Hi everyone, this Java Xu from University College London. Today i'll be presenting this SOK -- sysmatization of knowledge -- on your aggregators in DeFi -- decentralized finance. This is a joint work with Simon Cousaert and Toshiko Matsui.

Before diving into what your aggregators are, it is utterly important to understand what decentralized finance or DeFi is. DeFi is a financial system that operates according to protocols composed of smart contracts on blockchains.

On this slide you'll see that Yield aggregators are a type of DeFi applications.

So what the other different applications are there.

First of all, there are decentralized exchanges with automated market making protocols, or AMMs, such as Uniswap, Balancer curve dodo.

With AMMs, liquidity providers provide liquidity to a liquidity pool and exchange users swap tokens against the pool.

A liquidity pool is usually characterized by a bonding curve that specifies the exchange rate between two crypto assets algorithmically.

By using AMM decentralized exchanges, traders would need to pay a fee, which would ultimately be collected by liquidity providers as part of their return.

The second type of DeFi applications is lending protocols, such as MakerDAO, Compound and AAVE.

Self-explanatorily, with lending protocols, one can borrow assets and can also lend assets.

Borrowers will have to pay borrow interest, and this interest will ultimately also be distributed to the lenders who would collect lending interest.

The third type of different applications is the focus of this presentation, yield aggregators. Here I list some well-established yield aggregators such as Yearn finance, harvest finance and pickle finance, as well as an example of emerging ones such as Bank of Chain.

Last but not least, we have token-based insurance solutions such as nexus mutual, Etherisc and inSure. Although only optional, more and more yield aggregators are starting to incorporate insurance solutions in their protocols to create a more secure investment environment for their users.

So now let's take a step back. What exactly are yield aggregators and how do we define them.

Yield aggregator can essentially be considered as a decentralized fund manager that uses more contracts to determine and execute investment strategies.

But where do the yields come from?

Well, on this slide I list three sources of yields: borrowing demand, revenue sharing and liquidity mining.

Borrowing demand is usually associated with lending protocols. As explained, lenders of lending protocols are able to collect lending interest.

So if you deposit your assets into a lending protocol, you will earn return algorithmically defined by the lending Protocol. Usually, all other things equal, the higher the fund utilization ration, defined as borrow as a fraction of deposit, the higher the lending interest.

The second category is revenue sharing. Again, as explained for decentralized exchanges liquidity providers who provide liquidity to a decentralized exchange pool or collected some kind of fee ultimately paid by exchange users.

Revenue sharing usually pertains to liquidity provision for decentralized exchanges.

The third category is liquidity mining, this is a unique feature of defy protocols at the moment.

To incentivize to incentivize participation in protocols to incentivize participation, a lot of protocols now reward users with some kind of reward tokens, which are often governance tokens of the protocol, or we call them native protocol tokens.

These protocol tokens are often valuable and exchangeable.

So, how does the Yield farming process look like?

Well, as discussed, a yield aggregator is essentially a decentralized fund manager so first of all, so first and foremost the yield aggregator needs to collect funds deposited by users, or we call them farmers because they like to farm yields.

So in phase zero a year aggregating pool needs to be established, which consists of funds collected from the farmers, which consists of which consists of funds collected from the farmers.

Then, these funds collected it can be directly used for strategy execution in phase .

Or if those funds are not the qualified funds to be invested, they can be transformed into qualified or eligible funds through lending protocols, so those funds can be deposited into lending protocol acting as a collateral and then eligible funds can be borrowed out and then go to phase two for strategy execution.

When the strategy is executed your will be formed and the claim to yields can then be reinvested in Phase three into the original you're aggregating pool to achieve this kind of compounding effect.

So the most exciting part of the farming process is obviously face to strategy execution so let's have a closer look at strategy execution.

Here in this chart you'll see that the deploy capital is usually static assets that do not generate yield, what does that mean well, it means that

If you if you hold static assets in your wallet there will always stay the same. However, through investing, those static assets can be turned into yield bearing assets, for example, if you invest the static assets into letting protocol, such as AAVE, they can be turned into atokens which are type of yield bearing tokens that can accrue interest.

Or if the static assets are used as liquidity to be provided, into a decentralized exchange pool, then there will be turned into LP tokers which can collect exchange fees.

Once the static assets are turned into your bearing assets or one needs to do is to wait.

The longer the time passes, the more yields will be generated.

