamp Tax levied or imposed upon the other party or in respect of the other party's execution or performance of this Agreement by any such Stamp Tax Jurisdiction which is not also a Stamp Tax Jurisdiction with respect to the other party.

5. Events of Default and Termination Events

(a) ***Events of Default.*** The occurrence at any time with respect to a party or, if applicable, any Credit Support Provider of such party or any Specified Entity of such party of any of the following events constitutes (subject to Sections 5(c) and 6(e)(iv)) an event of default (an "Event of Default") with respect to such party:—

(i) ***Failure to Pay or Deliver.*** Failure by the party to make, when due, any payment under this Agreement or delivery under Section 2(a)(i) or 9(h)(i)(2) or (4) required to be made by it if such failure is not remedied on or before the first Local Business Day in the case of any such payment or the first Local Delivery Day in the case of any such delivery after, in each case, notice of such failure is given to the party;

(ii) ***Breach of Agreement; Repudiation of Agreement.***

(1) Failure by the party to comply with or perform any agreement or obligation (other than an obligation to make any payment under this Agreement or delivery under Section 2(a)(i) or 9(h)(i)(2) or (4) or to give notice of a Termination Event or any agreement or obligation under Section 4(a)(i), 4(a)(iii) or 4(d)) to be complied with or performed by the party in accordance with this Agreement if such failure is not remedied within 30 days after notice of such failure is given to the party; or

(2) the party disaffirms, disclaims, repudiates or rejects, in whole or in part, or challenges the validity of, this Master Agreement, any Confirmation executed and delivered by that party or any

5 **ISDA® 2002**

Source

A Promise in Tradfi

21 / 36 92%

14. Definitions

As used in this Agreement:—

"Additional Representation" has the meaning specified in Section 3.

"Additional Termination Event" has the meaning specified in Section 5(b).

"Affected Party" has the meaning specified in Section 5(b).

"Affected Transactions" means (a) with respect to any Termination Event consisting of an Illegality, Force Majeure Event, Tax Event or Tax Event Upon Merger, all Transactions affected by the occurrence of such Termination Event (which, in the case of an Illegality under Section 5(b)(i)(2) or a Force Majeure Event under Section 5(b)(ii)(2), means all Transactions unless the relevant Credit Support Document references only certain Transactions, in which case those Transactions and, if the relevant Credit Support Document constitutes a Confirmation for a Transaction, that Transaction) and (b) with respect to any other Termination Event, all Transactions.

"Affiliate" means, subject to the Schedule, in relation to any person, any entity controlled, directly or indirectly, by the person, any entity that controls, directly or indirectly, the person or any entity directly or indirectly under common control with the person. For this purpose, "control" of any entity or person means ownership of a majority of the voting power of the entity or person.

"Agreement" has the meaning specified in Section 1(c).

"Applicable Close-out Rate" means:—

(a) in respect of the determination of an Unpaid Amount:—

(i) in respect of obligations payable or deliverable (or which would have been but for Section 2(a)(iii)) by a Defaulting Party, the Default Rate;

(ii) in respect of obligations payable or deliverable (or which would have been but for Section 2(a)(iii)) by a Non-defaulting Party, the Non-default Rate;

(iii) in respect of obligations deferred pursuant to Section 5(d), if there is no Defaulting Party and for so long as the deferral period continues, the Applicable Deferral Rate; and

(iv) in all other cases following the occurrence of a Termination Event (except where interest accrues pursuant to clause (iii) above), the Applicable Deferral Rate; and

(b) in respect of an Early Termination Amount:—

(i) for the period from (and including) the relevant Early Termination Date to (but excluding) the date (determined in accordance with Section 6(d)(ii)) on which that amount is payable:—

(1) if the Early Termination Amount is payable by a Defaulting Party, the Default Rate;

(2) if the Early Termination Amount is payable by a Non-defaulting Party, the Non-default Rate; and

(3) in all other cases, the Applicable Deferral Rate; and

A Promise in Tradfi

(b) ***"Specified Transaction"*** [will have the meaning specified in Section 14 of this Agreement.][means .....
.....
.....]*

(c) The ***"Cross-Default"*** provisions of Section 5(a)(vi) [will][will not]* apply to Party A
[will][will not]* apply to Party B

[***"Specified Indebtedness"*** [will have the meaning specified in Section 14 of this Agreement.][means .....
.....]*

"Threshold Amount" means .....
.....]**

(d) The ***"Credit Event Upon Merger"*** provisions of Section 5(b)(v) [will][will not]* apply to Party A
[will][will not]* apply to Party B

(e) The ***"Automatic Early Termination"*** provision of Section 6(a) [will][will not]* apply to Party A
[will][will not]* apply to Party B

(f) ***"Termination Currency"*** [will have the meaning specified in Section 14 of this Agreement.][means .....
.....]*

(g) ***Additional Termination Event*** [will][will not]* apply. [The following will constitute an Additional Termination Event:— .....
.....
.....
.....
.....

For the purpose of the foregoing Termination Event, the Affected Party or Affected Parties will be:— .....
.....]***

Part 2. **Tax Representations.****

(a) ***Payer Representations.*** For the purpose of Section 3(e) of this Agreement[, Party A and Party B do not make any representations.][:—

[[(i)] [Party A] [and] [Party B] [each] make[s] the following representation:—

It is not required by any applicable law, as modified by the practice of any relevant governmental revenue authority, of any Relevant Jurisdiction to make any deduction or withholding for or on account of any Tax from any payment (other than interest under Section 9(h) of this Agreement) to

* Delete as applicable.
** Include if Cross-Default will apply to either Party A or Party B.
*** Include if Additional Termination Event will apply.
**** N.B.: the following representations may need modification if either party is a Multibranch Party.

30 ISDA® 2002

Source

Rents

PAYMENT NETWORK	AVERAGE CREDIT CARD PROCESSING FEES
Visa	1.29% + $0.05 to 3.29% + $0.10
Mastercard	1.39% + $0.05 to 3.29% + $0.10
Discover	1.58% + $0.05 to 3.28% + $0.10
American Express	1.5% + $0.10 to 3.15% + $0.10

Sources: Visa USA Interchange Reimbursement Fees published on April 23, 2022, Mastercard 2022–2023 U.S. Region Interchange Programs and Rates, Wells Fargo Merchant Services Payment Network Pass-Through Fee Schedule, and Wells Fargo Payment Network Qualification Matrix effective April 22, 2022.

Source

In Economics, a **rent** is any recurring payment earned in excess of the cost to provide it. Persistent rents are evidence of **barriers to entry** or other impediments to perfect competition.

Finance in the USA

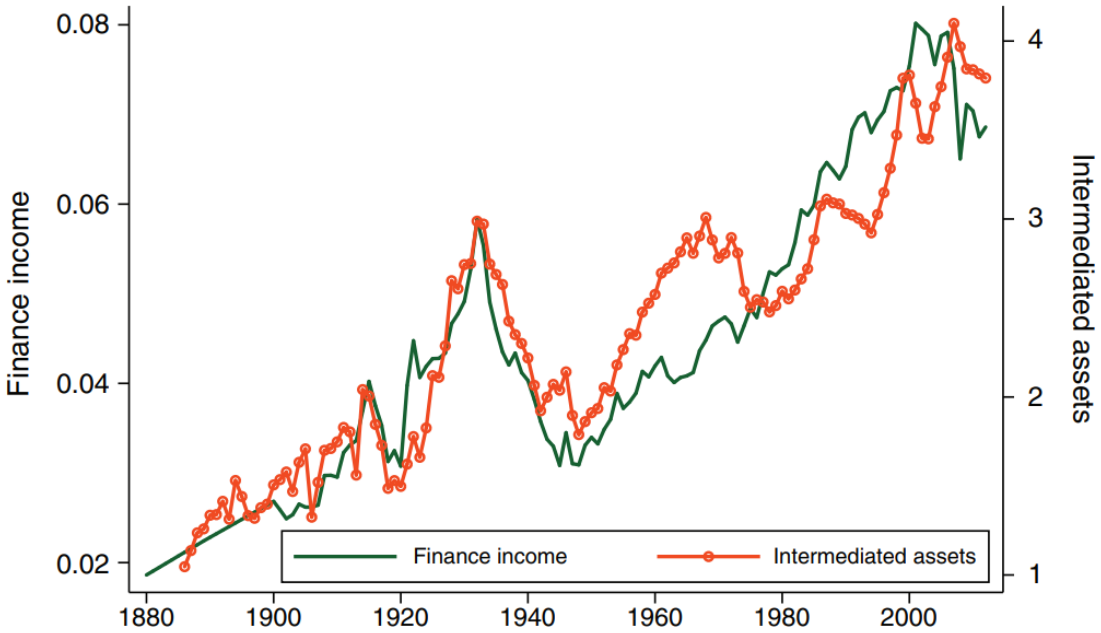


FIGURE 2. FINANCE INCOME AND INTERMEDIATED ASSETS OVER GDP

Notes: Both series are expressed as a share of GDP, excluding defense spending. Finance income is the domestic income of the finance and insurance industries, i.e., aggregate income minus net exports. It is available from 1880 to 2012. Intermediated assets include debt and equity issued by nonfinancial firms, household debt, and various assets providing liquidity services. Data range for intermediated assets is 1886–2012.

(Philippon (2015).) Are we getting 4x better value per GDP from the financial services industry than in 1880?

Will innovations like Venmo fix this?

venmo

We're reaching out to let you know that as of July 1, 2024, transaction fees for receiving payments tagged by the sender as a goods and services purchase will change to 2.99% per transaction.

This change won't affect fees for receiving payments into business or charity profiles, which remain at 1.9% + $0.10 for Venmo-to-Venmo transactions. **View our fees.** Eligible goods and services payments are covered by **Venmo** **Purchase Protection.**

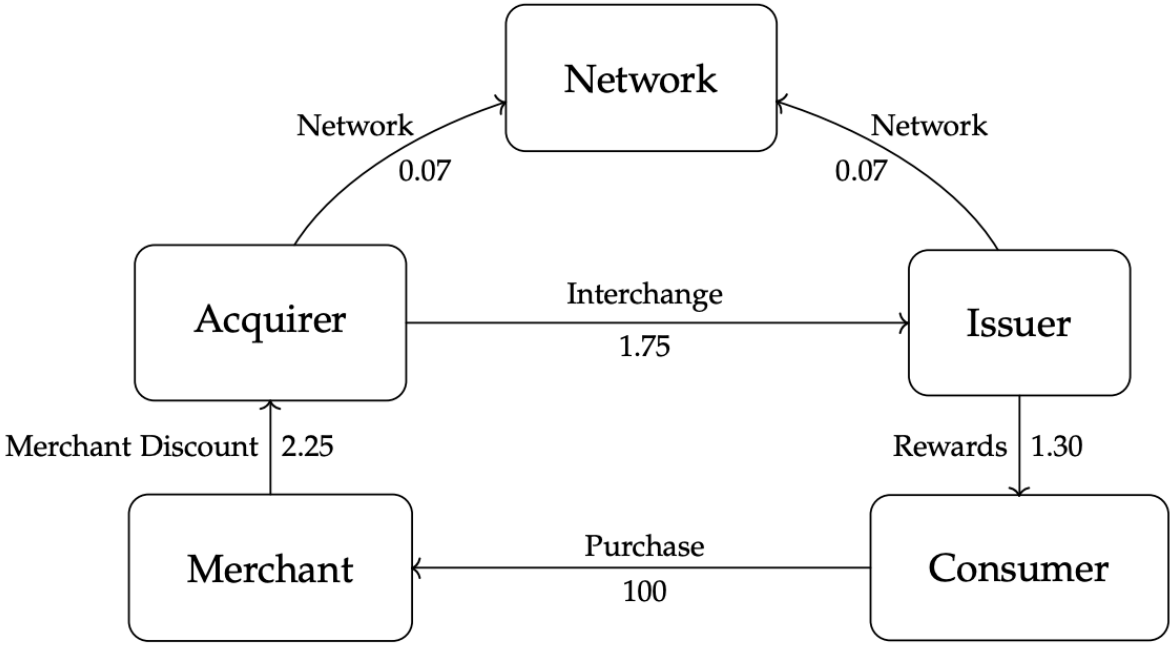
If you have questions, **get in touch with us.**

Thank you for choosing Venmo.

