Gauntlet

How much security does your restaking protocol *really* need?

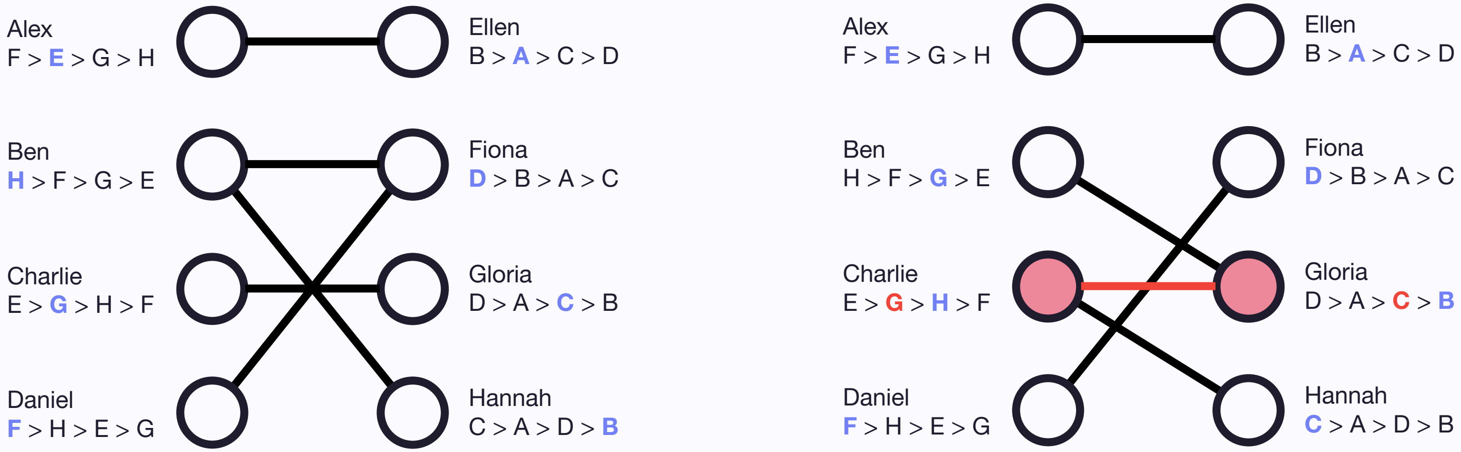
Scaling laws for security

Tarun Chitra | Devcon Bangkok | November 14, 2024

A Tripartite Tale

1. Restaking is a decentralized matching market
2. Threat model determines economic security
3. Minimum amount of security to pay for can be quantified by cascading risks

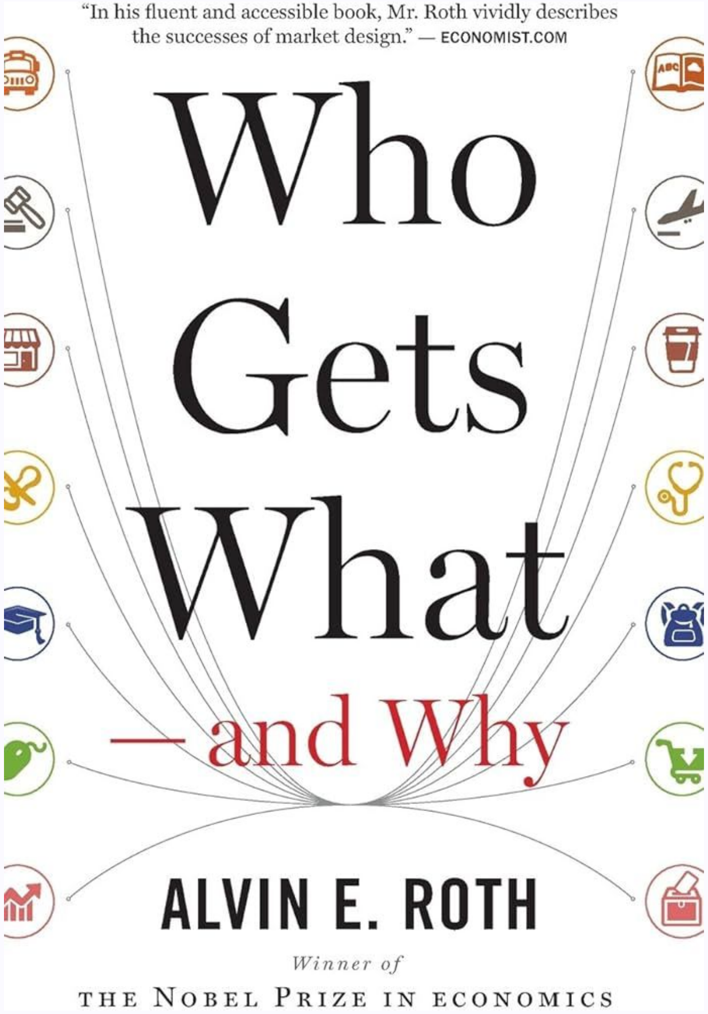
Act I: Matching Markets & Restaking



What is a matching market?

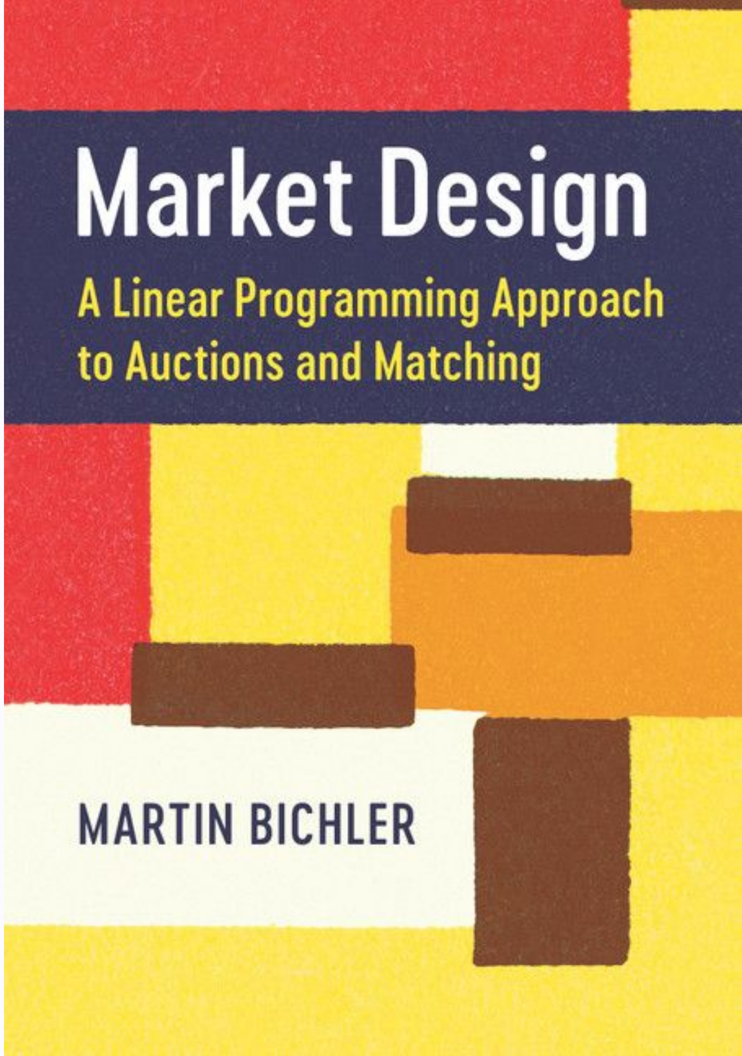
- Matching markets are everywhere
  - Kidney exchanges
  - Hospital <> Resident matching
  - Dating apps

- Main idea:
  - Supply: Inhomogenous goods (with some shared properties)
  - Demand: Buyers with constraints on what they can buy (i.e. kidney compatibility)



