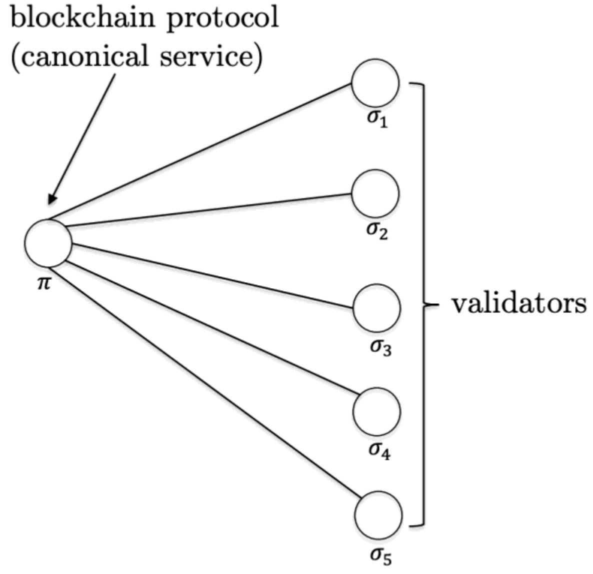
New paper with @n_durvasula offers a framework to reason about the risks of restaking. Key question: Under what conditions can validators be safely reused across multiple services? 1/13

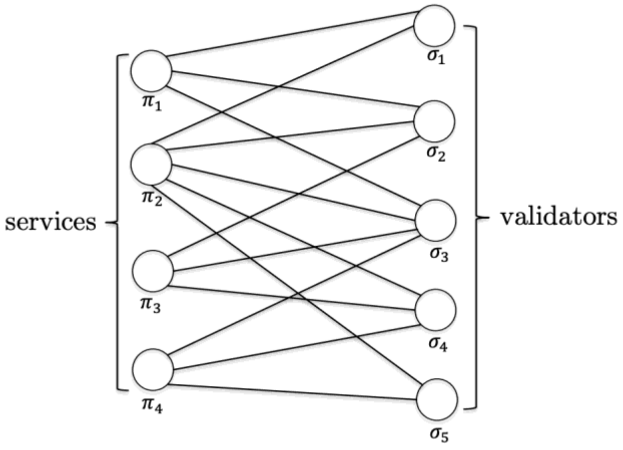
Robust Restaking Networks

Naveen Durvasula[*] Tim Roughgarden[†]

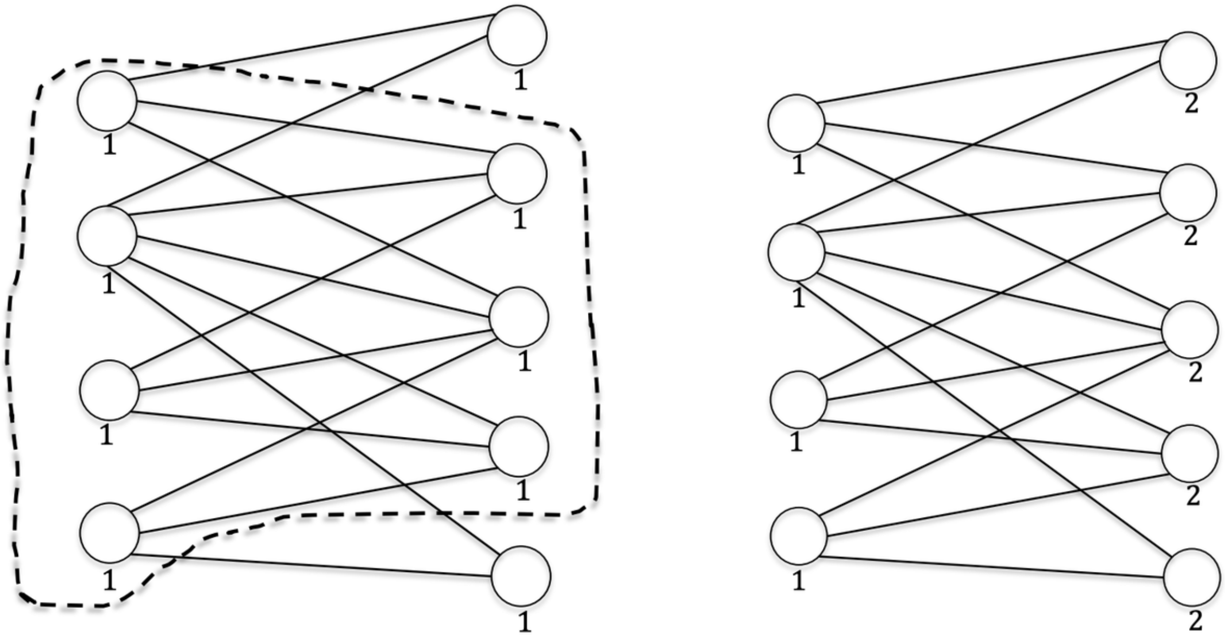
Baseline: One way to measure the "cryptoeconomic security" of a PoS blockchain protocol is to compare the cost incurred by attacking validators (e.g., due to slashed stake) with the estimated profit of an attack. Ideally, the former is significantly bigger than the latter. 2/13