Source

Will Venmo fix this?

Figure 1: Illustration of payment flows in a payment network.



Will Venmo fix this?

"This paper compares the relative merits of regulating prices versus increasing competition in U.S. payment markets ... merchants in the U.S. typically charge consumers the same price for different payment methods ... **Price coherence** incentivizes networks to charge high merchant fees to fund consumer rewards ... High credit card rewards inflate retail prices for all consumers while encouraging excessive credit card use ... There are large gains from either capping credit card merchant fees or uncapping debit card merchant fees, whereas encouraging competition is harmful [because it will re-create the forces that caused over-use of credit cards]."

Wang (2024) says No (do we agree?)

Justice?

INSIDER

Newsletters Hello, Anthony Lee!

HOME > NEWS

Canada says it will freeze the bank accounts of 'Freedom Convoy' truckers who continue their anti-vaccine mandate blockades

Matthew Loh Feb 14, 2022, 9:33 PM

Deputy Prime Minister Chrystia Freeland said banks are obligated to flag, freeze, or suspend accounts financing the "illegal blockades." Blair Gable/REUTERS

- Canada says it will freeze the bank accounts of truckers who continue to form "Freedom Convoys."
- On Monday, Prime Minister Justin Trudeau declared a national emergency to combat the protests.
- Canadian truckers have been protesting vaccine mandates for weeks by blocking streets and bridges.

Source 1 and source 2

Justice?

Prohibited Activities

You may not use the PayPal service for activities that:

1. violate any law, statute, ordinance or regulation.
2. relate to transactions involving (a) narcotics, steroids, certain controlled substances or other products that present a risk to consumer safety, (b) drug paraphernalia, (c) cigarettes, (d) items that encourage, promote, facilitate or instruct others to engage in illegal activity, (e) stolen goods including digital and virtual goods, (f) the promotion of hate, violence, racial or other forms of intolerance that is discriminatory or the financial exploitation of a crime, (g) items that are considered obscene, (h) items that infringe or violate any copyright, trademark, right of publicity or privacy or any other proprietary right under the laws of any jurisdiction, (i) certain sexually oriented materials or services, (j) ammunition, firearms, or certain firearm parts or accessories, or (k) certain weapons or knives regulated under applicable law.
3. relate to transactions that (a) show the personal information of third parties in violation of applicable law, (b) support pyramid or ponzi schemes, matrix programs, other "get rich quick" schemes or certain multi-level marketing programs, (c) are associated with purchases of annuities or lottery contracts, lay-away systems, off-shore banking or transactions to finance or refinance debts funded by a credit card, (d) are for the sale of certain items before the seller has control or possession of the item, (e) are by payment processors to collect payments on behalf of merchants, (f) are associated with the sale of traveler's checks or money orders, (g) involve currency exchanges or check cashing businesses, (h) involve certain credit repair, debt settlement services, credit transactions or insurance activities, or (i) involve offering or receiving payments for the purpose of bribery or corruption.
4. involve the sales of products or services identified by government agencies to have a high likelihood of being fraudulent.
5. involve the sending, posting, or publication of any messages, content, or materials that, in PayPal's sole discretion, (a) are harmful, obscene, harassing, or objectionable, (b) depict or appear to depict nudity, sexual or other intimate activities, (c) depict or promote illegal drug use, (d) depict or promote violence, criminal activity, cruelty, or self-harm (e) depict, promote, or incite hatred or discrimination of protected groups or of individuals or groups based on protected characteristics (e.g. race, religion, gender or gender identity, sexual orientation, etc.) (f) present a risk to user safety or wellbeing, (g) are fraudulent, promote misinformation, or are unlawful, (h) infringe the privacy, intellectual property rights, or other proprietary rights of any party, or (i) are otherwise unfit for publication.
6. relate to transactions involving any activity that requires pre-approval without having obtained said approval.

Source 1 and source 2

Access

Tiniest bit of personal opinion

I am in favor of discouraging offensive wars, but know the financial system to be a very blunt instrument for expressing society's preferences. In particular, while the global financial system and the governments giving them instructions have not actually banned the usage of oligarchs' wealth prior to now, they have already given many ordinary Russians (and *ordinary Ukranians*!) severe difficulties doing things we expect to be utterly routine for law-abiding members of society.

Without divulging any professional confidences, in the wake of the 2014 invasion of the Crimean Peninsula many U.S. banks decided to stop serving customers with Ukrainian passports. No one explicitly made the decision "Your nation got invaded, so you should have less access to financial systems *half a world away*. This is a natural and just outcome in a democratic society."

It flowed indirectly through "The Crimea now poses a heightened risk of money laundering", "We lack the ability to discriminate between the Crimea and the rest of Ukraine", "We care a lot more about not facilitating money laundering than we do about our infinitesimal Ukraine business so Ukraine is going on the High Risk Country list", "Sorry, you have citizenship from the High Risk Country list, accordingly I'm not allowed to open this account for you. This is a commercial decision of the bank and will not be reversed."

Source: Bits About Money on international transfers

Other Issues with Tradfi

- High entry costs, low competition
- Out-dated infrastructure, lack of composability
- Crashes, fragility, systemic risk
- Opacity, politicization