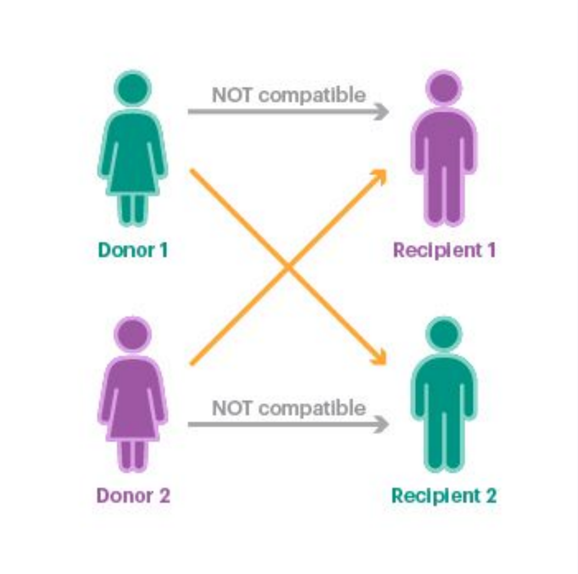
Matching vs Auctions

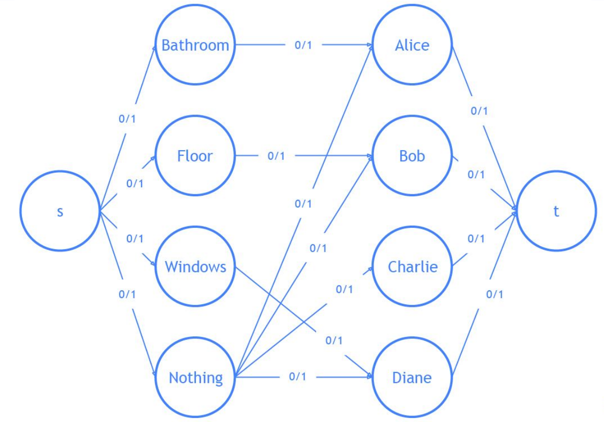
- Auctions focus on maximizing profit for the seller or welfare of both the buyer and seller
  - i.e. Good outcome for the seller to sell only 1% of their goods if it is revenue maximizing
- Matching markets are focused on maximizing matches and stability to perturbations vs. pure profit
  - Allows for mechanism design without money
  - e.g. Stable Matching Theorem
- Crypto has both: MEV auctions vs. intents (matching)



Matching Markets & Graph Theory

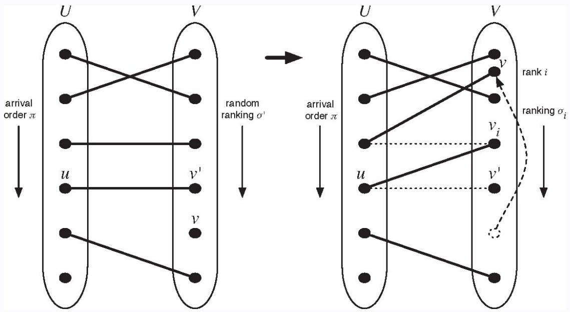
- Natural representation of a matching market is as a bipartite graph
  - One bipartition is the supply side, other is demand
- This graph is
  - Static (i.e. fixed ahead of time)
  - Has a central planner (i.e. National Kidney Registry) chooses the allocation or matching
- Decentralized matching markets don't have either of these features — parties utilize incentives to learn an (approximately) optimal matching





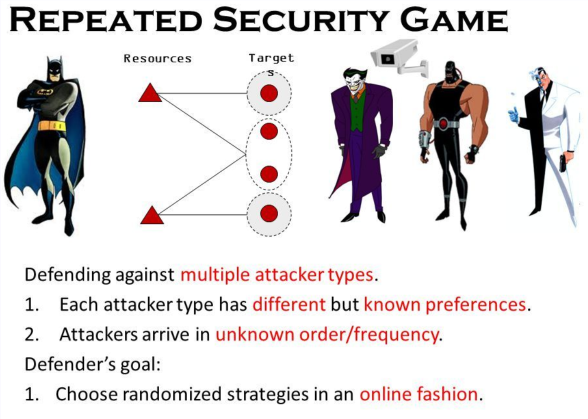
Restaking is a Decentralized Matching Market

Why are decentralized matching markets so much harder to analyze?



Permissionlessness means you can be ‘unmatched’ with as people join and leave at will

No central planner → Rely purely on incentives to reach equilibria



Requires explicit adversarial model

Act II: What is economic security?

toly @aeyakovenko

> Security would plummet. Without Ethereum's robust validator network, the L2 would rely solely on its own, leaving it far more vulnerable to attacks.

Please actually define a real attack vector instead of just parroting "economic security" meme. What attack? A double spend? Invalid state transition?

6:39 AM · Nov 3, 2024 · **1,548** Views

4 · 7 · 1

Sreeram Kannan @sreeramkannan · Jun 10

Tl;dr on **economic security**.

——————-

Economic security is NOT a metric of cost to attacker.

Economic security is a measure of the redistribution rights held by the protocol.

If a cex attacks the protocol it loses its clients money and it is redistributed to the protocol users.

Show more

> **toly** @aeyakovenko · Jun 10
>
> Replying to @llamaonthebrink
>
> It's not! A management change at cb/binance/lido can impact liveness. It's a cost to honest operators to acquire enough stake to guarantee liveness. But attacker can cause a liveness failure for much less.

3 · 20 · 135 · 62K

vitalik.eth @VitalikButerin · Jun 10, 2022

Replying to @kevinsekniqi @Corpetty and 2 others

Because the level of **economic security** is much higher when attackers can lose not just potential gains but also their principal.

27 · 70 · 173

Quantifying Economic Security in PoS

Defining economic security in an *absolute* sense is difficult, e.g.

- MEV complicating attack profit
- Enumerate the attack space
- Consider competitive pressures for stake
- Capital and temporal costs for executing the attack

But the cost is *generally* linear in the discounted numéraire (e.g. stablecoin) value stake

Minimum percentage of stake needed for an attack

Expected time to execute attack

$$\text{Cost of Attack} = \mathscr{C}(t) \geq C e^{k\tau} p(t) \Sigma(t)$$

Amount of asset staked

Price in numéraire terms of staking asset

Economic Security for Restaking

Restaking has two competing pressures for economic security

1. 📈: Participants purchase and stake $\delta\Sigma(t)$ to capture excess yield
2. 📉: Slashed stake from AVSs reduces over all network security

$$\mathscr{C}^R(t) \geq Cg(\delta\Sigma(t))e^{k\tau}p(t)(1+\delta)(1-R)\Sigma(t)$$

Price impact function
(i.e. how much does the price go up when people buy of stake and add it to the network?)

Risk Measure
Percentage of stake that is lost under a worst or average case threat model

When is restaking safe?

Restaking can be viewed as safe when the overall network value is non-decreasing, i.e.

$$\mathscr{C}^R(t) - \mathscr{C}(t) \geq 0$$

$$\Updownarrow$$

$$Ce^{k\tau}p(t)\Sigma(t)\Big(g(\delta\Sigma(t))(1+\delta)(1-R)-1\Big) \geq 0$$

$$\Updownarrow$$

$$R \leq 1 - \frac{1}{(1+\delta)g(\delta\Sigma(t))}$$

Dependence on dynamic elasticity
of borrowers to incentives
(e.g. points, tokens, fees)

Brief Detour: Comparison with Rollups

Rollups have a number of economic trade-offs for Ethereum

1. Execution, MEV revenue usually go to the L2 sequencer
2. DA revenue dwarfed by execution revenue

Q: When does revenue from *n* rollups breakeven with monolithic L1 revenue?