Next, I like to introduce you some specific classic your farming strategies and show you some simulation results.

Before that i'd like to present to you the simulation assumptions that we make in the paper we assume that there's no transaction cost and also We assume that the yield.

We assume that there's no transaction cost and that the your aggregator wealth is measured in day is stable coin this want one pegged to USD.

At T zero the year aggregator has a value that is one.

Also, the yield generating protocol distributes 0.01 governance token each day to its users proportionate to their stake, which means at the beginning 0.01 governance token times 1% will be distributed to the aggregator.

Next we assume that the governance token price remains constant during the simulation period just for simplicity.

We additionally assume that the lending platform has a fixed borrow rate of 10% and a collateral factor of 80%, which means that for each deposit of 1 DAI,

One is allowed to take 0.8 DAI worth of loans. We also assume that a time zero 70% of the funds in the learning protocol is lent out.

And also or other market participants additional borrow and repay as well as deposit or withdrawal cancel each other out at an aggregate level during the simulated period.

We also assume that the AMM exchanges has a fixed exchange fee of 5% and that it has a constant product conservation function this fee is charged by retaining 5% of the theoretical idealized fee free purchase quantity within the am and poor.

Lastly with automated market, making decentralized exchange hmm we assume that it has a fixed exchange fee of 5% and that it applies it comes from product conservation function.

This 5% fee is charged by returning 5% of the theoretical idealized fee free purchase quantity within the hmm pool.

The first year farming strategy that i'd like to discuss is very simple and trivial one it is simple ending. so intuitively with simple ending the assets of first deposit in the lending protocol.

This assets will then be transformed into interest bearing assets which would accrue supply interest and also collect native tokens rewarded to the depositors. Finally, the deposits can be withdrawn, together with the accrued supply interest whenever needed.

With the simulation we see that as the time passes the yield farming poor value would increase and, obviously, the higher the lending APY.

APY means annual percentage yield. basically the annual return so, of course, the higher the lending API, the higher the value of the pool will become.

And because the governance token will also be rewarded to depositors', the higher the governance token value the higher also the yard farming poor value would become.

The second strategy is what we call leveraged borrow which is little bit more complicated than the first strategy, the first step, the assets are deposited into a landing protocol.

The second step, the deposit assets act as collateral, which means that some assets can be bought out from the lending protocol and the third step the deposit assets.

In the next step, the ball as that's a redeposited in the third step the deposit the third step the ball SS or redeposited back into the learning protocol, and then we just repeat this borrowing and depositing reborn redeposited several times to form this kind of spiral borrow.

In the meantime, the interest will be accrued both for the supply side as well as for the borrower side and because lending protocols incentivize participation.

Which means they would reward tokens to both borrowers and lenders so both sides would collect reward tokens overtime.

Towards the end of the year farming period the collected reward tokens can be swapped into the assets borrowed and then can be used to repay the loans, together with the borrow interest.

And whenever needed the original deposits can be withdrawn, together with a crude supply interest.

In the simulation, we can see that, unlike simple lending leveraged borrow can be lost, generating as opposed to revenue generating.

173

00:34:44.940 --> 00:34:56.550

Jiahua (Java) Xu: This happens, especially when the rewarded native governance token has a sufficiently low value, such that it cannot cover the borrow interest rate.

174

00:34:56.940 --> 00:35:16.410

Jiahua (Java) Xu: And in that case the higher number of spirals spirals spirals the more loss, the strategy will generate but, of course, on the other side of the spectrum if the governance token price is very high, then the leverage borrow can also be very profitable.

The final strategy is concerning liquidity provision for automated market, making decentralized exchanges.

This one is also quite simple to explain, first of all the assets will be provided as liquidity in an AMA pool and transformed into interest bearing assets LP tokens.

177

00:35:39.150 --> 00:35:55.560

Jiahua (Java) Xu: LP token holders are entitled to collect exchange fees, as discussed and also they're entitled to collect native reward tokens over time and then, finally, the liquidity provided can be withdrawn whenever needed.

in this simulation we see that liquidity provision can be lost, generating. Well, this is because, by nature, more valuable assets will always be traded out, whereas less valuable assets will always be traded in so depending on the direction of liquidity trade.

So, depending on the market movements if more non denominated assets are being sold into the protocol and more nominating assets in our case die.

189

00:39:24.810 --> 00:39:34.560

Jiahua (Java) Xu: which is equivalent to USD is taken out of the pool, then the entire liquidity pool value will decrease denominated in day.

