

STARK proofs, due to their succinctness, seem the only viable candidate for recursive proofs. Recursive proofs, where proofs can be made to verify other proofs, can provide a seemingly optimal scalability solution. Are community members currently developing a blockchain (or Ethereum extension) to implement such a solution? I don't know of one, and I see no reason to wait, because STARKs are already fully developed. I'm confused why sharding, a tough concept to implement elegantly, is being pursued so vigorously when recursive proofs are already feasible. I don't even see much discussion on recursive proofs. Are there legitimate concerns regarding recursive proofs, or is the lack of activity due to a lack of sufficient mathematical expertise in the community?