A (C & Pai, 2024): *n* rollups need at most $\Theta(n^2)$ more revenue

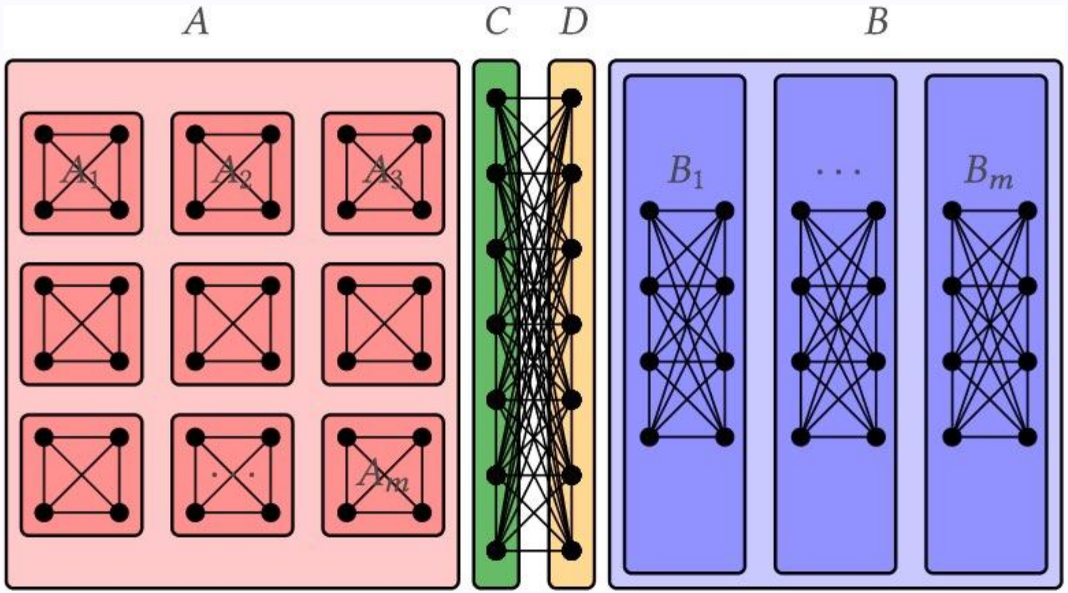
Q: When does revenue from *S* AVSs compensate for restaking risk?

A (C & Pai, 2024): *S* rollups need at most $\Theta\left(1 + \frac{1}{S^{3/2}}\right)$ more revenue

Question:

Can we model restaking risk the network *without* price or stake dynamics?

Act III: Restaking Graphs, Cascades, and All That

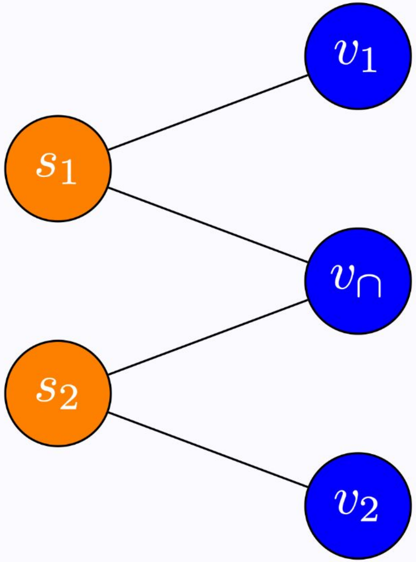


Restaking Graphs

α π S V σ

$\sigma_1 = 1$

$\alpha_1 = \frac{1}{3}$ $\pi_1 = 1$



$\sigma_\cap = 5$

$\alpha_2 = \frac{1}{2}$ $\pi_2 = 1$

$\sigma_2 = 1$

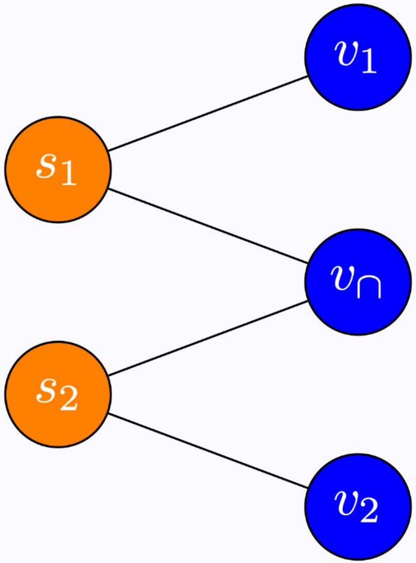
Restaking Graphs

Node Operators

α π S V σ

$\sigma_1 = 1$

$\alpha_1 = \frac{1}{3}$ $\pi_1 = 1$



$\sigma_\cap = 5$

$\alpha_2 = \frac{1}{2}$ $\pi_2 = 1$

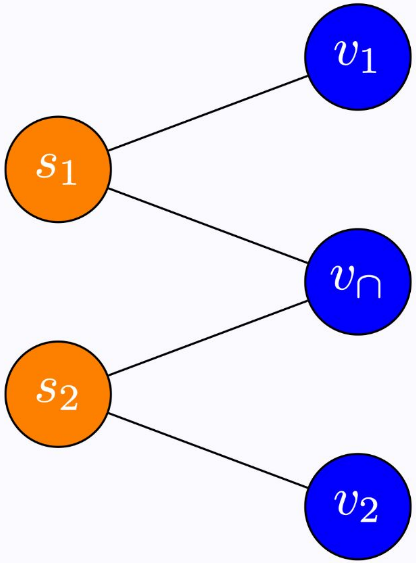
$\sigma_2 = 1$

Restaking Graphs

Node Operators

α π S V σ

Stake



$\alpha_1 = \frac{1}{3}$ $\pi_1 = 1$

$\alpha_2 = \frac{1}{2}$ $\pi_2 = 1$

$\sigma_1 = 1$

$\sigma_\cap = 5$

$\sigma_2 = 1$

Restaking Graphs

Services (AVSs)

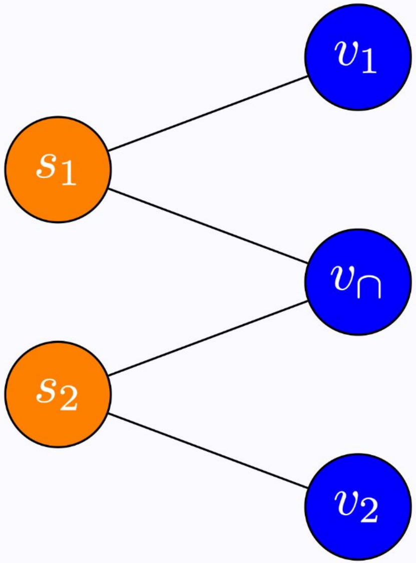
Node Operators

Stake

α $\quad \pi$ $\quad S$ $\quad V$ $\quad \sigma$

$\alpha_1 = \frac{1}{3} \quad \pi_1 = 1$

$\alpha_2 = \frac{1}{2} \quad \pi_2 = 1$



$\sigma_1 = 1$

$\sigma_\cap = 5$

$\sigma_2 = 1$

Restaking Graphs

Services (AVSs)