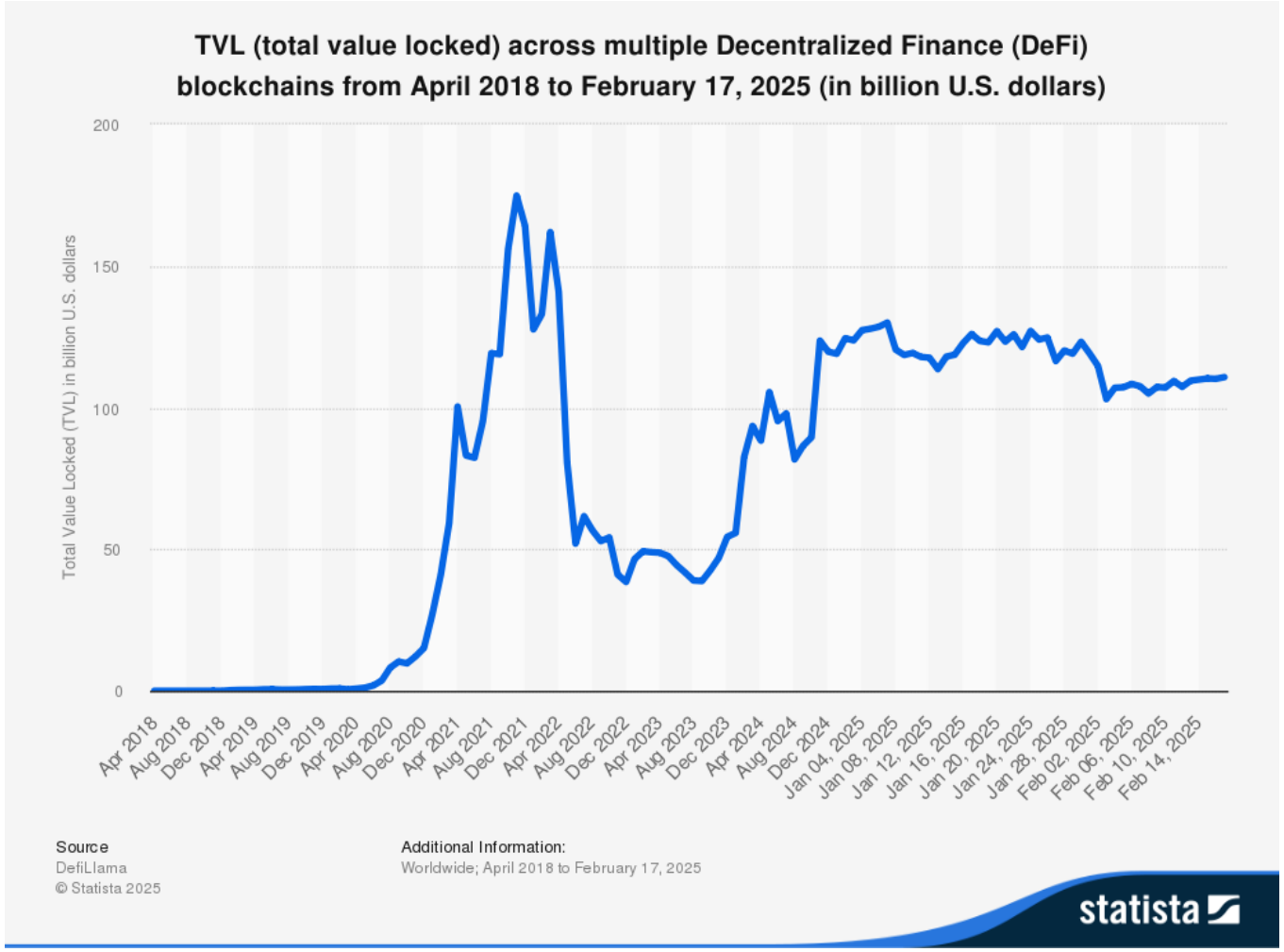
Roadmap

1. Pain Points of TradFi
2. Promise of DeFi
3. Lending Protocols
4. Derivatives

Decentralized Finance: The Vision

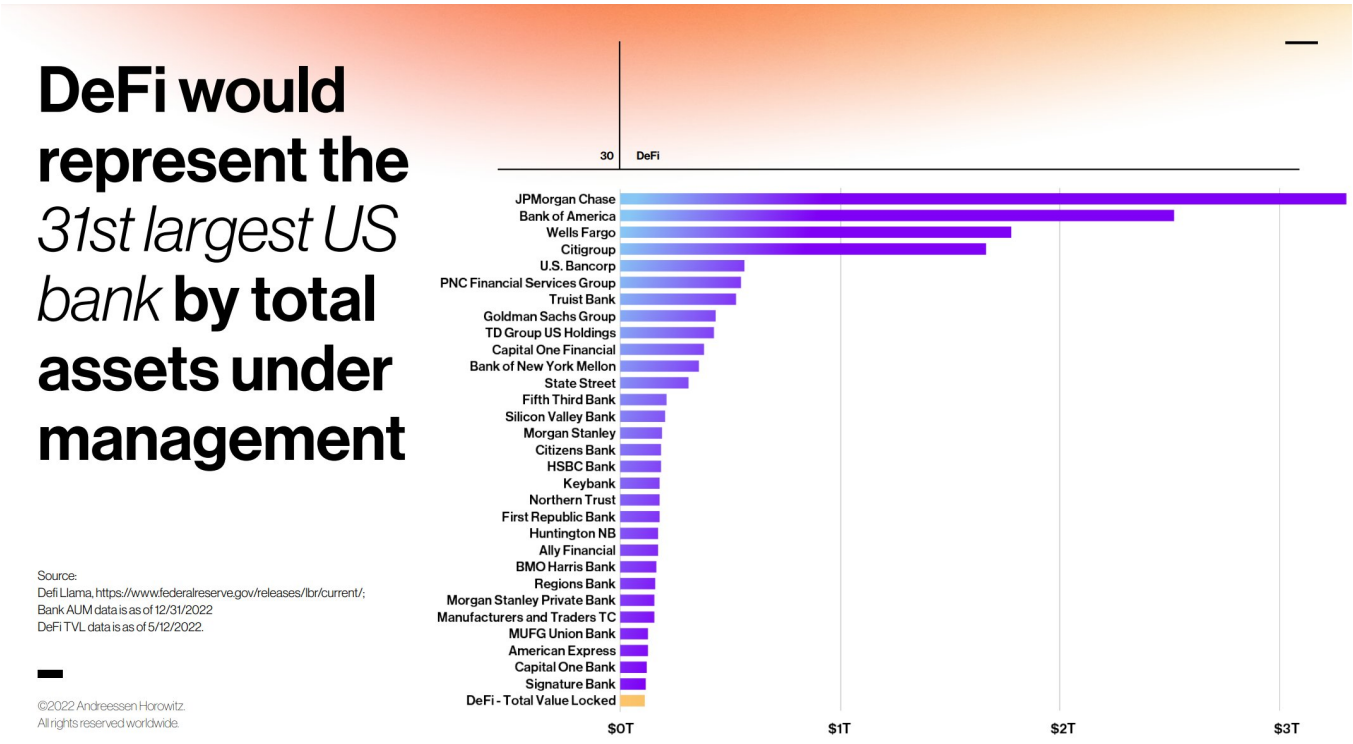
- Simple,
- Low-cost and competitive,
- Just and non-discretionary,
- Accessible,
- Always at the technological frontier,
- Transparent, and
- Trustlessly safe by design

DeFi has leveled off at $\sim \$100B$



Source

But remains small compared to TradFi...



Source

Defi Contracts...

Product Solutions Open Source Pricing Search

Uniswap Labs

Web3 infrastructure and products

1.2k followers · Ethereum · https://uniswap.org · @Uniswap · support@uniswap.org · Verified

Overview | Repositories 72 | Projects 2 | Packages | People 14

Pinned

v3-core Public
Core smart contracts of Uniswap v3
TypeScript 3k 1.5k

v3-periphery Public
Peripheral smart contracts for interacting with Uniswap v3
TypeScript 813 625

interface Public
An open source interface for the Uniswap protocol
TypeScript 3.7k 3.5k

v3-sdk Public
An SDK for building applications on top of Uniswap V3
TypeScript 400 268

v2-core Public
Core smart contracts of Uniswap V2
TypeScript 2.1k 2.3k

v2-periphery Public
Peripheral smart contracts for interacting with Uniswap V2
Solidity 832 1.3k

Source

Defi Contracts...

Product Solutions Open Source Pricing Search

Uniswap / v3-core Public

Code | Issues 16 | Pull requests 1 | Actions | Security | Insights

main | 3 branches | 13 tags | Go to file | Code

marktoda and lint-action feat: add stale config (#571) ... 412d9b2 on Jul 13 1,002 commits

.github	feat: add stale config (#571)	3 months ago
audits	add tob audit	2 years ago
contracts	Dual license under GPL or BUSL (#557)	5 months ago
test	change how we get wallets for testing against external nodes	16 months ago
.gitattributes	add prettier	3 years ago
.gitignore	big test infra upgrade (hardhat + typechain)	2 years ago
.prettierrc	add prettier	3 years ago
.solhint.json	prettier + solhint	2 years ago
.yarnrc	ignore scripts	2 years ago
LICENSE	add LICENSE and make associated changes (#433)	2 years ago
README.md	Dual license under GPL or BUSL (#557)	5 months ago
bug-bounty.md	add tob audit	2 years ago
echidna.config.yml	more robust price math testing + add incomplete pair echidna test (#98)	2 years ago

Source

Defi Contracts...

98 lines (91 sloc) | 4.52 KB

Raw | Blame

```
// SPDX-License-Identifier: BUSL-1.1
pragma solidity >=0.5.0;

import './FullMath.sol';
import './SqrtPriceMath.sol';

/// @title Computes the result of a swap within ticks
/// @notice Contains methods for computing the result of a swap within a single tick price range, i.e., a single tick.
library SwapMath {
    /// @notice Computes the result of swapping some amount in, or amount out, given the parameters of the swap
    /// @dev The fee, plus the amount in, will never exceed the amount remaining if the swap's `amountSpecified` is positive
    /// @param sqrtRatioCurrentX96 The current sqrt price of the pool
    /// @param sqrtRatioTargetX96 The price that cannot be exceeded, from which the direction of the swap is inferred
    /// @param liquidity The usable liquidity
    /// @param amountRemaining How much input or output amount is remaining to be swapped in/out
    /// @param feePips The fee taken from the input amount, expressed in hundredths of a bip
    /// @return sqrtRatioNextX96 The price after swapping the amount in/out, not to exceed the price target
    /// @return amountIn The amount to be swapped in, of either token0 or token1, based on the direction of the swap
    /// @return amountOut The amount to be received, of either token0 or token1, based on the direction of the swap
    /// @return feeAmount The amount of input that will be taken as a fee
    function computeSwapStep(
        uint160 sqrtRatioCurrentX96,
        uint160 sqrtRatioTargetX96,
        uint128 liquidity,
        int256 amountRemaining,
        uint24 feePips
    )
        internal
        pure
        returns (
            uint160 sqrtRatioNextX96,
            uint256 amountIn,
            uint256 amountOut,
            uint256 feeAmount
        )
    {
        bool zeroForOne = sqrtRatioCurrentX96 >= sqrtRatioTargetX96;
        bool exactIn = amountRemaining >= 0;

        if (exactIn) {
            uint256 amountRemainingLessFee = FullMath.mulDiv(uint256(amountRemaining), 1e6 - feePips, 1e6);
            amountIn = zeroForOne
                ? SqrtPriceMath.getAmount0Delta(sqrtRatioTargetX96, sqrtRatioCurrentX96, liquidity, true)
                : SqrtPriceMath.getAmount1Delta(sqrtRatioCurrentX96, sqrtRatioTargetX96, liquidity, true);
            if (amountRemainingLessFee >= amountIn) sqrtRatioNextX96 = sqrtRatioTargetX96;
            else
                sqrtRatioNextX96 = SqrtPriceMath.getNextSqrtPriceFromInput(
                    sqrtRatioCurrentX96,
                    liquidity,
                    amountRemainingLessFee,
                    zeroForOne
                );
        } else {
            amountOut = zeroForOne
                ? SqrtPriceMath.getAmount1Delta(sqrtRatioTargetX96, sqrtRatioCurrentX96, liquidity, false)
                : SqrtPriceMath.getAmount0Delta(sqrtRatioCurrentX96, sqrtRatioTargetX96, liquidity, false);
            if (uint256(-amountRemaining) >= amountOut) sqrtRatioNextX96 = sqrtRatioTargetX96;
            else
                sqrtRatioNextX96 = SqrtPriceMath.getNextSqrtPriceFromOutput(
                    sqrtRatioCurrentX96,
                    liquidity,
```

Source

Critical questions for DeFi

- What is the classic finance question being solved?
- How does the structure of blockchain tech influence the answer?

Critical questions for DeFi

- What is the classic finance question being solved?
- How does the structure of blockchain tech influence the answer?
- What weaknesses of tradfi do these applications address and improve on?
- What new weaknesses are introduced?

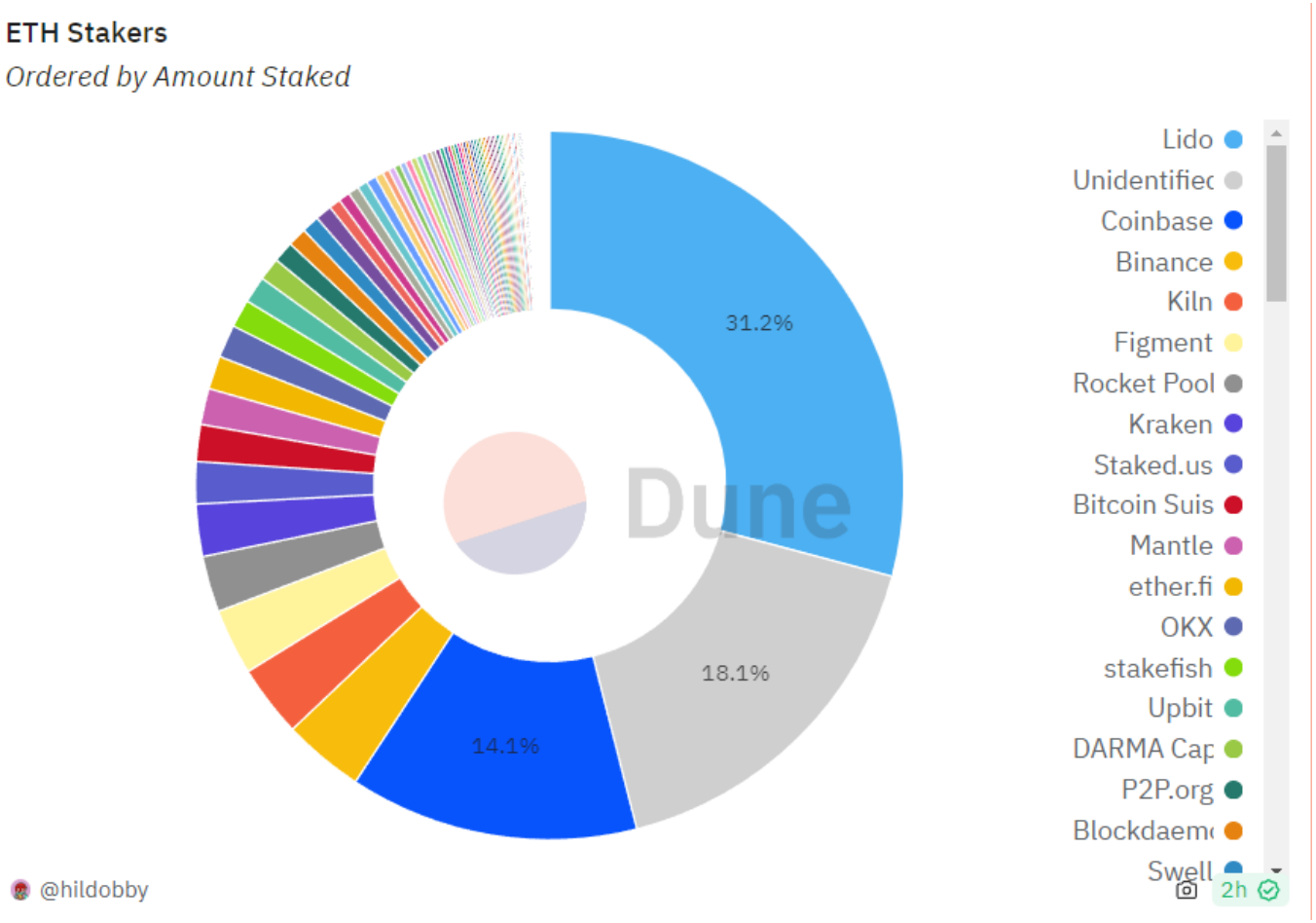
Critical questions for DeFi

- What is the classic finance question being solved?
- How does the structure of blockchain tech influence the answer?
- What weaknesses of tradfi do these applications address and improve on?
- What new weaknesses are introduced?
- What kinds of **promises** that couldn't be made, now can be made, thanks to blockchain technology?