Now suppose validators can help secure a number of services, in addition to a PoS protocol. This can be visualized as a bipartite graph, where each service has its own profit-from-corruption. 3/13



Security is now combinatorial (ideally, no *subset* of validators can profitably attack any *subset* of services), and closely related to the expansion of bipartite graphs. 4/13

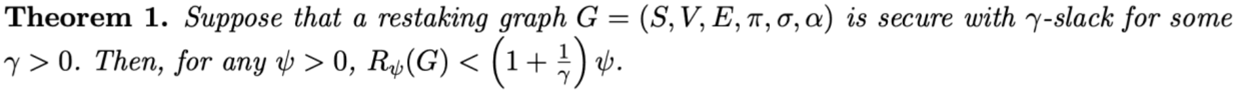


(a) A valid attack

(b) A secure network

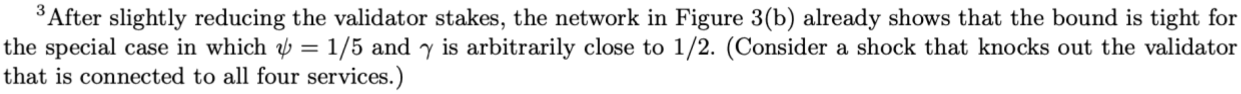
When is a restaking network “robustly secure,” meaning that a small "shock" (sudden loss of stake due e.g. to slashing caused by a bug) cannot enable a catastrophic attack? 5/13

Our first main result gives a tight characterization of robust security as a function of the shock size (psi) and the buffer between the costs and profits from attacks (gamma): 6/13



Theorem 1. *Suppose that a restaking graph $G = (S, V, E, \pi, \sigma, \alpha)$ is secure with γ-slack for some $\gamma > 0$. Then, for any $\psi > 0$, $R_\psi(G) < \left(1 + \frac{1}{\gamma}\right)\psi$.*

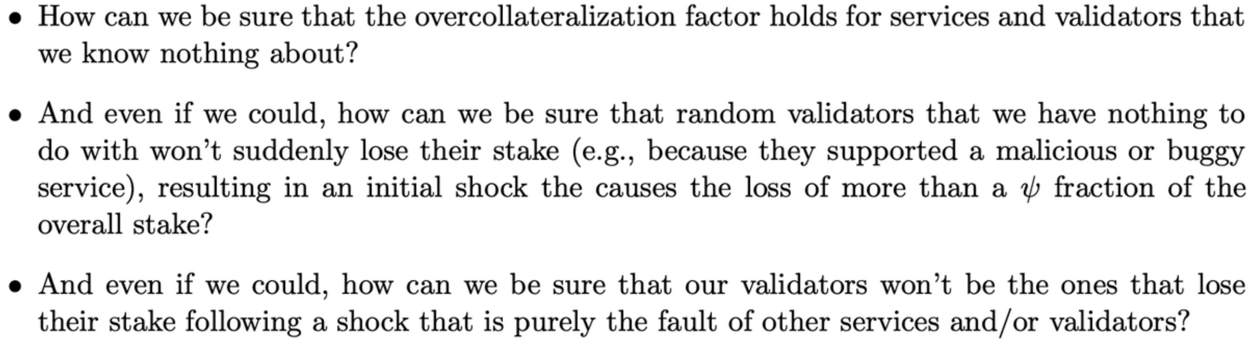
For example, our results imply that if attack costs always exceed attack profits by 10%, then a sudden loss of .1% of the overall stake cannot result in the ultimate loss of more than 1.1% of the overall stake. 7/13



[3] After slightly reducing the validator stakes, the network in Figure 3(b) already shows that the bound is tight for the special case in which $\psi = 1/5$ and γ is arbitrarily close to 1/2. (Consider a shock that knocks out the validator that is connected to all four services.)

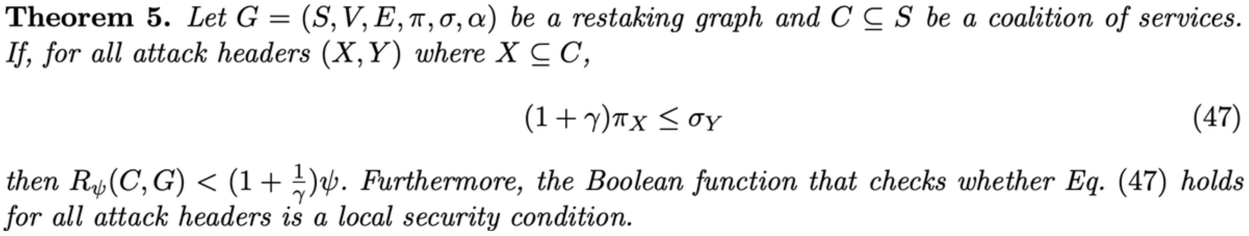
The overcollateralization factor of a network (meaning gamma, or 10% in the example above) is a measure of robustness that could be exposed to the participants in a restaking protocol (bigger is better). 8/13