Node Operators

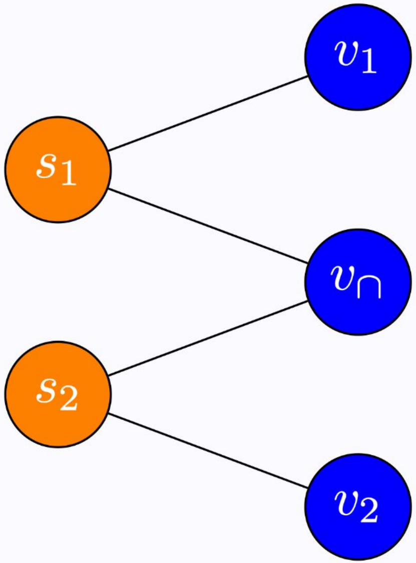
Maximum Profit

Stake

α π S V σ

$\alpha_1 = \frac{1}{3}$ $\pi_1 = 1$

$\alpha_2 = \frac{1}{2}$ $\pi_2 = 1$

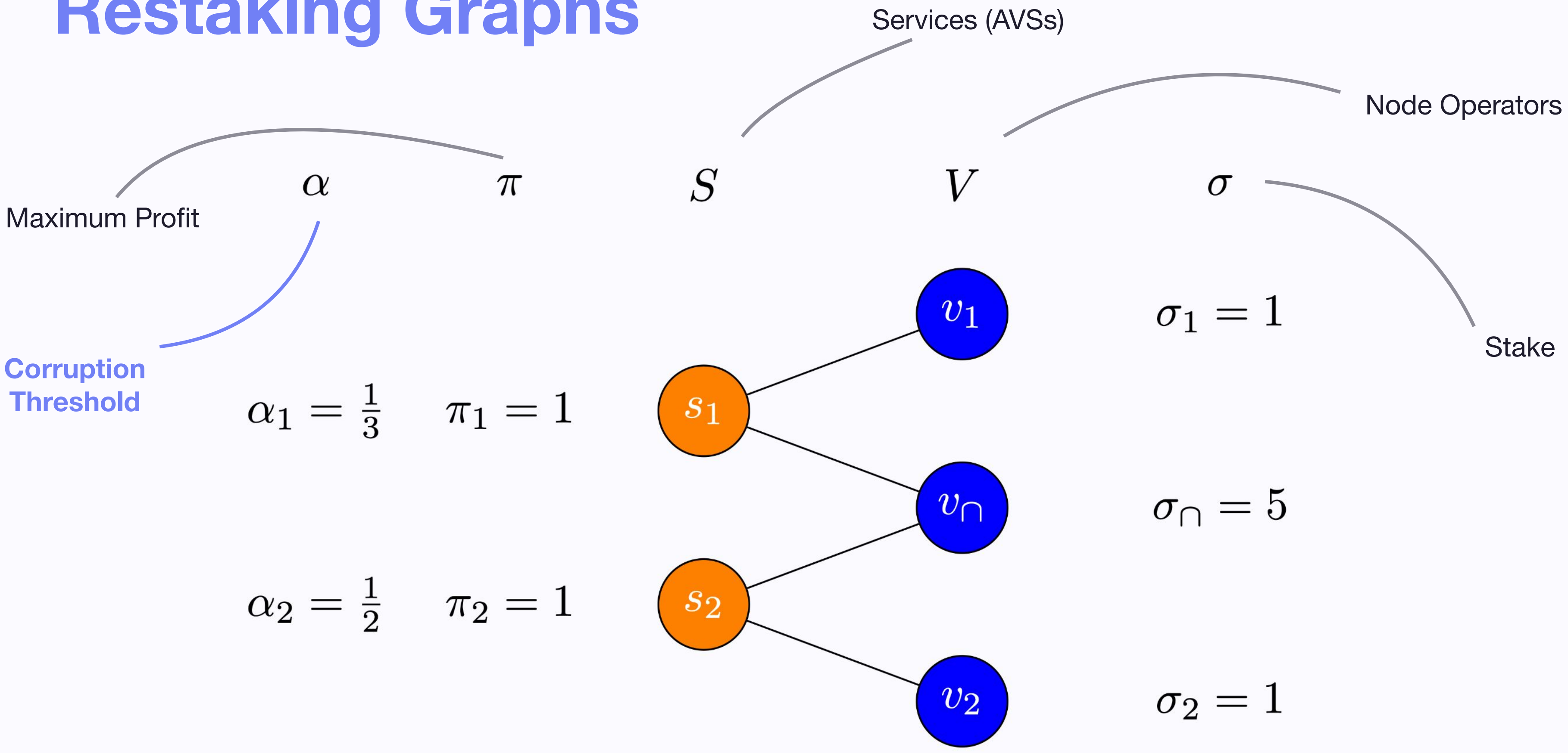


$\sigma_1 = 1$

$\sigma_\cap = 5$

$\sigma_2 = 1$

Restaking Graphs



Restaking Graphs

Services (AVSs)

Node Operators

Maximum Profit

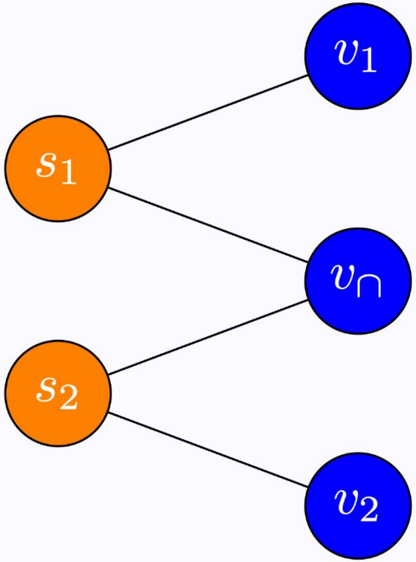
α π S V σ

Stake

Corruption Threshold

$\alpha_1 = \frac{1}{3}$ $\pi_1 = 1$

$\alpha_2 = \frac{1}{2}$ $\pi_2 = 1$



$\sigma_1 = 1$

$\sigma_\cap = 5$

$\sigma_2 = 1$

Operating multiple services with the same stake

Restaking Graphs

Services (AVSs)

Node Operators

Maximum Profit

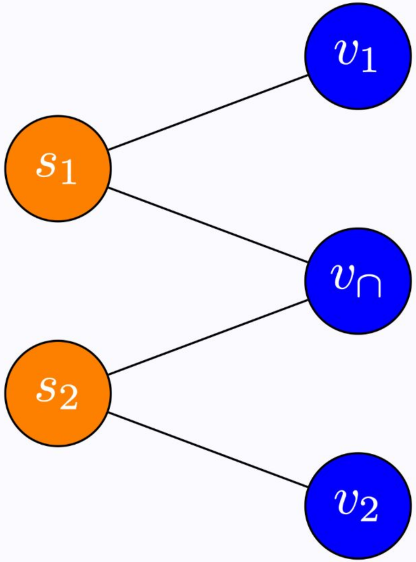
Corruption Threshold

Stake

α π S V σ

$\alpha_1 = \frac{1}{3}$ $\pi_1 = 1$

$\alpha_2 = \frac{1}{2}$ $\pi_2 = 1$



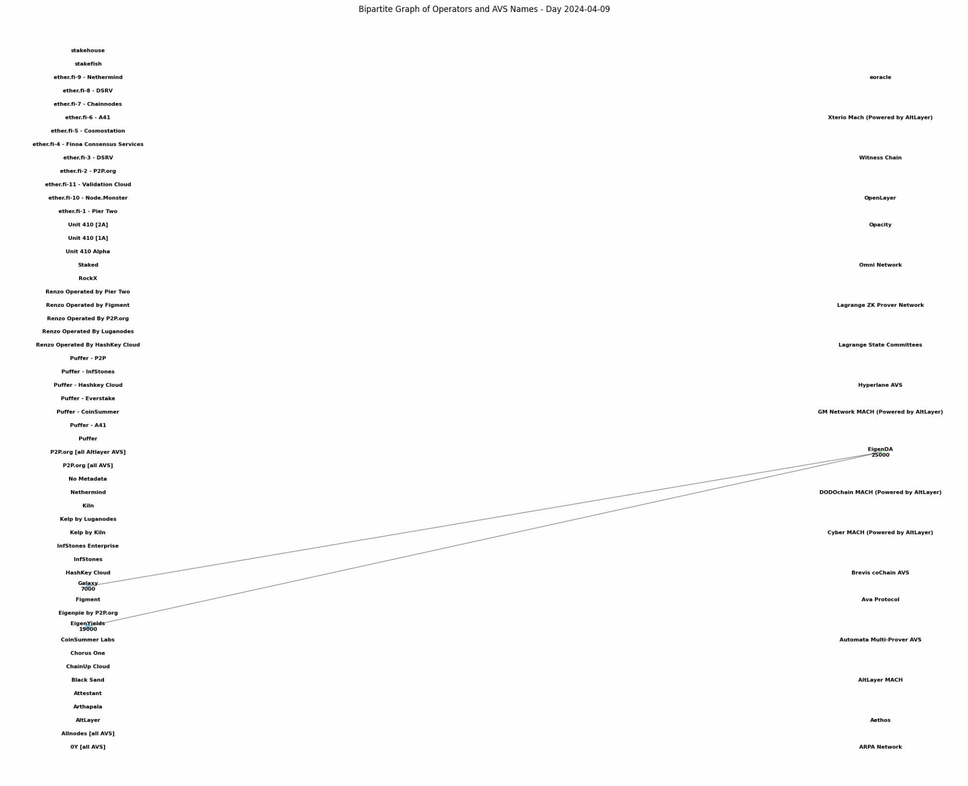
$\sigma_1 = 1$

$\sigma_\cap = 5$

$\sigma_2 = 1$

Operating multiple services with the same stake

Eigenlayer Restaking Graph over Time



Attacking Restaking Graphs

Profitability

Feasibility

Attacking Restaking Graphs

Profitability

Maximum Profit from
Attacking Services $A \subset S$

$>$

Maximum Slashing Penalty
for attacking cartel $B \subset V$

Feasibility

Attacking Restaking Graphs

Profitability

Maximum Profit from Attacking Services $A \subset S$

$>$

Maximum Slashing Penalty for attacking cartel $B \subset V$

Feasibility

For every service $s \in A$:

Stake held by attacking cartel $B \subset V$ that is operating s

$>$

α_s x total stake at s

Attacking Restaking Graphs

Profitability

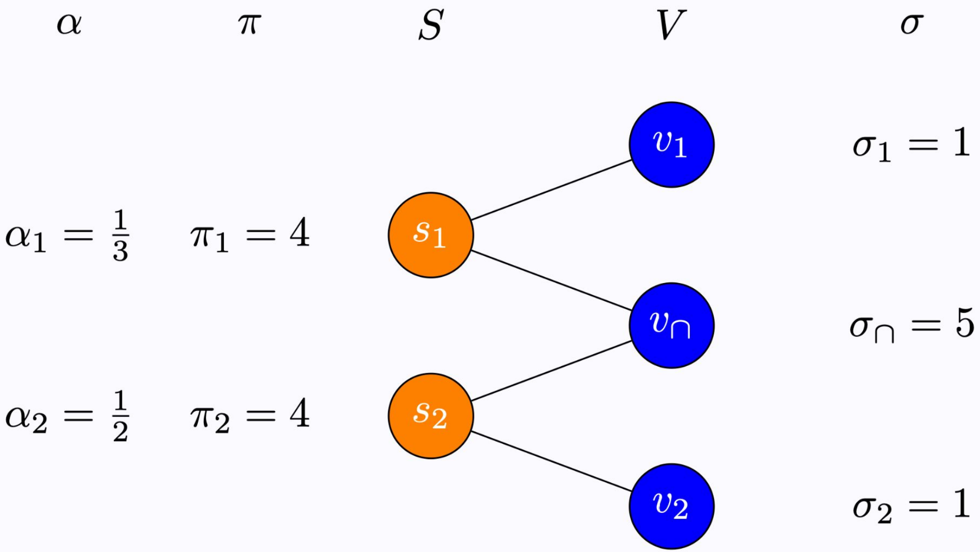
$$\sum_{s \in A} \pi_s > \sum_{v \in B} \sigma_v$$

Feasibility

$$\forall s \in A \sum_{v \in B \cap \partial s} \sigma_v > \alpha_s \sum_{v \in B} \sigma_v$$

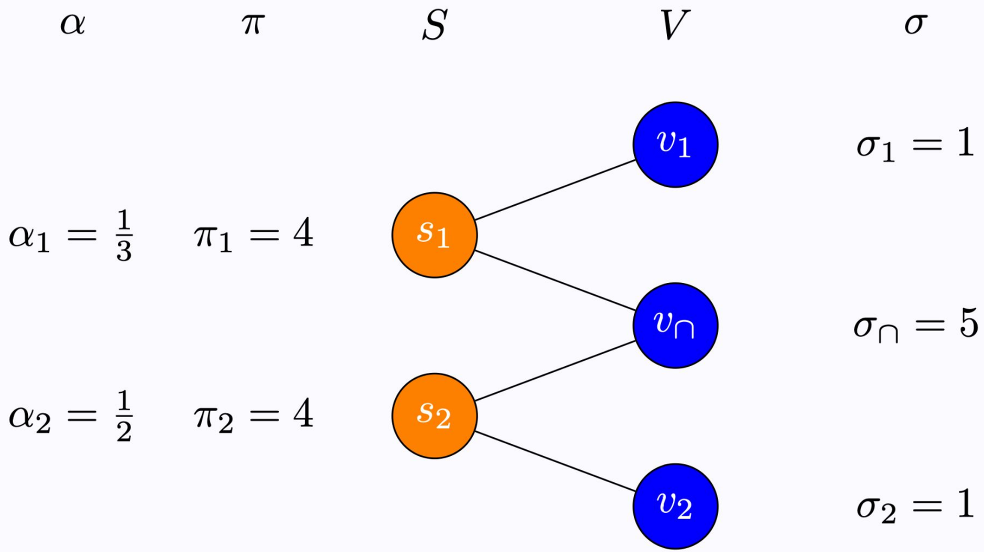
Def. from Eigenlayer whitepaper + Durvasula and Roughgarden, 2024

Attacking Restaking Graphs



Each individual service is over-collateralized in that Profit < Stake at each service…

Attacking Restaking Graphs

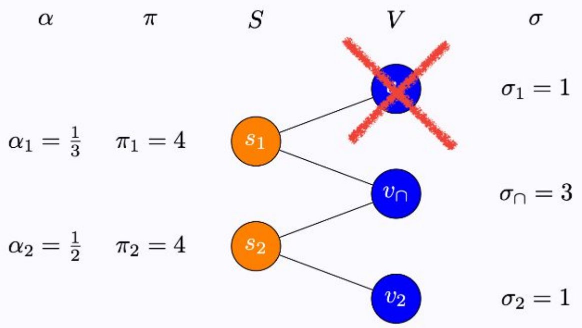


But all of the validators colluding can profitably attack both services:

