Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma

Joachim Neu, Nusret Tas, David Tse – {jneu,nusret,dntse}@stanford.edu

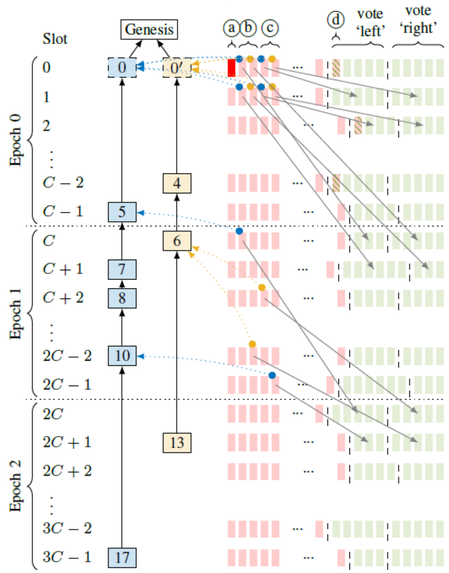
Stanford University

Gasper = Ethereum 2's beacon chain consensus protocol

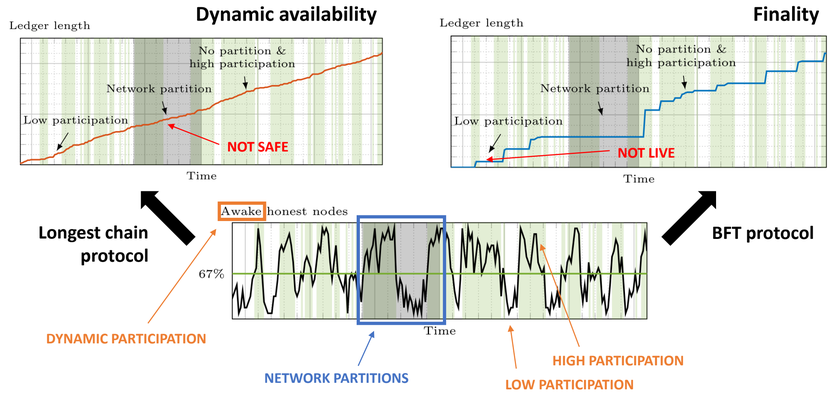
1. Found an attack on Gasper

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



Is there a consensus protocol that provides **both** availability and finality?
→ Availability-finality dilemma

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

NO!

3. → Ebb-and-Flow protocols (Cont'd)

Single ledger: $tx_1, tx_2, tx_3, \ldots$

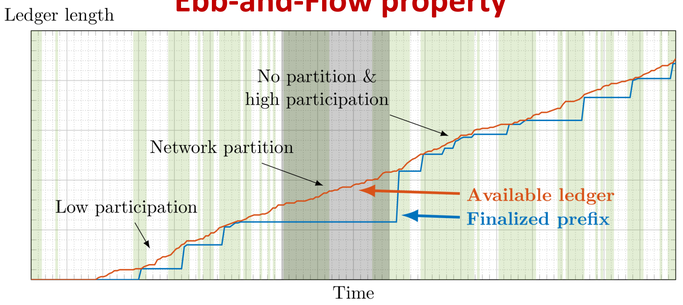
Always safe + live under network partitions and dynamic participation

Impossible!

Available full ledger
Always live, safe unless network partition

Finalized prefix ledger
Always safe, live unless low participation

Ebb-and-Flow property



(Nested ledgers: Nakamoto '08; Malkhi, Nayak, Ren '19)

4. Designed an optimal solution which is provably secure → Snap-and-Chat protocols

Finalized prefix ledger is secure under network partitions,

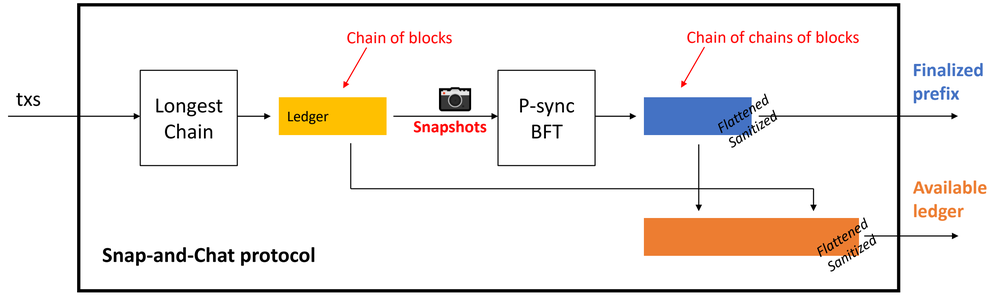
if < 33% of **all** participants adversarial

Available full ledger is secure under dynamic participation,

if < 50% of **awake** participants adversarial

Ledgers consistent (finalized is prefix of available)

Optimal



Links

Talk Preview (1min)

Talk (15min)

Paper
https://arxiv.org/abs/2009.04987

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"