hello,

vitalik dropped an interesting article about possible negative externalities that could come from restaking.

let's discuss about what are, in my opinion, the 2 main risks of eigenlayer, how to deal with it and what could/will be done to minimize them :

1- improper slashing : worst scenario could be a lot of ETH is restaked in one service, restakers behave correctly but slashing gets triggered due to a contract bug (malicious or not), a lot of honest restakers would lose their stake and put the ethereum protocol at risk.

this would be terrible for Ethereum, in order to avoid this type of situation, there will be a veto committee, we can imagine reputed ethereum members from layer 2s teams, flashbot, people similar to ethereum core devs, and deep distributed system builders as part of this committee. the only thing this committee could do is veto a slashing, nothing else, in fact in order to trigger slashing on eigenlayer, it will go through 2 steps : a) trigger slashing contract written in the evm and b) be approved by the committee

what's likely is that first services building on eigenlayer will depend on this committee. one can imagine services building on eigenlayer without depending on this committee but it will be harder to attract restakers, i mean this committee will represent like a backstop for restakers so they can opt in without being scared of improper slashing… at the end of the day, we are not at a stage where we are 100% sure that each contract does what it says but it will come (i hope) …

« but ser, this means that both restakers and services will be trusting this committee and this could be messy »

you make a good point, in fact we could imagine that a dao or eigenlabs will elect this committee. at launch restakers will have to trust that this dao will make sure that as long as restakers are honest, they cant get slashed. services will also trust this dao in the sense that they will trust the fact that the committee will only veto illegitimate slashing because if it veto legitimate slashing then the service is not secure …

now we have seen the initial condition, after that we can imagine this committee could change in the future …

even if it's a dao, it won't be based on a token where if you buy 50% of the supply, you can take control of eigenlayer, and do whatever you want …

now suppose there are changes within this committee, there will be a lag, i mean maybe 1 month before the new committee gets actuated …

if restakers or services don't like it, they are free to leave it but something important to keep in mind is the incentives for the eigendao or even eigenlabs …

aka making sure that nobody leaves and build a committee that can/will be trusted in order to attract more and more people …

we can even compare it to layer 2s that also have a human subjectivity layer for governance upgrades, it's an interesting topic as well …

this will be very important and useful, specially in the early days, it requires time before a protocol ossifies, same for eigenlayer …

2-overleveraged scenario

for this one the best way to start is to make a comparison with the ethereum protocol …

ethereum has ~20B at stake and is securing ~400B worth of dapps so we could say that ethereum is overleveraged by 20x and it turns out it is okay anons, don't you think ?

if you want to find more about it, i invite you to check this thread :
https://twitter.com/samnotmissing/status/1635385633647788032?s=46

but as you can find it on eigenlayer whitepaper, there might be dangerous scenarios, let's take an example :

suppose a service requiring economic trust has 2M of TVL and is secured by 8M at stake run by only 3 operators … well, even if operators collude they would still lose 50% of their stake aka 4M to get only 2M so looks like the crypto economics of this service are

.

now suppose there are 10 services with 2M TVL and still the same 3 operators putting 8M at stake to ensure the security of these 10 services …

now the total profit from corruption would be 20M and the amount slashed/lost would still be 4M so all the services are at risk and the operators could make a profitable attack …

note that as mentionned in the whitepaper, eigenlayer doesn't expect the ethereum protocol to create hardfork if some eth validators behave badly in different middlewares …

but still, this is not acceptable so what do to avoid this situation ?

on v1, looks like eigenlayer will provide a dashboard for services. this mechanism will help services to detect if some operators are in a position to collude (e.g small number of same operators restaked on many services) and make an attack hurting many services. eigenlayer, by helping services to be aware of this type of situation, make it possible for services to only accept operators/restakers that are restaked in a few number of middlewares in order to don't let the attack happen. one way to think about it is you get like elasticity on eigenlayer depending on the number of actively validated services and number of operators …

on v2, afaik, eigenlayer plans to let services buy insurance against slashing like bonds.

let's consider 20B restaked eth secures services on eigenlayer, if slashing happens on 10 services, services will ask where is that slashed money going to go to ?

turns out a middleware will have the possibility to pre-bought insurance bonds :

suppose you are a bridge and you restrict the value flow by not transacting more than 1B per day and it takes you 1 day to detect an attack, it could make sense to pre-bought 1B of insurance bonds.

this could then be sold considering the particular slashing priority that you get so you have the guarantee of that amount from the slashing insurance bonds, no matter what happens next.

by doing it, would also bring more security for the users of the bridge since they know that even if something bad happens, their funds are safe.

to conclude, even if it will probably not be the case in the early days, my humble opinion is that the best thing that could happen is to get all ethereum stakers restaked on eigenlayer …

might sound counterintuitive but would be much harder to attack the ethereum ecosystem in general, to make my point clearer let's use a well known analogy aka blockchains as nation state and dapps as cities …

to ensure the security of cities (dapps), nation state (ethereum) should secure the entire country and not only the frontiers (ethereum blocks) … what if you get an air attack (oracles, chain link goes down what u doing ?) or what if there are attacks coming from the ocean (bridges, data availability ?) …

this is the "endgame" mental model that makes the most sense imho because if all staked eth is restaked to secure all of this middlewares with objective slashing conditions for some services and eventually no slashing conditions for other services only accepting decentralized restakers, what you get basically is :

-pool/sharded security

-open innovation

-the growth of eth in value as it did in the early days when ethereum separated trust from innovation for dapps …

happy to start the discussion here, hope that makes sense and looking forward to discuss with all of you !