$$8 = \pi_1 + \pi_2 > \sigma_1 + \sigma_\cap + \sigma_2 = 7$$

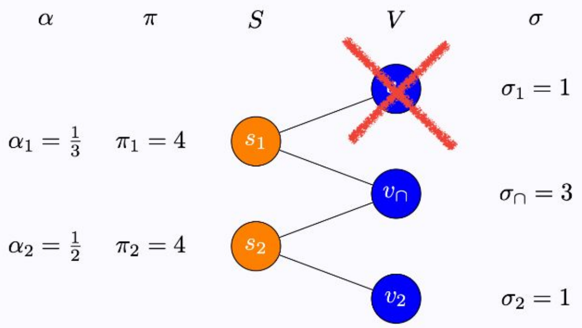
Cascading Attacks on Restaking Graphs

Step 1:
Lose a fraction ψ of stake

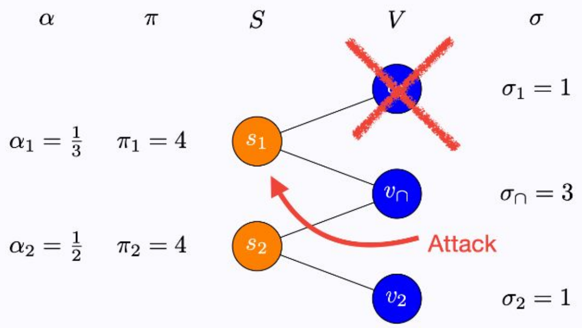


Cascading Attacks on Restaking Graphs

Step 1:
Lose a fraction ψ of stake

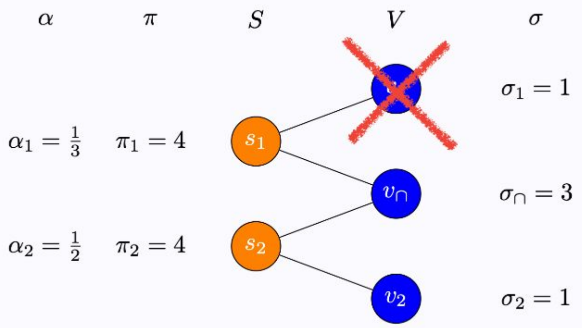


Step 2:
Creates new profitable attacks

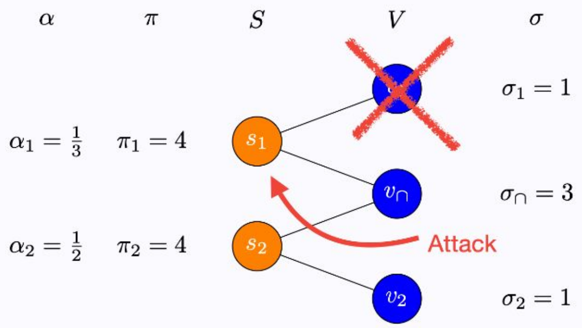


Cascading Attacks on Restaking Graphs

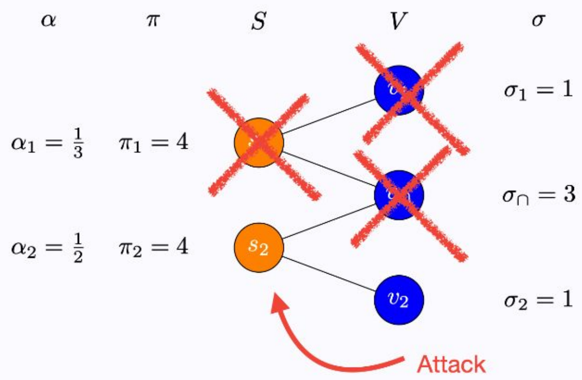
Step 1:
Lose a fraction ψ of stake



Step 2:
Creates new profitable attacks

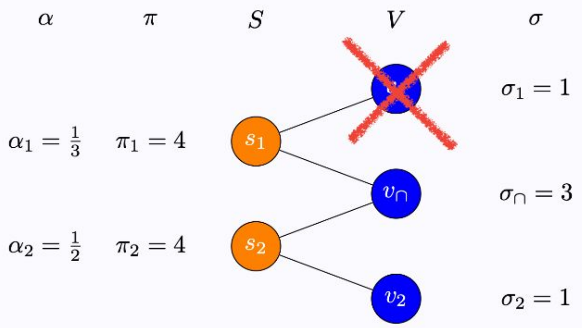


Step 3:
Repeat until no further attacks possible

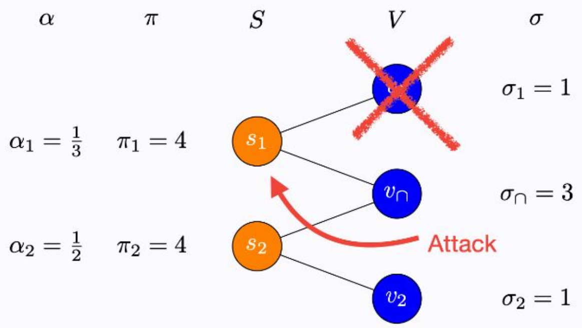


Cascading Attacks on Restaking Graphs

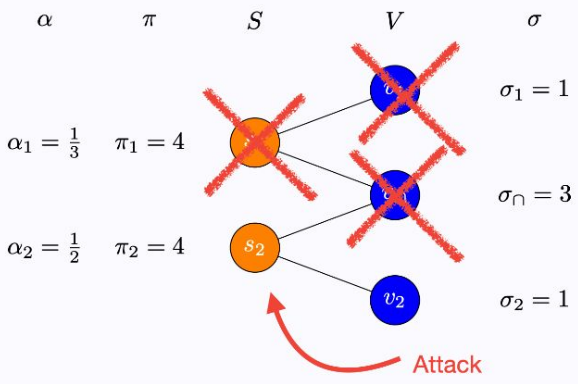
Step 1:
Lose a fraction ψ of stake



Step 2:
Creates new profitable attacks



Step 3:
Repeat until no further attacks possible



This is the PoS version of a lending liquidation cascade

Quantifying Cascading Attacks

$$(A_1, B_1), \ldots, (A_T, B_T)$$

Valid Attack Sequence:

Services ($A_t \subset S$), Operators ($B_t \subset V$) forming a profitable and feasible attack after attacks (A_1, B_1), …, (A_{t-1}, B_{t-1}) executed.

Quantifying Cascading Attacks

$$(A_1, B_1), \ldots, (A_T, B_T)$$

Valid Attack Sequence:
Services ($A_t \subset S$), Operators ($B_t \subset V$) forming a profitable and feasible attack after attacks (A_1, B_1), …, (A_{t-1}, B_{t-1}) executed.

$$R_\psi(G) \quad =$$

Maximum percentage of stake that can be lost due to a cascade attack given an initial loss of ψ percent of stake

(Worst-case version of R in earlier analysis)

Quantifying Cascading Attacks

$$(A_1, B_1), \ldots, (A_T, B_T)$$

Valid Attack Sequence:

Services ($A_t \subset S$), Operators ($B_t \subset V$) forming a profitable and feasible attack after attacks (A_1, B_1), …, (A_{t-1}, B_{t-1}) executed.

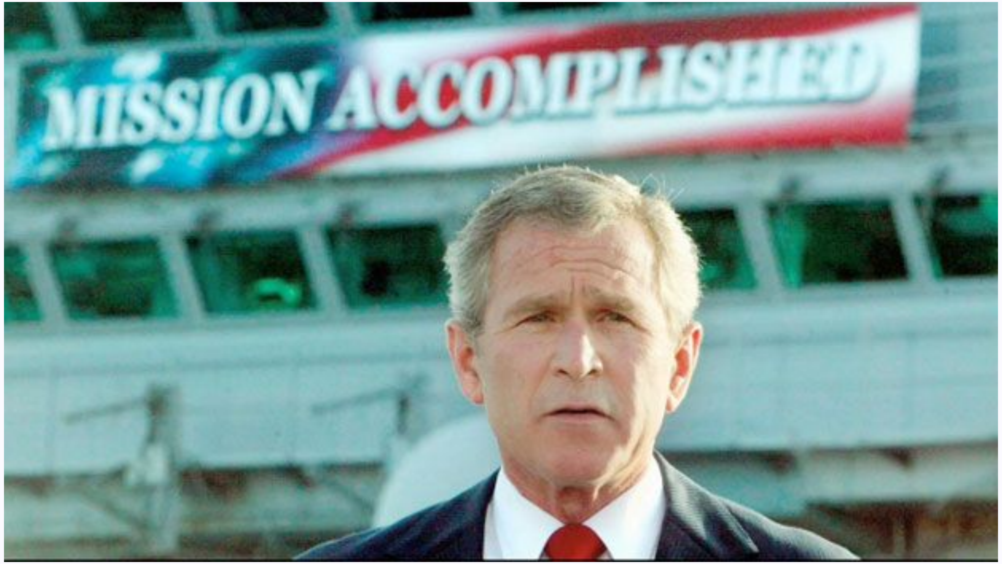
$$R_\psi(G) = \max_{D \in D_\psi(G)} \max_{(A_1,B_1),\ldots,(A_T,B_T)} \frac{\sum_{v \in \bigcup_t B_t} \sigma_v}{\sum_{v \in V} \sigma_v}$$

Total stake lost in attack

Initial Stake in network

Set of validators with less than ψ% of total stake

How much stake do we need to secure an AVS?