Proof of Stake

- Originally, ETH mining proof-of-work, similar to BTC
- On Sept 15 2022, ETH switched to proof of stake – called **"The Merge"**
- Reduced energy consumption by **over 99%**!
- Users deposit ("stake") 32 ETH into a special smart contract
- Stakers randomly selected (prop. to stake) to propose new blocks
- If a staker is caught trying to do "bad things" (e.g. propose 2 inconsistent blocks), they are "slashed": staked ETH is removed by smart contract
- Most newer blockchains (SOL, LUNA, AVAX) use proof-of-stake

Staking is Very Concentrated!



Source: Dune. Lido is itself a decentralized protocol.

Staking is Very Concentrated!

ETH Stakers

Ordered by Amount Staked

#	Entity	Category	ETH Staked	Validators	Marketshare	1WΔ
1	Lido	Liquid Staking	9,818,140	307k	31.2%	0%
2	Coinbase	CEXs	4,433,345	139k	14.1%	1%
3	Binance	CEXs	1,219,360	38k	3.9%	-9%
4	Kiln	Staking Pools	1,081,056	34k	3.4%	3%
5	Figment	Staking Pools	992,096	31k	3.1%	1%
6	Rocket Pool	Liquid Staking	838,007	26k	2.7%	-1%
7	Kraken	CEXs	779,009	24k	2.5%	0%
8	Staked.us	Staking Pools	620,668	19k	2.0%	5%
9	Bitcoin Suisse	CEXs	540,438	17k	1.7%	0%

Source: Dune. Lido is itself a decentralized protocol.

ETH L2s

ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled

ETH L2s

ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled
- Need to guarantee whatever happens on "rollup" is exactly what would happen on ETH main chain! Two methods:
  - **Optimistic rollup** (Optimism, Arbitrum, Coinbase Base): Can "challenge" L2 transactions, will (essentially) run on L1 if challenged
  - **ZK-rollup** (zkSync, StarkWare, Polygon): "Zero-Knowledge" (ZK) proofs of valid transactions are periodically added to the main chain in batches. More expensive than Optimistic, but fully trustless.
  - Currently, Optimistic is more popular

ETH L2s

ETH is getting expensive! One set of solutions is rollups (also called L2's). Idea:

- Put our ETH, tokens, etc. in a "smart contract pot" (L2 bridge)
- People do transactions (smart contract, etc.) using funds in the pot, without doing anything on "main chain"
- Transactions are periodically batch settled
- Need to guarantee whatever happens on "rollup" is exactly what would happen on ETH main chain! Two methods:
  - **Optimistic rollup** (Optimism, Arbitrum, Coinbase Base): Can "challenge" L2 transactions, will (essentially) run on L1 if challenged
  - **ZK-rollup** (zkSync, StarkWare, Polygon): "Zero-Knowledge" (ZK) proofs of valid transactions are periodically added to the main chain in batches. More expensive than Optimistic, but fully trustless.
  - Currently, Optimistic is more popular

ETH L2s

Source: L2beat

ETH L2s

Show rollups only | Select type | Select stack | Select stage | Select purpose

Active projects 42 | Upcoming projects 36 | Archived projects 11 | Layer 3 projects 4

#	NAME	RISKS	TYPE	STAGE	PURPOSE	TOTAL	MKT SHARE
1	Arbitrum One		Optimistic Rollup	STAGE 1	Universal	$13.80B ▲ 9.24%	45.42%
2	OP Mainnet		Optimistic Rollup OP	STAGE 0	Universal	$7.80B ▲ 5.67%	25.66%
3	Manta Pacific		Optimium OP	n/a	Universal	$1.87B ▼ 1.29%	6.16%
4	Starknet		ZK Rollup	STAGE 0	Universal	$1.26B ▼ 4.81%	4.15%
5	Base		Optimistic Rollup OP	STAGE 0	Universal	$996M ▲ 18.03%	3.28%
6	Metis		Optimium OVM	n/a	Universal	$879M ▲ 22.70%	2.89%
7	zkSync Era		ZK Rollup	STAGE 0	Universal	$803M ▲ 22.17%	2.64%
8	Mantle		Optimium OVM	n/a	Universal	$763M ▲ 13.89%	2.51%
9	dYdX v3		ZK Rollup	STAGE 1	Exchange	$339M ▲ 13.86%	1.12%
10	Linea		ZK Rollup	STAGE 0	Universal	$322M ▲ 29.24%	1.06%

Source: L2beat

Optimistic Rollup with Arbitrum

Ethereum is awesome, but it has its limitations. The Ethereum Blockchain can handle only about 20 to 40 transactions per second (TPS) for all users. Once it reaches this limit, users must compete for space to have their transactions included, increasing fees.

Arbitrum Rollup solves this issue! Here's how it works: an Arbitrum Rollup Chain acts as a submodule within Ethereum. Unlike regular Ethereum transactions, we don't need Ethereum nodes to handle every Arbitrum transaction. Instead, Ethereum takes an **"innocent until proven guilty"** stance with Arbitrum. Initially, the Parent chain assumes that actions on Arbitrum follow the rules. If there is a rule violation (like someone claiming, "Now I have all of your money"), that claim is challengeable on the parent chain. In this case, we can prove fraud, disregard the invalid claim, and penalize the guilty party. This ability to investigate and confirm fraud on the parent chain is Arbitrum's main feature and explains why it benefits from Ethereum's security.

Analogy to Paper Checks

Has anyone ever paid with a paper check at the grocery store?

Analogy to Paper Checks

Has anyone ever paid with a paper check at the grocery store?
This used to be common!
Your check would be assumed good until proven otherwise.

Analogy to Paper Checks

Has anyone ever paid with a paper check at the grocery store?
This used to be common!
Your check would be assumed good until proven otherwise.
Knowingly writing bad checks is a **felony**!

Analogy to Paper Checks

Has anyone ever paid with a paper check at the grocery store?
This used to be common!
Your check would be assumed good until proven otherwise.
Knowingly writing bad checks is a **felony**!

Arbitrum works similarly: you are given the benefit of the doubt, but punished severely for betraying the trust offered you by the system.

Welcome! Today is Wednesday, October 1st!

Office Hours this week will be by appointment over Zoom.
Contrary to what I said verbally on Monday, the Midterm is in fact **October 15**, not Oct 13.

Mango Markets vs. FTX

Q: Why did Mango Markets fail?

Mango Markets vs. FTX

Q: Why did Mango Markets fail?
A: Avraham Eisenberg manipulated the perceived price of his collateral in order to take out and default on large loans.

Mango Markets vs. FTX

Q: Why did Mango Markets fail?
A: Avraham Eisenberg manipulated the perceived price of his collateral in order to take out and default on large loans.
Q: Why did FTX fail?

Mango Markets vs. FTX

Q: Why did Mango Markets fail?
A: Avraham Eisenberg manipulated the perceived price of his collateral in order to take out and default on large loans.
Q: Why did FTX fail?
A: FTX used its customers' funds in a totally different way than they claimed. They were able to hide it because FTX did <u>not</u> use transparent smart contracts.

Weakness of DeFi: Miner Extractable Value

To have your (valid) transaction accepted onto the chain, you must bribe a miner (/staker) to include it in their block.

Since each block can only contain a limited number of transactions, block producers have full autonomy in selecting which pending transactions in the mempool—the location block producers store unconfirmed transactions off-chain—they will include in their block. While block producers by default order transactions by the highest gas price (transaction fee) in order to maximize their profits, this is not a requirement by the network. As a result, block producers can extract additional value by taking advantage of their ability to arbitrarily reorder transactions, creating what is known as maximal-extractable value (MEV).

Transactions can be "sniped"! If I see you submit a transaction and know it's guaranteed to net $1, I can bribe miners up to $1 to copy your trade and execute it before you!

Miner Extractable Value and Slippage

The Blockchain is a highly adversarial environment.

- See Dan Robinson, Georgios Konstantopoulos, Ethereum is a "Dark Forest"
- See Flash Boys 2.0
- Transaction ordering matters! Miners have power over this
- Flashbots quite dominant player in this space protocol-wise
- Many very profitable "MEV funds", like crypto HFTs.
- MEV tracks demand for **immediacy**

Miner Extractable Value and Slippage

The Blockchain is a highly adversarial environment.

- See Dan Robinson, Georgios Konstantopoulos, Ethereum is a "Dark Forest"
- See Flash Boys 2.0
- Transaction ordering matters! Miners have power over this
- Flashbots quite dominant player in this space protocol-wise
- Many very profitable "MEV funds", like crypto HFTs.
- MEV tracks demand for **immediacy**
- It is called **slippage** when your order is filled at a worse price than what was quoted

See here

Avoiding Slippage

To avoid front-runners and slippage, you can

- Use a protocol that supports setting a *slippage tolerance*: your order is canceled if the price change exceeds your tolerance setting
- Paying a higher gas fee to prioritize your transaction
- Route your orders through an alternative L2 that polices front-runners
- Use a protocol like Arbitrum TimeBoost

Roadmap

1. Pain Points of TradFi
2. Promise of DeFi
3. Lending Protocols
4. Derivatives

Collateralized lending

Collateralized lending in tradfi:

- Houses $\implies$ mortgages
- Cars $\implies$ auto loans
- Stocks $\implies$ margin loans
- Firms $\implies$ equipment, real estate, etc. collateralized loans
- Bonds $\implies$ repo loans

Collateralized Debt in Tradfi

- I want to buy a house for $400k, but don't have all the $$
- I tell a bank: "lend me $200k; I'll pay you back $250k; if I don't, you get the house"
- Key is, the bank only needs to believe that the house is worth over $250k
- Collateral provides safety to lenders, making them willing to lend me more

