Non-linear bond

as sybil attack resistance mechanism

Idea & assumptions:

Within risk framework provided in Risk assessment for community staking one of the risks explored and evaluated is *EL rewards stealing - malicious actor reroutes EL rewards for personal address.*

As possible rewards for performing such an action are highly volatile and could well exceed any reasonable amount **no level of bond could prevent it, but with greater bond risk exposure decreases.**

As one entity (Node Operator - NO) could control more than one validator, pooling up bonds for all validators controlled by this entity would increase available capital for mitigation, but to avoid that “Sybil” behaviour by malicious actor could be chosen - to explicitly open up opportunities for exploiting EL rerouting.

Within this paper I’ll provide an approach exploring the possibility of incentivization transparency for NO in terms of connecting all related validators within one entity by reducing the required bond per validator

Base assumptions:

- Permissionless entry with bond
- Triggerable exits
- APR = 4.5%
- EI rewards structure identical to observed from beginning of 2023 to October 2023

EI stealing strategy valuation:

As a first step within this research, I'll provide a valuation of possible returns on performing EL-stealing strategy.
Model conditions for actor behaviour simulations would be:

- 820 000 Total Validators (~3.2 proposals per validator a year)
- 4 ETH bond with 32 ETH provided capital
- 90% commission of all rewards on bond
- 7.5% commission of all rewards on provided capital

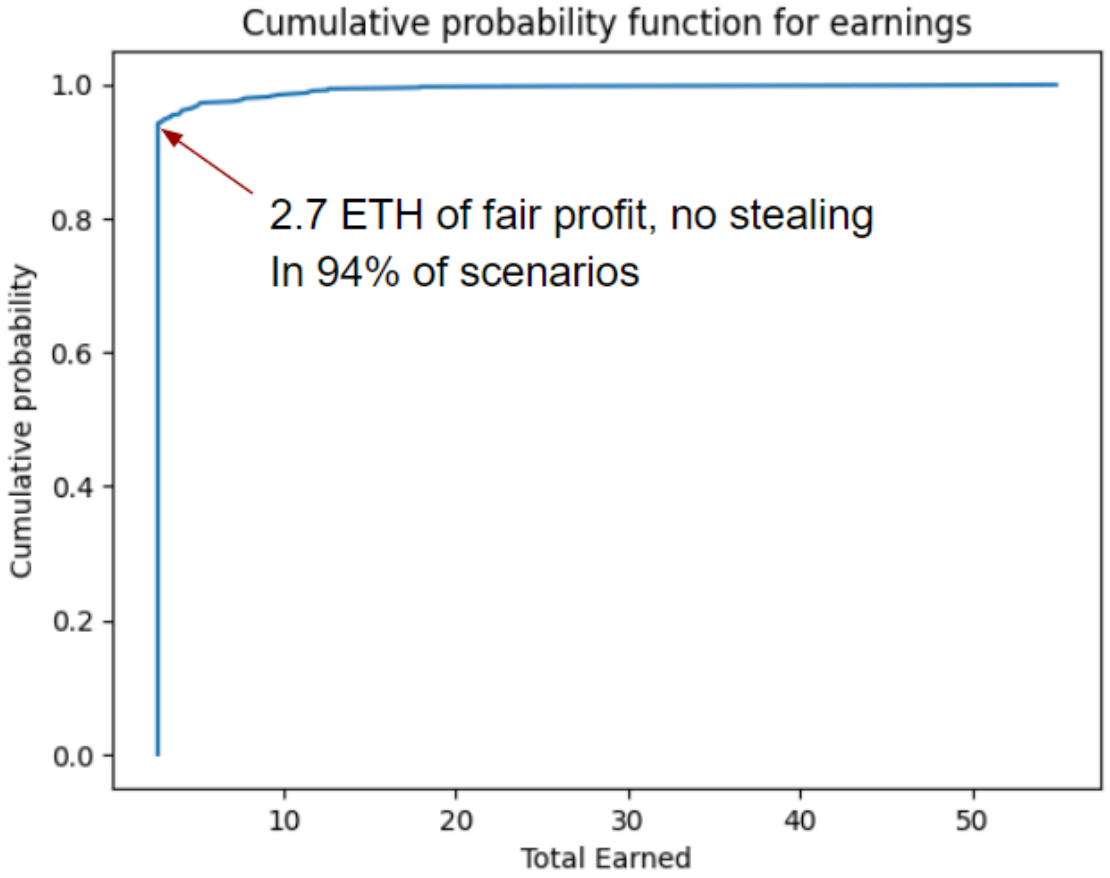
Within this assumptions, **expected return for non-stealing strategy would be:**
4.5%*(90%*4+7.5%*32) = **0.27 ETH per year.**

Stealing strategy assumes:

- Stealing any block rewarding more than bond value (4 ETH)
- Getting bond reduced to zero, and immediately exiting validator after performing an attack

- Immediately re-entering validator after exit (due to Permissionless entry)

As EL rewards are random, returns on such a strategy are random by nature too. Simulating 1000 scenarios of performing this strategy for 1 year for an actor with 40 ETH of capital (10 validators), corresponding distribution of possible earnings is created:



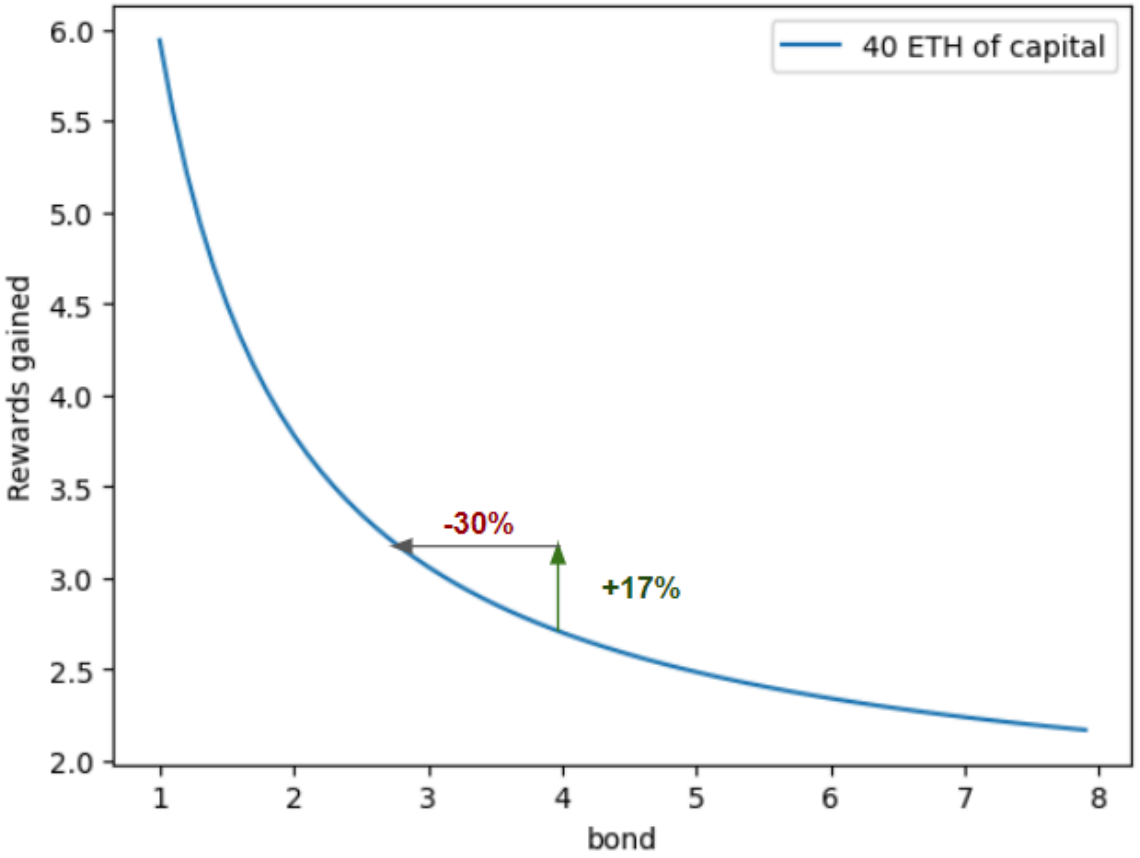
For the majority of simulations (94%) this strategy doesn't lead to EL rerouting events (due to the extremely rare nature of blocks valued more than 4 ETH), but for remaining 6% earnings from executing such a strategy may lead to magnitude higher rewards.

Moving from simulations to expected values based on EL rewards distribution:

- Expected profit from stealing: **0.046157 ETH** *(excess over 2.7 ETH for running 10 Validators with non-stealing strategy)*
- Expected edge on stealing: **+17.1%** *(relative excess over non-stealing strategy)*

Corresponding bond discount:

For **rational and risk-neutral actor** to incentivize non-Sybilling return on reduced bond should be equal or more than expected return on MEV stealing:



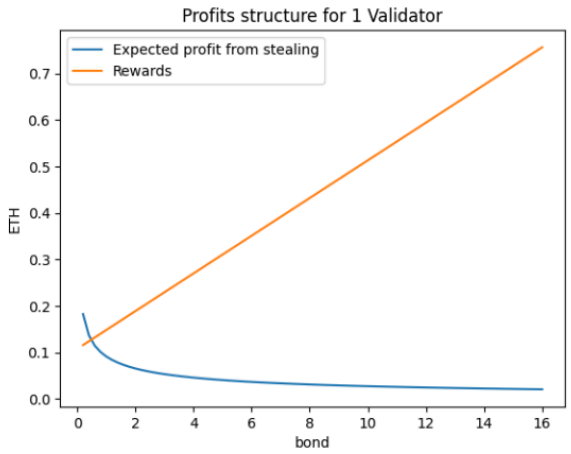
Providing **17.1%** increase in rewards would require **30% reduction on bond value** (4->2.8). The reasons for such a drastic decrease are:

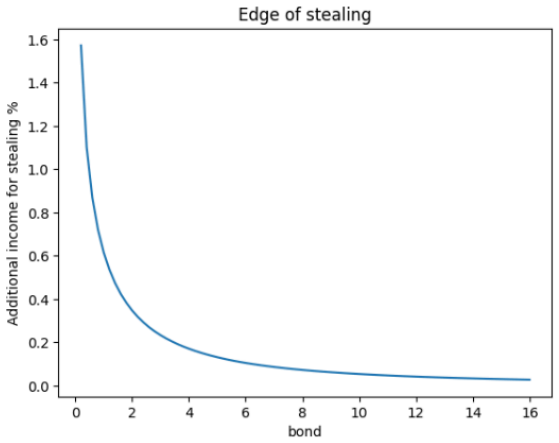
- 60% of total rewards for non-stealing actor comes from bonds
- Lowering bond with constant capital would affect only remaining 40% rewards from running a validators

And this effect is constant on actor capital as total rewards for non-stealing strategy are linear on capital and edge for performing Sybilling and stealing strategy (17.1%) is constant.

Sybil-resistant bond discount curve:

In this section i'll explore corresponding bond discounts to incentivize non-Sybilling for different bond values



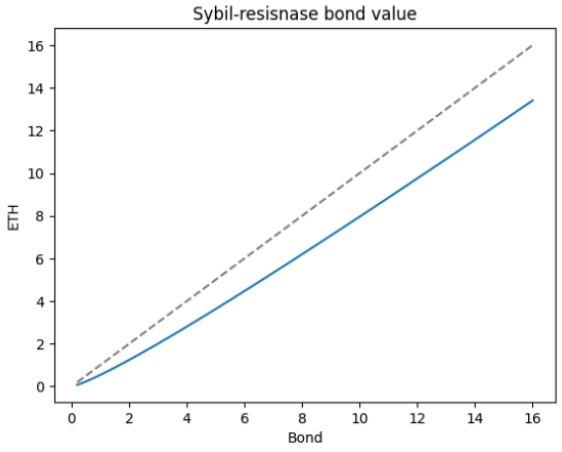


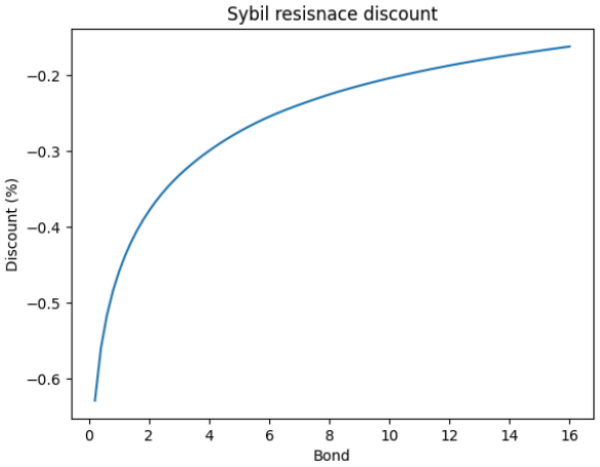
Rewards on one validator: ~0.1 ETH for provided capital + rewards on bonded capital
Incentives for stealing grows dramatically with lower amount of bond corresponding with EL structure

Therefore, with lower *base* bond value there are two opposite effects:

- Edge of stealing strategy increases, as probability of getting a block with rewards exceeding bond value grows
- Discount in bond to provide increase for in non-stealing strategy increases as lesser share of total rewards corresponds to bonds

Combining this effects together:



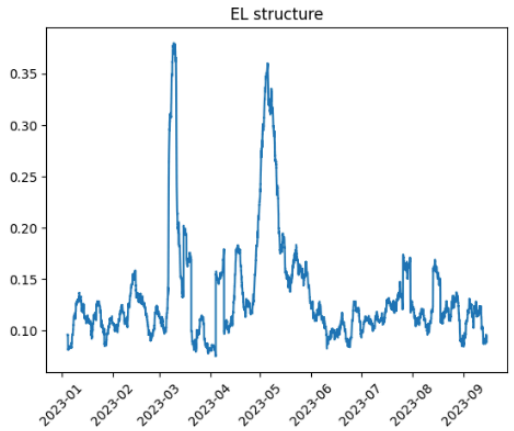


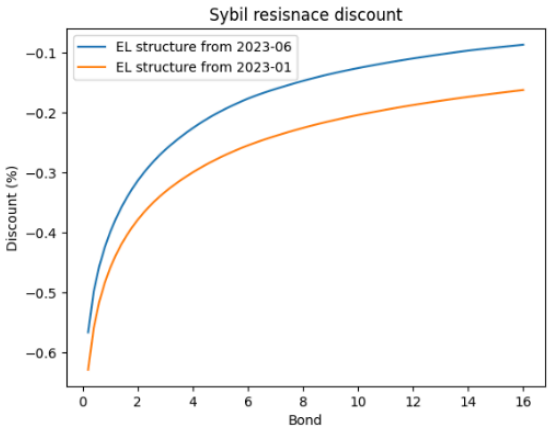
The first one outweighs the second - with lesser initial bond, greater discount provides same earnings for non-stealing strategy as stealing & Sybilling.

Conclusion

Non-linear bond could function as a mechanism to prevent Sybilling and EL-stealing strategies, but require drastically high reduction in bond per validator to offset expected returns on performing stealing strategy, so it should be considered, but not as determining factor to prevent EL stealing

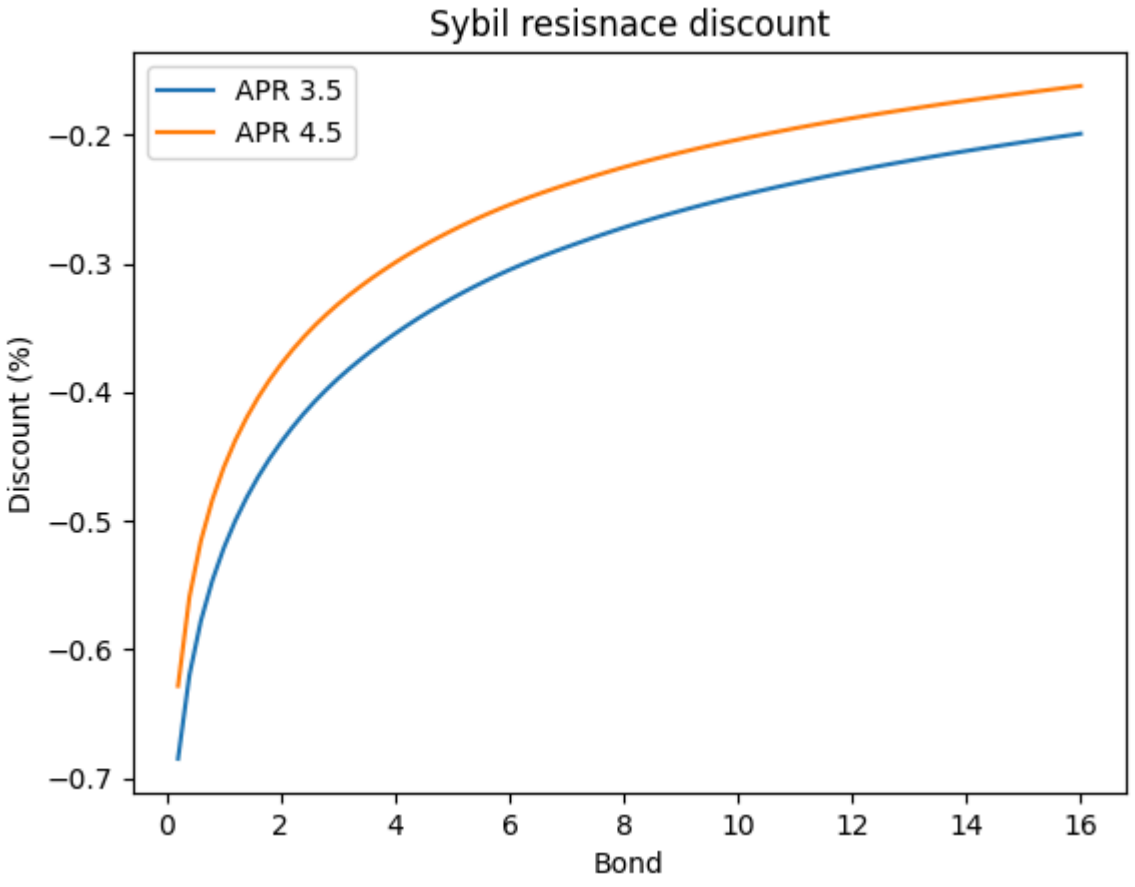
Appendix A: EL structure assumption effect





Assumptions on EL structure change the level of the curve, but doesn't change magnitude

Appendix B: APR assumption effect



The lower the APR - the more discount for bonds should be provided to compensate and edge for MEV stealing

Specifically, it depends on the relation between CL APR and EL APR (represented by assumption on EL structure)