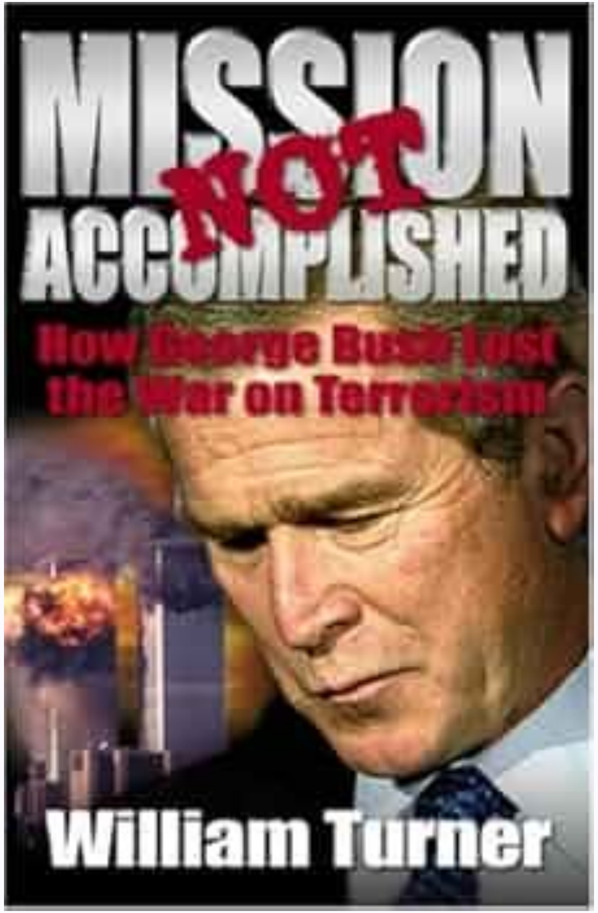


Enough stake σ_v such that $R_\psi(G)$ is smaller than some tolerated amount (i.e. restaking network is willing to lose 5% of stake given $\psi \leq 33\%$)

Bad News

Theorem (Durvasula & Roughgarden, 2024):

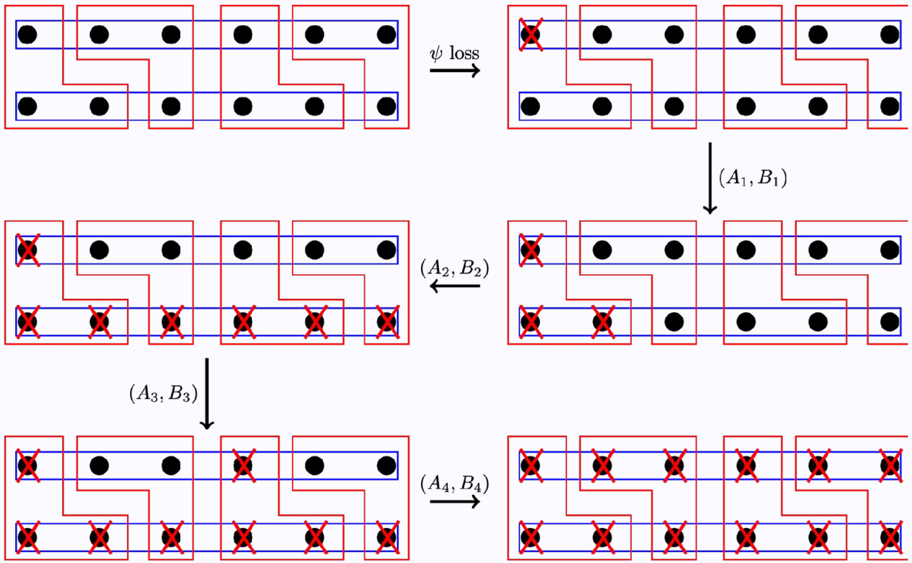
There exist an infinite family of graphs G_n with n validators such that $R_\psi(G_n) = 1$



Bad News

Theorem (Durvasula & Roughgarden, 2024):

There exist an infinite family of graphs G_n with n validators such that $R_\psi(G_n) = 1$



Slightly Less Bad News

Theorem (Durvasula & Roughgarden, 2024):

If a restaking graph G is γ-overcollateralized, then $R_\psi(G) \leq \psi(1+\gamma^{-1})$

Slightly Less Bad News

Theorem (Durvasula & Roughgarden, 2024):

If a restaking graph G is γ-overcollateralized, then $R_\psi(G) \leq \psi(1+\gamma^{-1})$

Translation:

PoS analogue of "Your decentralized stablecoin needs to be sufficiently overcollateralized to avoid cascading depeg events"

Slightly Less Bad News

Theorem (Durvasula & Roughgarden, 2024):

If a restaking graph G is γ-overcollateralized, then $R_\psi(G) \leq \psi(1+\gamma^{-1})$

Translation:

PoS analogue of “Your decentralized stablecoin needs to be sufficiently overcollateralized to avoid cascading depeg events”

But:

Overcollateralization condition is so strong that for many graphs every service is overcollateralized as much as the total profit $\pi_1+\ldots+\pi_S$

Slightly Less Bad News

Theorem (Durvasula & Roughgarden, 2024):

If a restaking graph G is γ-overcollateralized, then $R_\psi(G) \leq \psi(1+\gamma^{-1})$

Translation:

PoS analogue of "Your decentralized stablecoin needs to be sufficiently overcollateralized to avoid cascading depeg events"

But:

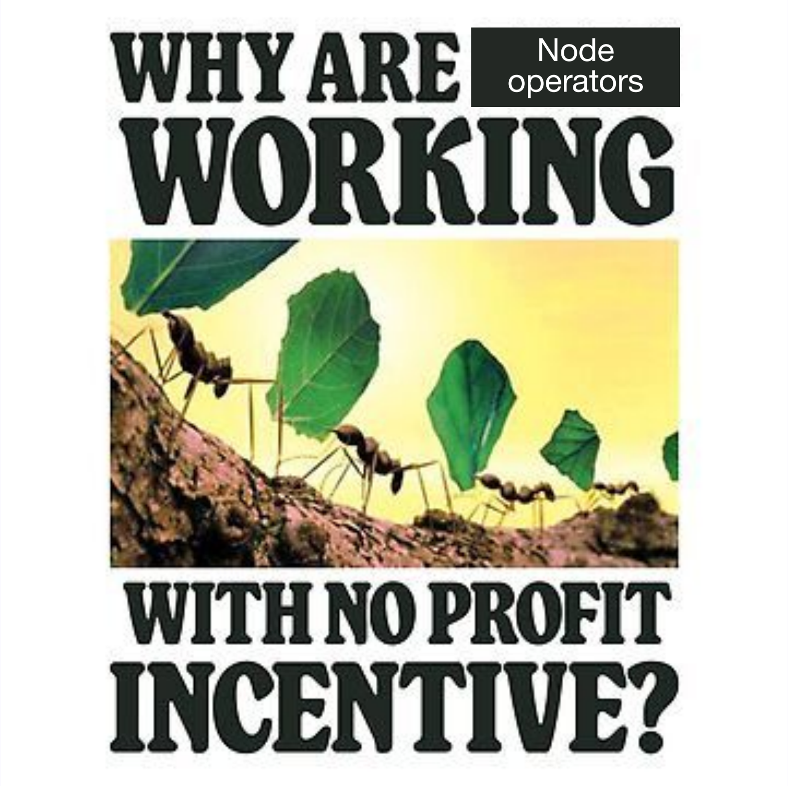
Overcollateralization condition is so strong that for many graphs every service is overcollateralized as much as the total profit $\pi_1+\ldots+\pi_S$

Translation:

Two services with 1 ETH & 1,000,000 ETH of max profit — the 1 ETH service needs to attract 1,000,001 ETH to be secure to cascading attacks (!!!!)

Is this route to pricing AVS security a dead-end?

