Twitter Thread by Nick Chong



Nick Chong
@n2ckchong

If you've been following DeFi or Ethereum over the past few months, you've likely heard the term "flash loan" mentioned again and again.

This new DeFi primitive has been at the core of a number of economic exploits and arbitrages.

A thread on the basics of flash loans - ■



Most DeFi loans take place across days, weeks, or even months.

You can deposit Ethereum into Aave, then withdraw stablecoins for yield farming in Yearn, for instance.

On-chain loans have garnered much traction, with total debt outstanding moving toward $2.5 billion.

While popular, DeFi loans are not capital efficient: to account for custodial risk and volatility risk, you need to put up 130-150% of the value of your loan in collateral.

If your collateral slips below the threshold, you're liquidated, resulting in a fee anywhere from 5-13%.

Flash loans are much different than longer-term DeFi loans.

Flash loans are non-custodial, take place over the course of one block, and require no collateralization.

That's to say, the coins you borrow never appear in your wallet.

When taking a flash loan, you can direct the coins to any protocol and function, as long as you pay back the loan + interest fee within the same transaction.

So what the hell? What are flash loans used for?

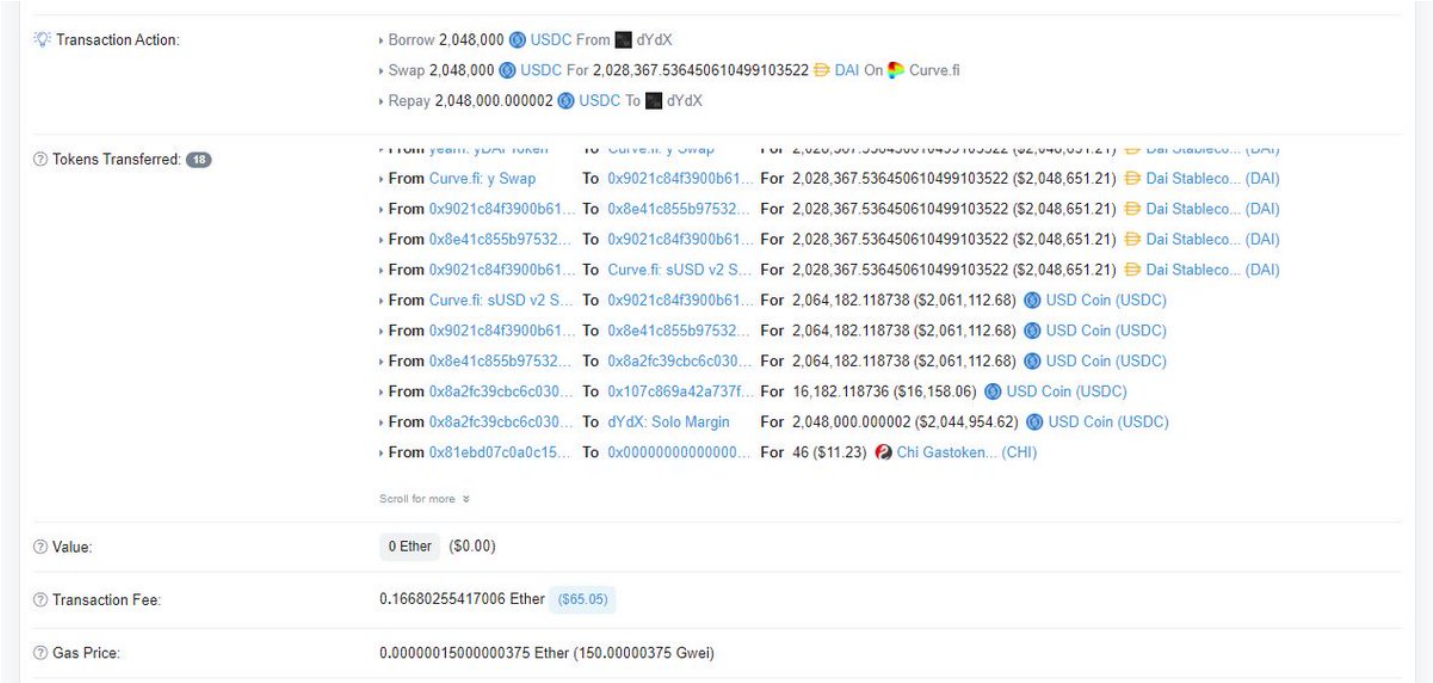
More often than not, arbitrage.

This means that if you spot mispriced markets between AMMs or dexs, you can take a flash loan to arbitrage the pools.

Here's a simple example I spotted in the mempool a few months back:

https://t.co/hiBHuTerQH

More on what's happening in the next tweet.



- This user flash borrowed 2,048,000 USDC from dYdX

- Traded that USDC for 2,028,367 DAI in Curve's Y pool

- Traded that DAI for 2,064,182 USDC in Curve's sUSD pool

- Paid dYdX back + 2 wei

All in one block...

Profit: 16,182 USDC
Cost: $60 in gas

Crazy, right?

The transaction I mentioned is just one of many simple arbitrages between different AMMs and diff pools. (More on AMMs in the linked thread.)

There are also advanced arb strategies that enabled the "attacks" on Eminence, Harvest, etc.

Let's take a look.

https://t.co/wftj1YuPtG

> Bitcoin is resilient around $13k, Ethereum hit $420, and DeFi TVL is at an ATH at $12 billion.
>
> As DeFi continues to grow, decentralized exchanges will remain pivotal.
>
> Here\u2019s a thread on the outlook of the AMM market (Uniswap, Balancer, Sushiswap, LinkSwap, DODO). pic.twitter.com/LPWVkCaKbM
>
> — Nick Chong (@n2ckchong) October 27, 2020

Many of these arbs are not AMM based. Instead, these arbs are accomplished by leveraging some faulty or buggy logic in the economic design of a protocol.

Eminence:

- Borrow 15 million DAI from Uniswap
- Mint EMN
- Burn some EMN for eToken, driving up EMN up the curve
- Sell remaining EMN for DAI
- Make millions

The bug was the bonding curve was steep and could be manipulated.

https://t.co/fP3ae4oDXQ

Harvest:

The bug was that Harvest didn't use the get_virtual_price() function from Curve, allowing for manipulation.

Flash loans can also be used for other purposes.

Governance attacks are a good example. They're scary but still kind of sick, to be honest.

On October 26th, a user used flash loans to influence a MakerDAO proposal.

https://t.co/naqLqOi1bS

This user completed multiple complex functions with a single tx, within a single block.

They

- borrowed $20m worth of WETH from dYdX
- deposited it on Aave to borrow $7m worth of MKR
- Locked MKR in governance
- Voted on a proposal
- Unlocked MKR
- Sent MKR, then ETH back

Related to flash loans, developers are working on flash mints for Wrapped Ethereum and DAI. Will do another thread on these later.

Flash loans will be similar in concept to flash mints but will involve the minting, then burning of tokens rapidly to accomplish some feat.

To conclude: Flash loans are an extremely powerful DeFi primitive.

I forgot who said it but they're going to accelerate the wheat from the chaff when it comes to protocols with good economic design.

I'm excited (and scared) to see what flash loans are used for next.