Collateralized Debt in Tradfi

- I want to buy a house for $400k, but don't have all the $$
- I tell a bank: "lend me $200k; I'll pay you back $250k; if I don't, you get the house"
- Key is, the bank only needs to believe that the house is worth over $250k
- Collateral provides safety to lenders, making them willing to lend me more
- IRL, what happens if house price falls below $300k?
  - Safe collateral (e.g. U.S. treasuries) doesn't face this risk!
  - No design is *necessarily* better or worse: someone has to hold the risk, just a question of who is best suited to bear it

Margin Calls

- A much better finance movie than The Big Short

Margin Call: Example

- I put in $10,000 to buy $20,000 of stock with a **maintenance margin** of 30%[1]. The **margin** is (my equity / the total position), so 50% initially. I am in compliance because 50% exceeds 30%.
  - The broker lends me the other $10,000

[1] FINRA minimum is 25%

Margin Call: Example

- I put in $10,000 to buy $20,000 of stock with a **maintenance margin** of 30%[1]. The **margin** is (my equity / the total position), so 50% initially. I am in compliance because 50% exceeds 30%.
  - The broker lends me the other $10,000
- The value of the stock drops to $14,000
- My equity is now $14,000 - $10,000 = $4,000
- My margin is now $4,000/$14,000 = 28%

[1] FINRA minimum is 25%

Margin Call: Example

- I put in $10,000 to buy $20,000 of stock with a **maintenance margin** of 30%[1]. The **margin** is (my equity / the total position), so 50% initially. I am in compliance because 50% exceeds 30%.
  - The broker lends me the other $10,000
- The value of the stock drops to $14,000
- My equity is now $14,000 - $10,000 = $4,000
- My margin is now $4,000/$14,000 = 28%
- My broker makes a **margin call**: I need to deposit $200 to bring my margin back up to the required 30%

[1] FINRA minimum is 25%

Margin Call: Example

- I put in $10,000 to buy $20,000 of stock with a **maintenance margin** of 30%[1]. The **margin** is (my equity / the total position), so 50% initially. I am in compliance because 50% exceeds 30%.
  - The broker lends me the other $10,000
- The value of the stock drops to $14,000
- My equity is now $14,000 - $10,000 = $4,000
- My margin is now $4,000/$14,000 = 28%
- My broker makes a **margin call**: I need to deposit $200 to bring my margin back up to the required 30%
- This happens because the collateral is the stock itself, which has uncertain value
- If I refuse to meet the margin call, the broker liquidates my position: He sells the stock to make himself whole. He pays me back what's left of my equity, locking in my loss.

[1] FINRA minimum is 25%

Defi Collateralized Lending

- Collateralized lending requires:
  1. System for collateral custody
  2. System for evaluating collateral value and "margin calls"
- Defi good at 1., can have a "collateral pot" smart contract
- Defi less good at 2. (See Mango Markets)!

Aave (Finnish for "Ghost")

- Deposit $150 of ETH into Aave
- Aave allows you to borrow up to $\$150 \times (1 - \text{margin})$ of other tokens

Aave (Finnish for "Ghost")

- Deposit $150 of ETH into Aave
- Aave allows you to borrow up to $\$150 \times (1 - \text{margin})$ of other tokens
  - Where do other tokens come from?
  - Others are lending into Aave to borrow other tokens

Aave (Finnish for "Ghost")

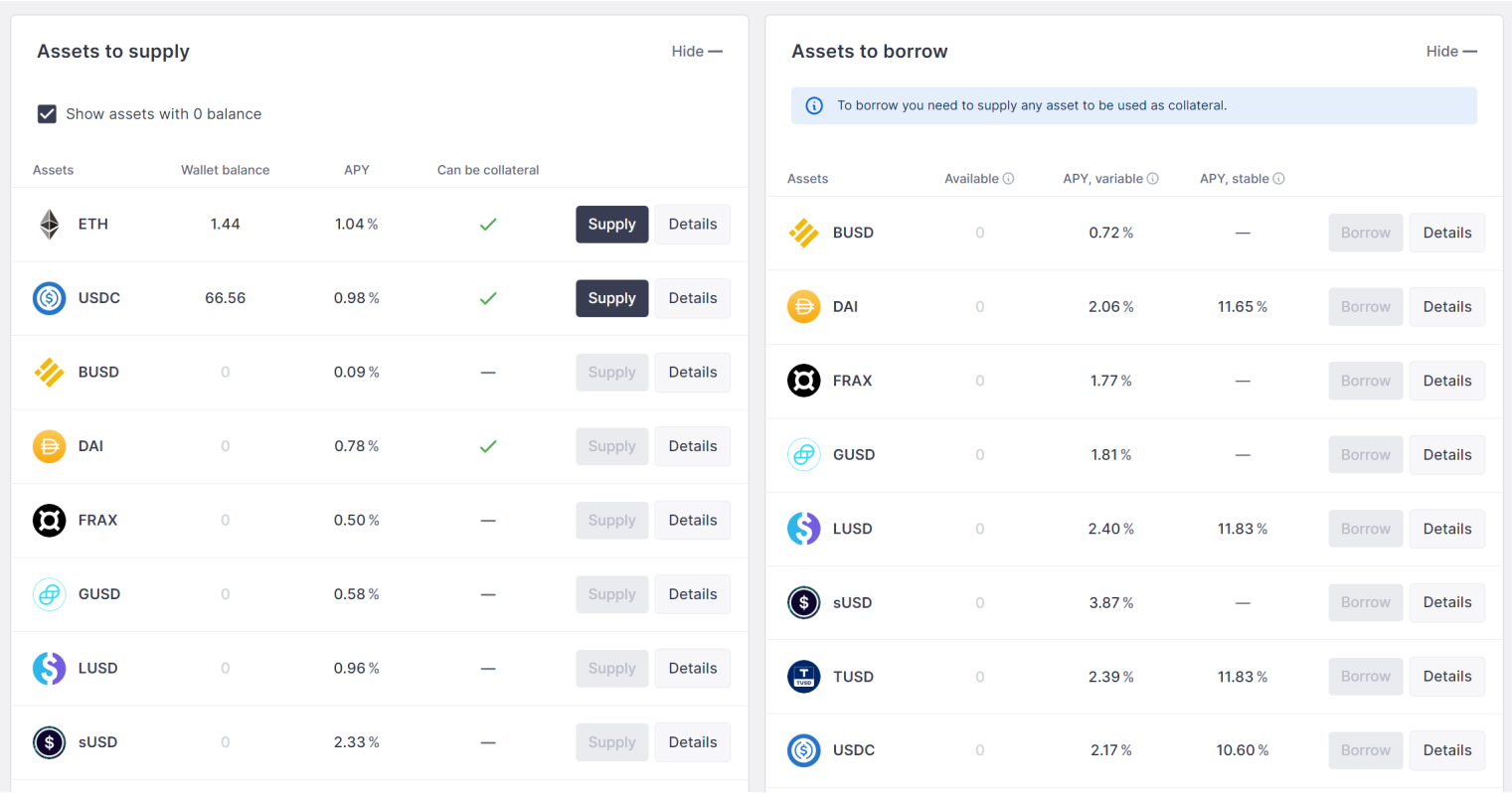
- Deposit $150 of ETH into Aave
- Aave allows you to borrow up to $\$150 \times (1 - \text{margin})$ of other tokens
  - Where do other tokens come from?
  - Others are lending into Aave to borrow other tokens
- If ETH price falls, so collateral worth $100, if loans more than $\$100 \times \gamma$, borrower choices:
  - Add more collateral ("margin call")
  - Reduce leverage (pay back loans)
  - Liquidate collateral

Aave (Finnish for "Ghost")

- Deposit $150 of ETH into Aave
- Aave allows you to borrow up to $\$150 \times (1 - \text{margin})$ of other tokens
  - Where do other tokens come from?
  - Others are lending into Aave to borrow other tokens
- If ETH price falls, so collateral worth $100, if loans more than $\$100 \times \gamma$, borrower choices:
  - Add more collateral ("margin call")
  - Reduce leverage (pay back loans)
  - Liquidate collateral
- With a sufficiently strict smart contract that can liquidate quickly, this protocol should never lose money

Aave Rates

Lenders in Aave play the role of "brokers", earning yield:



Assets to supply Hide —

☑ Show assets with 0 balance

Assets	Wallet balance	APY	Can be collateral		
ETH	1.44	1.04 %	✓	Supply	Details
USDC	66.56	0.98 %	✓	Supply	Details
BUSD	0	0.09 %	—	Supply	Details
DAI	0	0.78 %	✓	Supply	Details
FRAX	0	0.50 %	—	Supply	Details
GUSD	0	0.58 %	—	Supply	Details
LUSD	0	0.96 %	—	Supply	Details
sUSD	0	2.33 %	—	Supply	Details

Assets to borrow Hide —

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

Assets	Available	APY, variable	APY, stable		
BUSD	0	0.72 %	—	Borrow	Details
DAI	0	2.06 %	11.65 %	Borrow	Details
FRAX	0	1.77 %	—	Borrow	Details
GUSD	0	1.81 %	—	Borrow	Details
LUSD	0	2.40 %	11.83 %	Borrow	Details
sUSD	0	3.87 %	—	Borrow	Details
TUSD	0	2.39 %	11.83 %	Borrow	Details
USDC	0	2.17 %	10.60 %	Borrow	Details

Who uses Aave?

Why would you lend to Aave?

- Have many tokens but few opportunities, want returns

Who uses Aave?

Why would you lend to Aave?

- Have many tokens but few opportunities, want returns

Why would you borrow from Aave?

- Have few tokens but many opportunities, want leverage

Who uses Aave?

Why would you lend to Aave?

- Have many tokens but few opportunities, want returns

Why would you borrow from Aave?

- Have few tokens but many opportunities, want leverage
  - Leverage: hold $100 of assets with only $50 of cash
  - Mortgages, margin buying...

Who uses Aave?

Why would you lend to Aave?

- Have many tokens but few opportunities, want returns

Why would you borrow from Aave?

- Have few tokens but many opportunities, want leverage
  - Leverage: hold $100 of assets with only $50 of cash
  - Mortgages, margin buying...
- Need tokens for some utility function
  - Borrow tokens to vote on governance proposals?

Rate Setting on Aave

- Aave interest rates based on utilization:

$$U = \frac{Total\ Borrowed}{Total\ Lent}$$

- Interest rate is higher when U is higher
- When lots of people want to borrow, what happens?

Rate Setting on Aave

- Aave interest rates based on utilization:

$$U = \frac{Total\ Borrowed}{Total\ Lent}$$

- Interest rate is higher when U is higher
- When lots of people want to borrow, what happens?
  - U increases, decreasing borrowing, increasing lending
  - Pool equilibrates at a larger size, possibly higher rate

Rate Setting on Aave

- Aave interest rates based on utilization:

$$U = \frac{Total\ Borrowed}{Total\ Lent}$$

- Interest rate is higher when U is higher
- When lots of people want to borrow, what happens?
  - U increases, decreasing borrowing, increasing lending
  - Pool equilibrates at a larger size, possibly higher rate
- When few people want to borrow, what happens?