Act IV: Incentivized Restaking Graphs



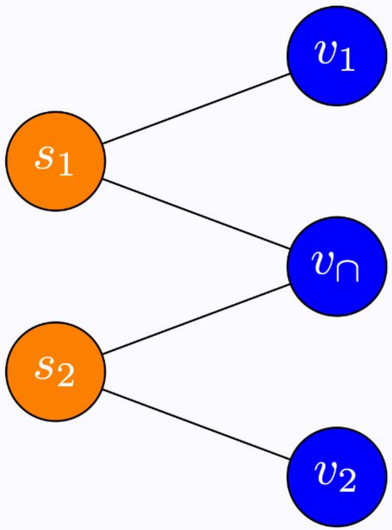
Incentivized Restaking Graphs

r α π S V σ

Rewards/points paid by each service

$r_1 = \sqrt{K}$ $\alpha_1 = \frac{1}{3}$ $\pi_1 = (1+\epsilon)K$

$r_2 = \sqrt{K}$ $\alpha_2 = \frac{1}{2}$ $\pi_2 = (1+\epsilon)K$



$\sigma_1 = 1$

$\sigma_\cap = K$

$\sigma_2 = 1$

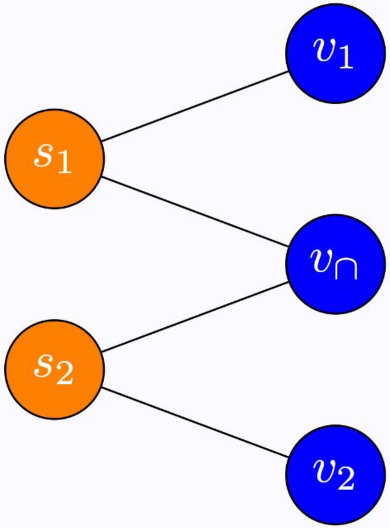
Incentivized Restaking Graphs

r $\quad$ α $\quad$ π $\quad$ S $\quad$ V $\quad$ σ

Rewards/points paid by each service

$$r_1 = \sqrt{K} \qquad \alpha_1 = \frac{1}{3} \qquad \pi_1 = (1+\epsilon)K$$

$$r_2 = \sqrt{K} \qquad \alpha_2 = \frac{1}{2} \qquad \pi_2 = (1+\epsilon)K$$



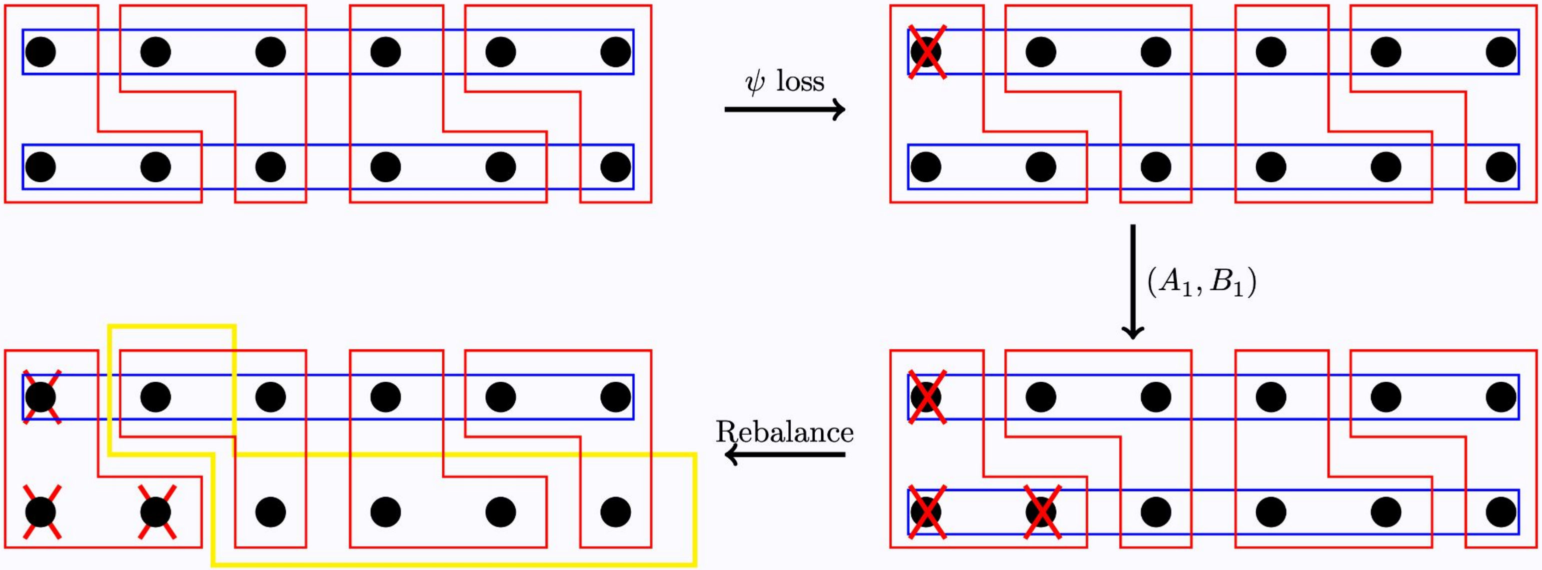
$$\sigma_1 = 1$$

$$\sigma_\cap = K$$

$$\sigma_2 = 1$$

Validators can adjust stake in response to rewards (i.e. rebalancing)

Rebalancing is All You Need



New Threat Model

Adversaries

We weaken the adversary to place realistic liquidity and cost of attack constraints on how many networks one could attack simultaneously

New Threat Model

We strengthen node operators, who previously were static (i.e. never rebalanced stake across AVSs) to instead be dynamic

Operators rebalance according to the expected rewards paid by the services and services can adjust rewards to reduce risk

Node Operators

Good News

Theorem [Informal] (Chitra & Pai, 2024):

Given an incentivized restaking graph G where adversaries realize p-norm profit and rewards $r_s \geq KS^{1/p}$, then

$$R_\psi(G) \leq \psi + \frac{C}{S^{1-\frac{1}{p}}}$$

There is also an efficient convex approximation algorithm to compute the minimal rewards to achieve this bound

Good News

Interpretation:

When,

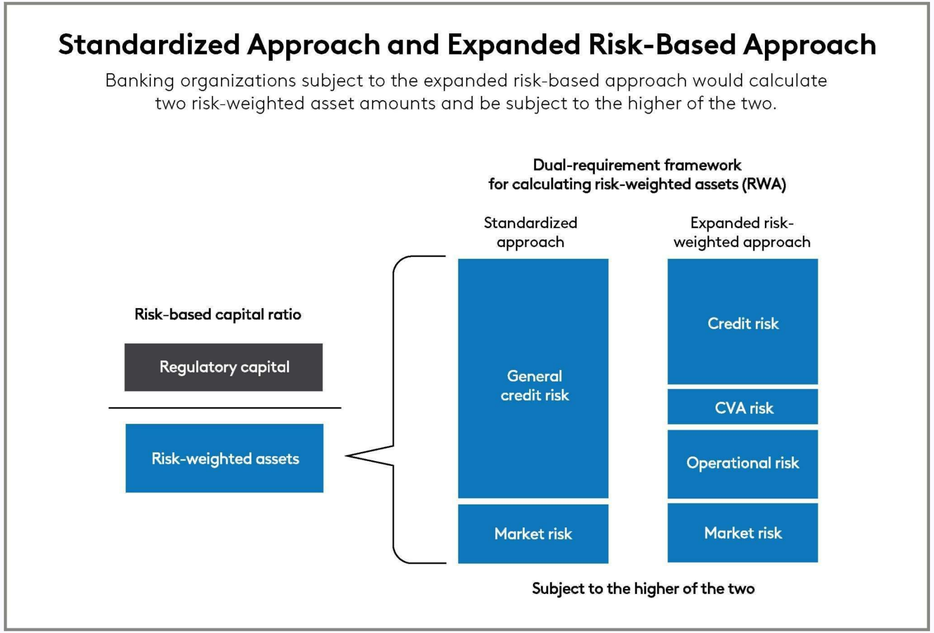
1. 💸 **Adversaries face costs…**
2. 🧠 **Node operators are smarter…**
3. 💰 **Services (e.g. AVSs) pay sufficiently high rewards…**

…only a small amount of stake can be lost in cascading attacks 🏆

[Note: The cascade guarantee degrades smoothly to the old model, p=1]

How do we reduce in practice?

- Eigenlayer (largest restaking network) proposed a new mechanism: unique stake
  - Service s reserves percentage $u_s \in (0,1)$ of stake only it can slash
  - Caps the maximum overlap between services stake
- Unique stake, adapted to market prices and elasticities, combined with incentives can provide efficiently verifiable guarantees that R is small
  - e.g. Verifiable Basel III



Gauntlet

Thanks!