Next we prove analogous "local" conditions and guarantees, specific to a subset C of services (e.g., a set of closely related services that share a number of dedicated validators). 9/13



- How can we be sure that the overcollateralization factor holds for services and validators that we know nothing about?
- And even if we could, how can we be sure that random validators that we have nothing to do with won't suddenly lose their stake (e.g., because they supported a malicious or buggy service), resulting in an initial shock the causes the loss of more than a ψ fraction of the overall stake?
- And even if we could, how can we be sure that our validators won't be the ones that lose their stake following a shock that is purely the fault of other services and/or validators?

The local case poses additional challenges: it is necessary and sufficient to restrict to the subset of "stable" attacks and require overcollateralization of all "attack headers." 10/13

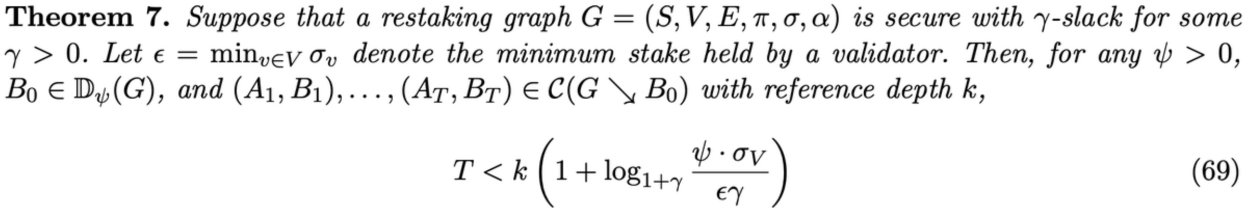


Theorem 5. *Let $G = (S, V, E, \pi, \sigma, \alpha)$ be a restaking graph and $C \subseteq S$ be a coalition of services. If, for all attack headers (X, Y) where $X \subseteq C$,*

$$(1+\gamma)\pi_X \leq \sigma_Y \tag{47}$$

then $R_\psi(C, G) < (1 + \frac{1}{\gamma})\psi$. Furthermore, the Boolean function that checks whether Eq. (47) holds for all attack headers is a local security condition.

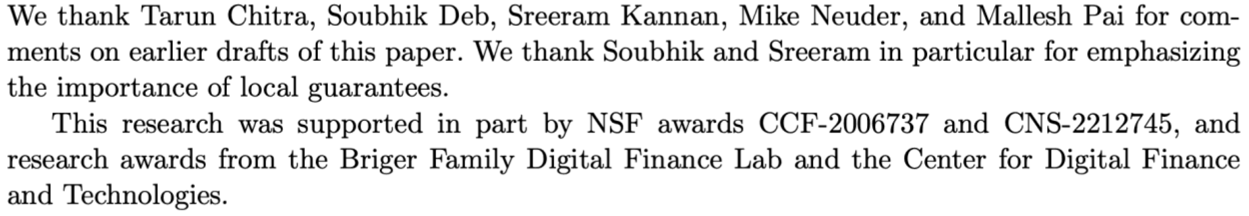
Final result: the maximum-possible length of a cascade of attacks is also governed by the overcollateralization factor: 11/13



Theorem 7. *Suppose that a restaking graph $G = (S, V, E, \pi, \sigma, \alpha)$ is secure with γ-slack for some $\gamma > 0$. Let $\epsilon = \min_{v \in V} \sigma_v$ denote the minimum stake held by a validator. Then, for any $\psi > 0$, $B_0 \in \mathbb{D}_\psi(G)$, and $(A_1, B_1), \ldots, (A_T, B_T) \in \mathcal{C}(G \searrow B_0)$ with reference depth k,*

$$T < k\left(1 + \log_{1+\gamma} \frac{\psi \cdot \sigma_V}{\epsilon\gamma}\right) \tag{69}$$

Acknowledgements @tarunchitra @soubhik_deb @sreeramkannan @mikeneuder @malleshpai 12/13



We thank Tarun Chitra, Soubhik Deb, Sreeram Kannan, Mike Neuder, and Mallesh Pai for comments on earlier drafts of this paper. We thank Soubhik and Sreeram in particular for emphasizing the importance of local guarantees.

This research was supported in part by NSF awards CCF-2006737 and CNS-2212745, and research awards from the Briger Family Digital Finance Lab and the Center for Digital Finance and Technologies.

Link to paper: https://arxiv.org/pdf/2407.21785 13/13