Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma
Joachim Neu, Nusret Tas, David Tse – {jneu,nusret,dntse}@stanford.edu

Gasper = Ethereum 2’s beacon chain consensus protocol

1. Found an attack on Gasper
An adversary with an arbitrarily small fraction of stake stalls liveness by proposing two competing chains and influencing honest participants’ votes to maintain a tie.

To influence honest votes, the adversary strategically releases adversarial votes from earlier slots.

2. Reverse engineered and formalized Gasper’s design goals: Availability-finality dilemma → Ebb-and-Flow protocols

3. → Ebb-and-Flow protocols (Cont’d)

4. Designed an optimal solution which is provably secure

→ Snap-and-Chat protocols

---

Links

Talk Preview (1min)
Talk (15min)

Paper

Blog post: Resolving the Availability-Finality Dilemma

Ethresear.ch discussion: A balancing attack on Gasper, the current candidate for Eth2’s beacon chain

*The Availability-Accountability Dilemma and its Resolution via Accountability Gadgets*

---

Is there a consensus protocol that provides both availability and finality?

→ Availability-finality dilemma

(CAP theorem: Gilbert, Lynch ’02; Lewis-Pye, Roughgarden ’20)