Rate Setting on Aave

- Aave interest rates based on utilization:

$$U = \frac{Total\ Borrowed}{Total\ Lent}$$

- Interest rate is higher when U is higher
- When lots of people want to borrow, what happens?
  - U increases, decreasing borrowing, increasing lending
  - Pool equilibrates at a larger size, possibly higher rate
- When few people want to borrow, what happens?
  - U decreases, decreasing lending, increasing borrowing
  - Pool equilibrates at a smaller size

Rate Setting on Aave

- Aave interest rates based on utilization:

$$U = \frac{Total\ Borrowed}{Total\ Lent}$$

- Interest rate is higher when U is higher
- When lots of people want to borrow, what happens?
  - U increases, decreasing borrowing, increasing lending
  - Pool equilibrates at a larger size, possibly higher rate
- When few people want to borrow, what happens?
  - U decreases, decreasing lending, increasing borrowing
  - Pool equilibrates at a smaller size
- When some lenders need to withdraw, what happens?
  - U increases, so remaining lenders have incentive to stay in pool
  - New lenders higher incentive to join pool
  - Borrowers have incentives to scale down

See Aave website

The Defi Fixed Income Ecosystem

Borrowing/lending protocols imply there is now an ecosystem of fixed income strategies available in defi:

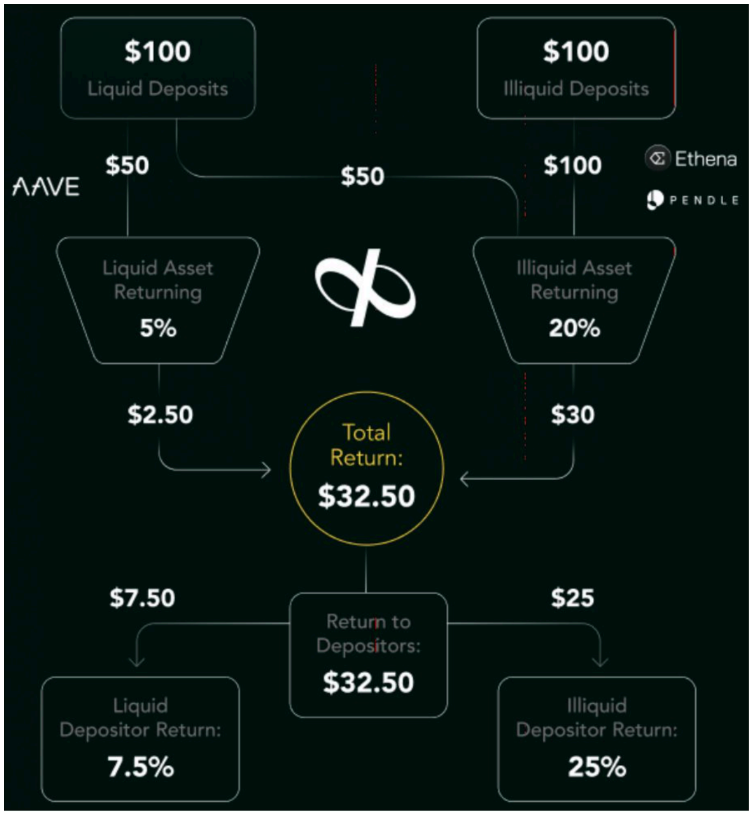
- Pure borrow/lend (Aave, Compound)
- Stablecoin market making (Curve, Convex)
- Clones/variants on other chains besides ETH
- Frontiers: uncollateralized lending, fixed rates...

Fractional Reserve Banking with Infinifi

infinifi.xyz

Fractional Reserve Banking with Infinifi

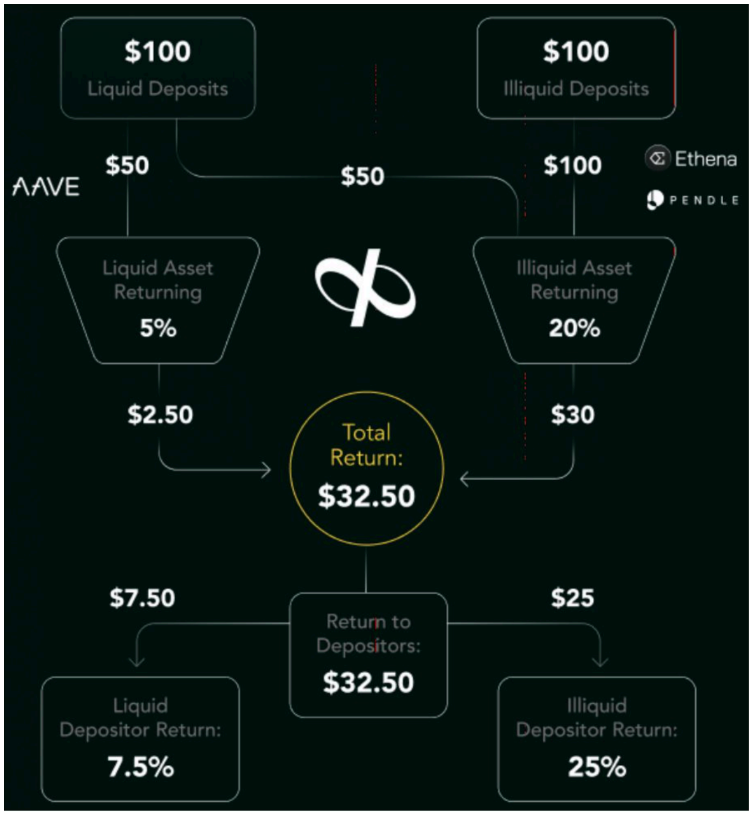
Fractional reserve banking/ Maturity transformation in DeFi



Will this work without deposit insurance?

Fractional Reserve Banking with Infinifi

Fractional reserve banking/ Maturity transformation in DeFi



Will this work without deposit insurance?

- My prediction: This protocol is vulnerable to bank runs.

Uncollateralized lending relies on Reputation

ledgerscore

Web3 Identity

- What's in a physical wallet?

Web3 Identity

- What's in a physical wallet?
  - Cash, credit cards, and identity cards!
- An ID card is an item which:
  - Proves who you are (student, gym member...)
  - Gives you certain rights (discounted tickets, gym access...)
- ID cards are not transferrable!
- We can create web3 ID cards through non-transferable tokens
- May 2022 Weyl-Ohlhaver-Buterin paper: soulbound tokens as the basis of web3 identity

Project Ideas: SBTs and Web3 Identity

Identity very young, essentially no apps yet, so a good area for class projects! Many taken from WOB paper

- What are good SBT use cases?
  - Diplomas? Employment history?
  - "Social credit scoring"? Rewards for good deeds?
  - Some examples: Otterspace, Disco.xyz, Lens, and others
- How should SBTs work?
  - Who gets to bestow SBTs?
  - Who gets to remove SBTs? Privacy? "Scarlet letter" SBTs?
  - How do we solve "walking away from my soul"?
- In a world where SBTs are ubiquitous, what functions are enabled that can't exist yet?
  - SBT-based uncollateralized lending?
  - SBT-ML and recommendation filtering?
  - SBT-gated social organization? Private clubs? Dating apps?
- More broadly, what are some implications of "native composability" that the world hasn't realized yet?

Native Composability

- Web3 (DeFi) gives us native composability
- In web2, app functions and data are closed by default
  - Facebook, Google, Twitter have internal functions, data...
  - But can't access each other's data + functions, unless they specifically build APIs to do so
  - If Google doesn't want your app to "plug into" Google maps, hard for you to do so

Native Composability

- Web3 (DeFi) gives us native composability
- In web2, app functions and data are closed by default
  - Facebook, Google, Twitter have internal functions, data...
  - But can't access each other's data + functions, unless they specifically build APIs to do so
  - If Google doesn't want your app to "plug into" Google maps, hard for you to do so
- In web3, app functions + data are open by default!
  - Very hard for Uniswap to "stop" your app from calling Uniswap functions!
  - All data is on chain: everyone can see every app's data!

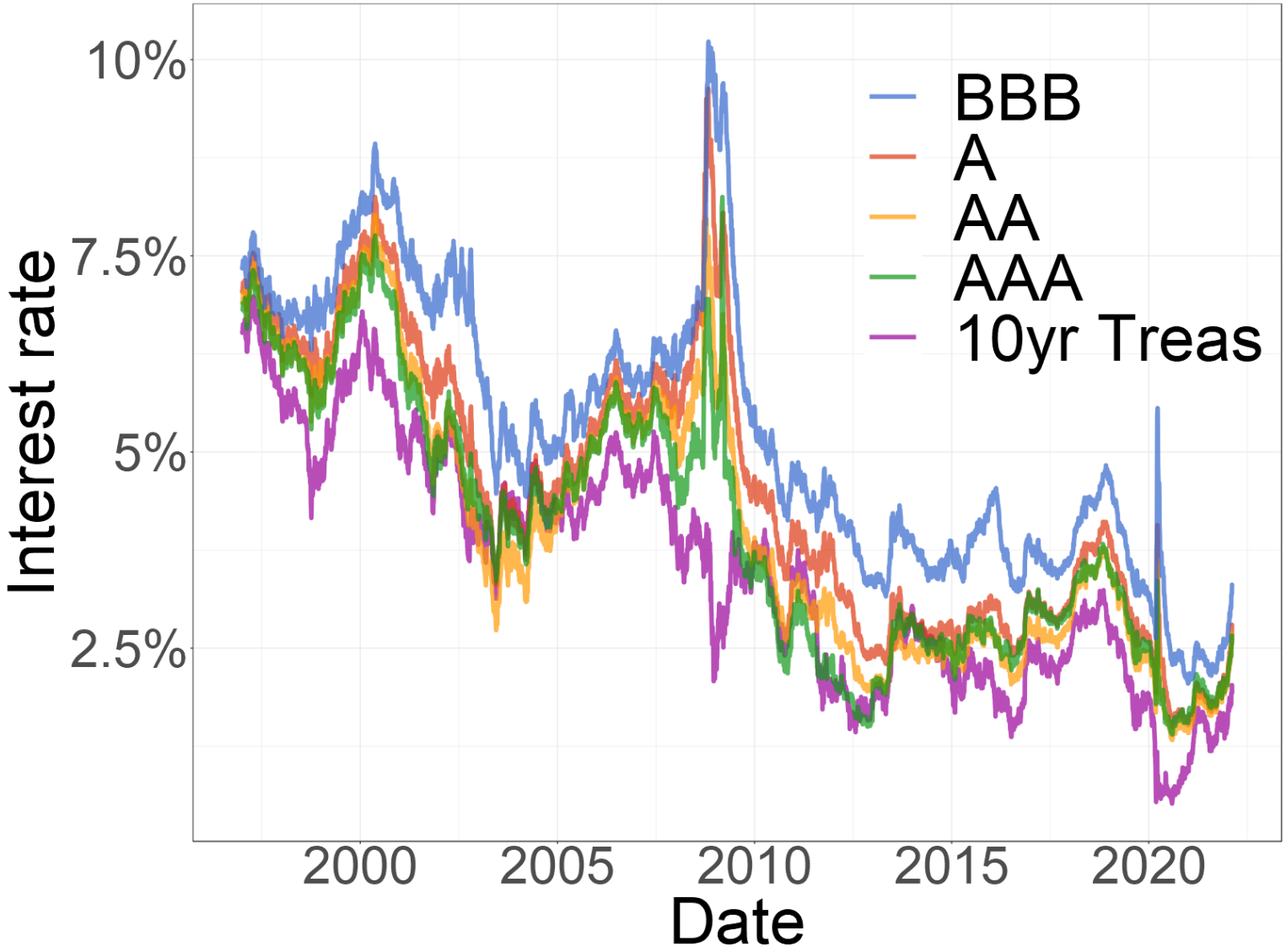
Native Composability

- Web3 (DeFi) gives us native composability
- In web2, app functions and data are closed by default
  - Facebook, Google, Twitter have internal functions, data...
  - But can't access each other's data + functions, unless they specifically build APIs to do so
  - If Google doesn't want your app to "plug into" Google maps, hard for you to do so
- In web3, app functions + data are open by default!
  - Very hard for Uniswap to "stop" your app from calling Uniswap functions!
  - All data is on chain: everyone can see every app's data!
- Harder to construct "walled garden ecosystems", lower barriers to entry + less incumbent advantage

