DeFi executes fast and capital efficient liquidations and other similar transactions by using flash loans and real-time price oracles. However, the cost of this efficiency is that there are rarely options available for recourse when something goes wrong. Recourse is useful because it gives parties a way to address deviate outcomes ex-post.

Consider the following examples where recourse might have resulted in a different, more anticipated, outcome:

- Incorrect prices provided to contracts (1) (2) (3)

- Incorrect liquidations due to manipulated prices (1) (2)

- Auctions accepting zero bids due to network congestion (1)

- Governance bugs (1) (2)

- Flash loan attacks (1) (2)

The intent of these examples is not to denigrate any of the protocols involved, but rather to demonstrate that DeFi users accept significant tail risk by operating in an environment without recourse. This type of tail risk is not present in TradFi, so why do we accept these risks in DeFi?

In this article, we attempt to formalize some of our internal discussions about this tail risk by focusing on the trade-off between three properties of financial systems:

1. Anonymity

: Anyone can interact with anyone in a trustless manner; whether or not they know their counterpart

1. Instant resolution

: A transaction is settled as soon as it has been processed. For example, a liquidation in DeFi is processed in the same block that it is sent.

1. Recourse

: Ability to dispute the validity of a particular transaction and seek reparation.

These properties apply differently to various financial systems:

TradFi

TradFi has instant resolution and recourse, but does not have anonymity.

For example, consider the purchase of a stock. When an individual purchases a stock, it appears in their portfolio. If the stock does not show up in their portfolio then the individual can take legal action against their broker. Anonymity in this system is impossible because participants must be able to identify one another in order to seek compensation through the judicial system.

Fast DeFi

The vast majority of DeFi today operates under what we call "Fast DeFi". Fast DeFi provides instant resolution and anonymity, but does not have recourse options available.

In order to have instant resolution, Fast DeFi needs access to instantaneous and robust price feeds. This can be difficult because there can be manipulations of the actual market price even when the price feed reports the price correctly.

Flash loans are a powerful innovation created for DeFi. They allow any individual, independent of their personal access to capital, to borrow the capital required to liquidate even the largest positions. Flash loans require instant resolution which is one reason why Fast DeFi prioritizes instant resolution over recourse.

Regarding the lack of recourse, consider how a liquidation on a protocol like AAVE or Compound works: One (anonymous) user determines that another (anonymous) user's position is under-collateralized according to a price reported by a real-time price oracle. The first user submits a transaction (possibly using flash loans) to repay a fraction of the second user's debt and, in return, is given some fraction of the users collateral. There is instant resolution and both users remain anonymous, however, liquidated users have no opportunity for recourse if the liquidation occurred at an inaccurate price.

Slow DeFi

There are some pieces of DeFi where we can create delays without degrading the user experience. We refer to these types of DeFi applications as "Slow DeFi". Slow DeFi sacrifices instant resolution to achieve anonymity and recourse.

For example, a predictions market, like Augur or Polymarket, allows users to take positions on relatively bespoke questions

like, "Will there be a named tropical system Wanda that forms before November 1, 2021?" A user can trade on these outcomes using the prices implied by the demand for each token. Individuals who trade this type of an asset are often operating on a longer time-horizon so instant resolution is a lower priority for them.

A small percentage of DeFi applications currently operate in the Slow DeFi environment, but Slow DeFi has been successful in settling certain types of smart contracts where users value recourse over resolution.

The future of DeFi

The question is, what is the future of DeFi if the status quo regarding recourse continues? Or what if DeFi seeks wider availability of recourse? The above framework for how to think about financial systems emphasizes the trade off between instant resolution and recourse in the DeFi space, where anonymity is usually prioritized. Over the next few years, there are a few ways that DeFi could evolve:

The lack of recourse is embraced

While a system without recourse is incompatible with today's traditional finance systems, this may not be a catastrophic blow. There are significant benefits to DeFi and it is plausible that the tail risks are perceived to be sufficiently small that it is not worth the investment required to establish a recourse-compatible Fast DeFi system.

There are a few things we should take into account if DeFi ends up on this path:

- There are certain subsets of the population that will be crypto-hesitant while recourse is unavailable. In other words, it is hard to imagine a CFA putting client's life savings into DeFi without a viable option for recourse.

- We should allow tail risk to be priced in. Right now, tail risk is not priced in because assets typically are forced to trade at their off-chain market value. Importantly, this off-chain value does not account for on-chain risk. For example, a synthetic representation of an equity on the blockchain may trade at a discount relative to fair-value because there is a higher probability that the DeFi synthetic is lost in an attack. This doesn't mean that this synthetic will trade at a discount, though, because there are also benefits in DeFi that might lead the synthetic to trade at a premium.

Options for recourse emerge

It is also plausible—whether through innovation or regulation—that providing options for recourse becomes the standard for many DeFi protocols.

We have a few ideas for how recourse could be provided:\

- The expansion and broader uptake of existing insurance protocols. Protocols like Nexus Mutual already provide insurance for certain types of smart contract failure and other hacks.

- More slow DeFi. Slow DeFi is clearly not a good fit for all types of DeFi applications, but it could be used more widely than it currently is. Contracts that operate on a longer time-horizon and don't require liquidations make good candidates.

- Another alternative is to create "insured oracles" which would align incentives between the user and the oracle. Currently, risk is fully assumed by the users, whereas the oracle is insulated from the consequences of their reported prices. An insured oracle might operate in the following way:

- A user requests a price that they can use to liquidate a position of size $X. (off-chain)

- The insured oracle responds with two things: A fee that they would need to be paid to provide a price, and, a price that they would be willing to insure for the liquidation. This price might be higher than the market price if there is uncertainty or suspicious fluctuations. (off-chain)

- The user then utilizes that message on-chain to obtain a price that they can perform the liquidation with and the oracle's message is used to lock $X of the insured oracle's capital into a recourse contract.

- If the person liquidated feels that the price was inaccurate, they could seek recourse against insured oracle's locked $X.

- A user requests a price that they can use to liquidate a position of size $X. (off-chain)

- The insured oracle responds with two things: A fee that they would need to be paid to provide a price, and, a price that they would be willing to insure for the liquidation. This price might be higher than the market price if there is uncertainty or suspicious fluctuations. (off-chain)

- The user then utilizes that message on-chain to obtain a price that they can perform the liquidation with and the oracle's message is used to lock $X of the insured oracle's capital into a recourse contract.

- If the person liquidated feels that the price was inaccurate, they could seek recourse against insured oracle's locked $X.

What to do?

In a space as fast-moving as DeFi, no doubt more refined and robust solutions for recourse will emerge. Or they will not, and tail risk will be accounted for in other ways. Exploring whether or not recourse should be available highlights areas for growth in DeFi and the potential pitfalls of an ever evolving financial landscape.

Chase (UMA)

This article benefited from discussions with the entire team at UMA. A special thanks to Hart Lambur, Clayton Roche, and Kevin Chan for comments on this post. Any remaining lack of judgement or other errors are solely my own.