190

00:39:35.760 --> 00:39:50.880

Jiahua (Java) Xu: Then in the entire liquidity pool valued denominated in day will decrease, but of course governance token, but of course rewarded governance token can be used to compensate for this kind of loss but depending on.

191

00:40:07.710 --> 00:40:14.070

Jiahua (Java) Xu: But of course the rewarded governance token can, to some extent also compensate for this type of loss.

Of course, the reward governance token can, to some extent compensate for this type of loss.

On the other hand, if more non denominated assets are being bought out from the pool and more denominated assets in our case die i've been put back into the pool, then the total value of the liquidity poor denominated in day will increase.

let's summarize.

As we have seen in our simulations there are risks associated with your farming, it is not always revenue generating, it is not always yield generating sometimes the API can be negative.

198

00:41:48.900 --> 00:42:07.680

Jiahua (Java) Xu: So what are the risks associated with your farming.

First of all, the risks associated with lending and borrowing, which includes liquidity risk and liquidation risk with liquidity risk.

liquidity risk is associated to low demand on the side of borrowing if there's low borrow demand than the.

then course if there's lowball demand then correspondingly the lending interest will also below the second risk is associated to liquidation risk.

The second risk is associate with liquidation risk, as we have shown some your farming strategies also involve borrowing from lending protocols and when there is severe market movements high market volatility, then there is a risk that the deposit collateral is.

Then there's a pause but then there's a possibility that the value of deposit then there's a possibility that the value of the deposits that act as collateral is insufficient to collateralized the value of the loan such that the deposits will be liquidated.

Then there are compatibility risks so first we have individual small contract risks, of course, where contracts are composed by humans and humans make mistakes.

208

00:44:17.460 --> 00:44:35.100

Jiahua (Java) Xu: So individual contracts, they would have vulnerabilities but secondly multiple contracts when they work together, they can also generate new vulnerabilities that do not exist when we look at smart contracts individually.

And lastly, there is return or API instability this that kind of.

This can be caused by multiple this can be caused by multiple factors, first with automated market, making decentralized exchanges, there is divergence loss which is.

There is divergence loss or in permanent loss on the side of liquidity providers, which has caused due to the market movement of tokens supplied.

Then there's no trading activity low trading activity would be associated with low fees connected that would have a negative impact on the annual percentage yield.

And then there is a price fluctuation in liquidity incentives in our case governance tokens as the simulation shows when the governance talking value is low.

That would result in a low API and when the governance token value is high, the high API will be generated but price fluctuations in these kind of reward tokens would indeed result instability of annual percentage yield.

: And last but not least, there is uncertainty on high yield sustainability as we've seen a large part of the yield relies on.

Governance token reward or the incentive plan of different protocols and at some point if protocols cease to distribute incentive tokens then that yield would also drop.

Here I would like to show empirically the performance of some existing your farming protocols, especially yarn finance harbor finance and idle finance.

You can see that in most cases the yard farming poor as a ever increasing value through time, but in the case of hyper finance in the middle chart.

In the vault that's called USDC volt there's a large shop immediately after the initiation of the poor, this is due to a flash law attack that occurred on harvest and that's associated to the possibility risk that we discussed in the previous slide well alone is related to.

As the attacker utilizes as the attacker as then Tucker as an attacker took advantage of the flesh on feature of a lending protocol to perform the attack on harvest and.

They are

numerous established and emerging yield phone and protocols out there and it's impossible for me to cover every single one of them.

But here, just as one example I like to show an emerging your farming protocol that demonstrates the trend and developments directory of the yield farming field. Bank of chain is a smart multi chain your optimizer that provides think of cheating is a smart multi chain yield optimizer their claims to provide long term risk free return.

Here you can see that multi chain cooperation is definitely a way forward, as in this example bank of chain as incorporated several ebm ethereum virtual machine compatible blockchains including if you're into self b&b chain and Polygon.

Risk risk free or low risk has also become an attractive feature, for your farming protocols as we've seen in

the previous example with harvest and the tag of such a scale will be detrimental to your farmers so with bank of change only selected protocols are so with bank of chain only selected vetted audited protocols are incorporated.

In our paper we cover a few more protocols and you are more than welcome to have a read.

This is the end of my presentation, thank you very much for your attention, if you have any further questions feel free to let me know. And these are the references that appeared in this presentation.