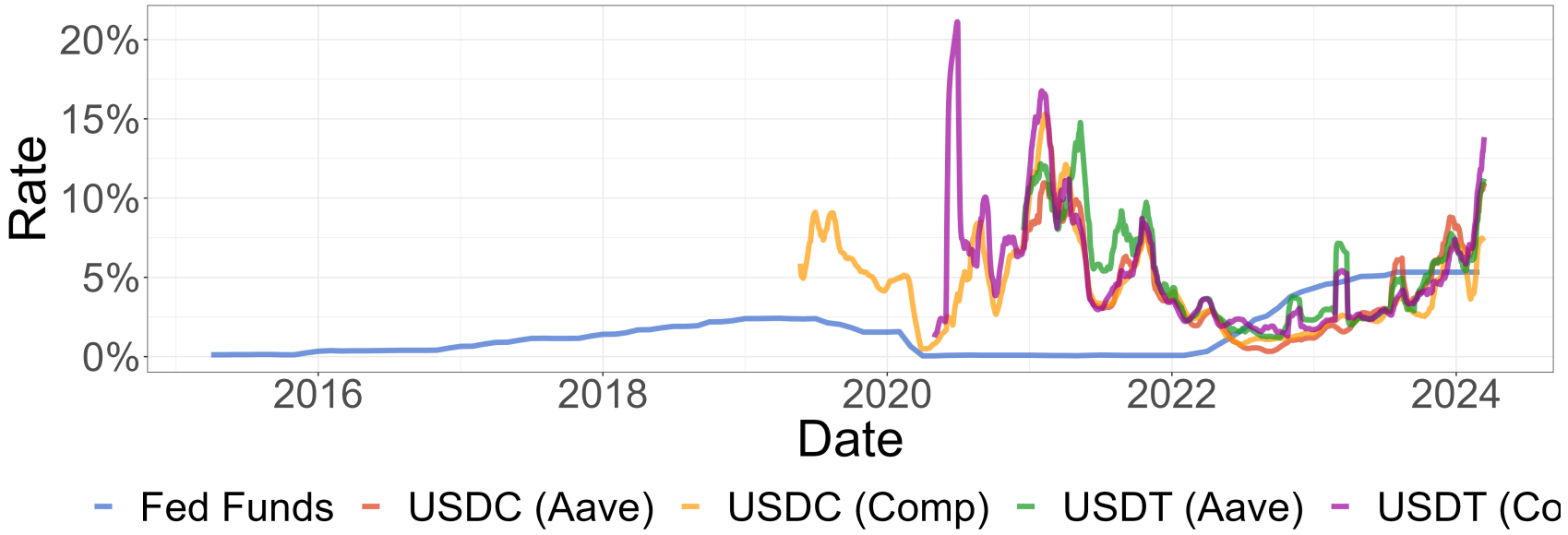
See "Appendix: Composability" in Saffron Huang's post here

Faster Horses?

Interest Rates in Traditional Finance



Interest Rates in Defi



Liquidation

I borrow $400k against my $500k house

- Ideal case: I pay back $400k, live in my house
- Non-ideal: I can't make payments, bank sells my house and keeps $400k
- Safety of bank's mortgage debt depends on how well they can "liquidate collateral"
- How does a smart contract play the role of the bank in liquidating collateral?

Ideal Liquidation

- Suppose you borrow $100 USD against $150 of ETH
- ETH price drops to be worth $149, so your position must be liquidated
- "Ideal" procedure:
  - Protocol detects that ETH price dropped, your position is insolvent
  - Protocol sells ETH to pay down your debt
- Is this possible?

Ideal Liquidation

- Suppose you borrow $100 USD against $150 of ETH
- ETH price drops to be worth $149, so your position must be liquidated
- "Ideal" procedure:
  - Protocol detects that ETH price dropped, your position is insolvent
  - Protocol sells ETH to pay down your debt
- Is this possible?
- Requires:
  - An Oracle to tell it relevant prices
  - Either a human in the loop or a replenishing supply of gas to continually check prices and liquidate as necessary
  - Someone to whom to sell the ETH

Liquidation in Practice: Sale Mechanism

- Sell to AMM?
  - Large order, may move prices too much
- Sell to humans? How?

Liquidation in Practice: Sale Mechanism

- Sell to AMM?
  - Large order, may move prices too much
- Sell to humans? How?
- **Aave/Compound:** fixed price, below current oracle price, see risk parameters

Liquidation in Practice: Sale Mechanism

- Sell to AMM?
  - Large order, may move prices too much
- Sell to humans? How?
- **Aave/Compound:** fixed price, below current oracle price, see risk parameters
  - Fast, safe, but potentially leaves a lot of money on the table

Liquidation in Practice: Sale Mechanism

- Sell to AMM?
  - Large order, may move prices too much
- Sell to humans? How?
- **Aave/Compound:** fixed price, below current oracle price, see risk parameters
  - Fast, safe, but potentially leaves a lot of money on the table
- **Maker**: collateral sold in descending auction
  - Slower, but very likely to get more money

Risks: Oracle Risk

- Unlike AMMs, collateralized lending systems require oracle inputs for prices
- Risk factor: if oracle gets manipulated, lending system is at risk!
- How would you attack Aave through oracle manipulation?

Risks: Oracle Risk

- Unlike AMMs, collateralized lending systems require oracle inputs for prices
- Risk factor: if oracle gets manipulated, lending system is at risk!
- How would you attack Aave through oracle manipulation?
  1. Deposit $100 Xtoken as collateral
  2. Manipulate oracle, make Aave think $100 Xtoken is worth $100,000
  3. Borrow $50,000 USDC against your Xtoken
  4. Default: you've just traded $100 Xtoken for $50,000 USDC!
- See here for other examples of oracle attacks
- Chainlink is the main oracle provider
  - Uses off-chain data! Ironic, as it's more "principled" to use on-chain data

Alleviating Oracle Risks?

Liquidation Bonds: While a loan's eligibility to be liquidated is determined formulaically by the contract, no actual liquidation will occur unless an external user triggers one. In order to trigger a liquidation this user must pledge a liquidation bond. A liquidation bond is effectively a bet, with a payoff curve similar to a short put option spread (effectively a bet that the bidders in the dutch auction will place bids below the Neutral Price of the loan, see 7.3.1 Determining the Neutral Price), on the outcome of a pay-as-bid dutch auction for the collateral. This mechanism encourages fair outcomes by imposing a penalty on spurious liquidations. While there is no endogenous incentive to spuriously liquidate a borrower in Ajna, this introduces an overt disincentive to liquidate loans that are well collateralized with respect to the market price of the collateral (as well as an incentive to liquidate loans that are comparatively undercollateralized).

Source: Ajna protocol

Alleviating Oracle Risks?

Liquidation Bonds: While a loan's eligibility to be liquidated is determined formulaically by the contract, no actual liquidation will occur unless an external user triggers one. In order to trigger a liquidation this user must pledge a liquidation bond. A liquidation bond is effectively a bet, with a payoff curve similar to a short put option spread (effectively a bet that the bidders in the dutch auction will place bids below the Neutral Price of the loan, see 7.3.1 Determining the Neutral Price), on the outcome of a pay-as-bid dutch auction for the collateral. This mechanism encourages fair outcomes by imposing a penalty on spurious liquidations. While there is no endogenous incentive to spuriously liquidate a borrower in Ajna, this introduces an overt disincentive to liquidate loans that are well collateralized with respect to the market price of the collateral (as well as an incentive to liquidate loans that are comparatively undercollateralized).

Source: Ajna protocol

Put simply: Ajna makes loans that fail margin *eligible* for liquidation. A human must always "pull the trigger", and that human is penalized *ex-post* if the collateral turns out to be good after all (a "**spurious liquidation**").

Welcome! Today is Wednesday, October 8

Homework 3 is due Monday. Some students have observed that Uniswap defaults to a high gas fee – this can be changed in the transaction settings.

Also for Monday: read "In Praise of Ponzis" by Dror Poleg: https://www.drorpoleg.com/in-praise-of-ponzis/

The second and final **Midterm Exam** is **Wednesday, October 15**. The Practice Midterm is on Canvas. The practice answer key will be revealed on Friday.

In the News: Key Cybersecurity Law Expires

CISA 2015 Has Sunset. Now What?

Congress failed to renew the Cybersecurity Information Sharing Act of 2015 before its expiration despite broad bipartisan support. Companies must assess their cyber threat intel sharing relationships and mitigate legal risks.

By Michael T. Borgia

10.02.25

What does this mean?

- A patchwork of federal and state laws restrict companies' ability to share data. Two main concerns:
  - **Privacy**: companies may compromise the privacy of their users by sharing data
  - **Antitrust**: companies who share data may be accused of colluding to raise prices instead of competing in the free market
- From 2015 to 2025, companies had **safe harbor** to share data concerning cybersecurity threats with each other and the federal government
- With this protection gone, companies may stop sharing information with each other.

In the News: Arc White Paper

Abstract

Arc is a purpose-built, EVM-compatible Layer-1 blockchain advancing the frontier of stablecoin finance and tokenization. It features USDC as native gas, deterministic settlement finality, opt-in privacy, and a stable transaction fee architecture. Optimized for stablecoin-native use cases, such as global payments, FX, and capital markets, Arc serves as a foundational settlement layer for programmable money on the internet.

- **Circle**, the issuer of USDC (#2 largest stablecoin), encourages developers to ditch Ethereum for Arc

In the News: Arc White Paper

Why denominate gas fees in USDC (Circle's USD stablecoin)?
My inbox yesterday:

Coinbase	Inbox	Price alert: Ethereum (ETH) is down ↘ -4.99% ·	11:57 AM
Coinbase	Inbox	Price alert: Ethereum (ETH) is up ↗ +5.02% - h	Oct 6

In the News: Arc White Paper

Circle's Philosophy: "It is built on the conviction that the future of finance and commerce is not a wholesale replacement of the old, but a synthesis of the new and the established: the programmability of smart contracts with the enforceability of law (i.e., GENIUS Act); the efficiency of blockchain with the stability of fiat-backed currency; and the transparency of public ledgers with the privacy required for commercial transactions."

In the News: Arc White Paper

- "Arc will rely on a permissioned, **Proof-of-Authority (PoA)** validator set composed of a limited number of known, established, and geographically distributed institutions held to high standards of accountability and operational guarantees."
- The Arc project **gives up on decentralization** and **gives up on value appreciation** in order maximize its utility and stability for the current, existing financial system.
- Giving up on value appreciation is a big deal! Early adopters cannot capture the value of the future adoption that they encourage.

Fire Sale and Contagion: a Vicioius Cycle

Recall the discussion of **leverage** (borrowing money) and **liquidations** (e.g. a margin call).

- Suppose price of ETH drops
- People borrowing against ETH get liquidated, so ETH gets sold
  - This is called a **fire sale**
- Selling pressure pushes down ETH prices...
- Leading to more liquidations...
  - This is called **contagion**

Systemic Fragility

Systemic Fragility in Decentralized Markets

Alfred Lehar*
Haskayne School of Business
University of Calgary

Christine A. Parlour†
Haas School of Business
UC Berkeley

July 16, 2022
Preliminary
Comments Welcome

Abstract

We analyze a unique data set of collateral liquidations on two Decentralized Finance lending platforms – Compound and Aave. Such liquidations require arbitrageurs to repay the loan in return for the discounted collateral. Using Blockchain transaction data, we observe if arbitrageurs liquidate positions out of their own inventory or obtain "flash loans." To repay flash loans, arbitrageurs immediately sell the collateral asset. We document the high frequency price impact of such liquidity trades on nine different decentralized exchanges. Consistent with large block trades in equity markets there is a temporary and permanent price impact of collateral asset sales in DeFi. We document the effect of these trades on return distributions. Our work highlights the systemic fragility of decentralized markets.

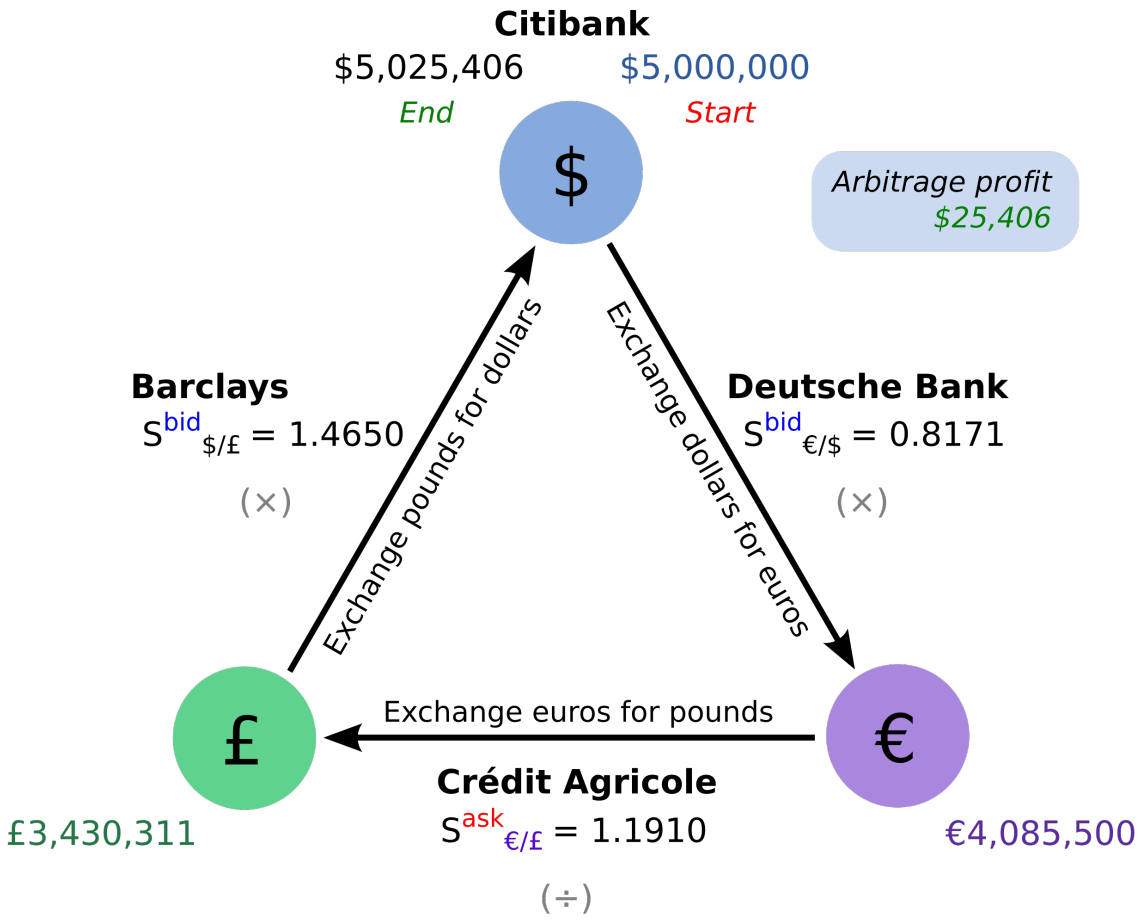
Keywords: Decentralized Lending, Blockchain, Decentralized Finance, Systemic Risk

Source

Flash Loans

- Unlike traditional finance, transactions in defi are atomic: either the whole tx finishes, or none of it does
- Enables a cool trick called flash loans
- You can borrow a very large amount of money, unsecured...
- ...as long as you pay it back *in the same transaction!*
- If you can't pay back the money, tx fails, so you never borrowed it in the first place!
- Flash loans available from Aave, Compound...

Triangular Arbitrage in Traditional Currency Markets



The elimination of triangular arbitrage imposes strict limits on bilateral exchange rates **in frictionless markets**: if Euros are X/dollar, and Pounds are Y/dollar, Euros <u>must</u> be (X/Y)/Pound.

Flash Loans: Consequences

- In tradfi, arbitrage requires capital and infrastructure
  - Hedge funds can do trades you can't
- In DeFi, infrastructure accessible by default; flash loans democratize capital
- If there are arbitrage opportunities, anyone can extract them!
  - "Triangular arbitrage" becomes close to frictionless!

Case Study: The Cream Finance Hack

- Zhang writes about the CREAM finance attack
- Attacker submitted a bundle of 20 transactions, borrowed a billion dollars, made $130mil, paid $6,500 in gas fees!
- Details complicated, but essentially:
  - CREAM finance allows you to borrow collateralized, borrowing amount determined by price oracle
  - Attacker builds a large collateral + debt position through "rehypothecation"
  - Flash borrow $1.5bil, deposit in CREAM
  - Manipulate price, to make CREAM think $1.5bil of collateral is worth $3bil
  - Borrow $2bil of ETH against collateral, worth only $1.5bil
  - Default on collateral, keep $2bil in ETH, pay back $1.5bil flash loan, keep $500mil ish in profit (actually only $130mil)

Case Study: The Beanstalk Attack

- Tweet thread on the Beanstalk attack
- Beanstalk is an algo-stablecoin, holds collateral
  - A **stablecoin** is a coin intended to trade always at $1
  - An **algo-stablecoin** tries to do this without relying on the regulated banking system (recall "Terra")
- Governance done through equity tokens: majority token vote approves any change

Case Study: The Beanstalk Attack

- Tweet thread on the Beanstalk attack
- Beanstalk is an algo-stablecoin, holds collateral
  - A **stablecoin** is a coin intended to trade always at $1
  - An **algo-stablecoin** tries to do this without relying on the regulated banking system (recall "Terra")
- Governance done through equity tokens: majority token vote approves any change
- **Does this sound like a good idea?**

Case Study: The Beanstalk Attack

- Tweet thread on the Beanstalk attack
- Beanstalk is an algo-stablecoin, holds collateral
  - A **stablecoin** is a coin intended to trade always at $1
  - An **algo-stablecoin** tries to do this without relying on the regulated banking system (recall "Terra")
- Governance done through equity tokens: majority token vote approves any change
- **Does this sound like a good idea?**
- Attacker proposed: "send entire treasury to my address"

Case Study: The Beanstalk Attack

- Tweet thread on the Beanstalk attack
- Beanstalk is an algo-stablecoin, holds collateral
  - A **stablecoin** is a coin intended to trade always at $1
  - An **algo-stablecoin** tries to do this without relying on the regulated banking system (recall "Terra")
- Governance done through equity tokens: majority token vote approves any change
- **Does this sound like a good idea?**
- Attacker proposed: "send entire treasury to my address"
- Flash borrowed a bunch of equity tokens, passed the proposal, took all the money!

Flash Loans: Consequences

Consequences of flash loans:

- "On-chain" price oracles (for collateral valuation, derivatives settlement, etc.) very rarely used: often attackable
- Hacky solution: just use Binance prices, imported through Chainlink, instead
  - Binance is a "traditional exchange" that holds on-chain assets for you
  - These have a "human in the loop"
- Governance attacks rarer: beanstalk a unique case
- The threat of "51% attacks" is why most modern protocols do not operate on unconstrained democracy.

Roadmap

1. Pain Points of TradFi
2. Promise of DeFi
3. Lending Protocols
4. Derivatives

Derivatives

Derivatives are simply contracts that take the prices of other contracts (or commodities) as inputs. Popular derivatives include:

- Synthetics: I pay you the price of an asset X
  - Exposed to counterparty risk!
  - **Clearinghouses** are trusted intermediaries who mitigate counterparty risk, e.g. by holding collateral
- Options: I pay you (the greater of 0 or) the price of a stock x minus the strike price k at the expiration date t (this example is called a "call option").
- Futures: I pay you the price of X at date t
- X could be a price, an interest rate, a ratio of prices, let your imagination go wild...

Options

- Off-chain options on crypto fairly widely available: Binance, Deribit, FTX...
- Liquidity remains low (high bid-ask spread, volatile prices)
- Many projects trying to build on-chain options. A few classes of approaches:
  - Standard options: Premia
  - "Power perpetuals", gamma exposure through convex futures: Opyn Squeeth
  - Replicating options through AMM LP positions: Panoptic
- Application layer:
  - Structured products: Ribbon Finance, Friktion
- Some other projects: dopex, Lyra, rysk, Primitive

Others

Futures, Synthetic Assets

- Create an on-chain derivative to track price of some index or asset. Goal:
  - Leverage
  - Access (US stock exposure for non-US residents)
- See dYdX, Synthetix, GMX, Mycelium
- Interesting (off-chain) innovation: the perpetual contract, a never-expiring futures contract
  - See Dave White's guide

Others

Bridges, Cross-Chain Defi

- With rise of multiple L1's, "bridging" assets across chains becoming more important
- Binance, Wormhole, Ronin some examples
- All 3 have been subject to $> \$100mil$ hacks!

Insurance

- Risk Harbor: automated on-chain op risk insurance
- Nexus Mutual: "DAO court" system

The main problem (same as in TradFi!): deciding whether a physical event meets a definition given in the contract.

- Another manifestation of the *Oracle Problem*

Oracles

All derivatives rely on oracles to tell them prices, just as insurance contracts rely on claims adjusters (and, in case of dispute, judges) to determine payouts.

- Chainlink very dominant on Ethereum
- Pyth on Solana

No one has yet built a reliable and widely-used on-chain oracle!