Hi everyone,

We'd like to introduce VRF-based mining, a surprisingly simple and effective way of making pooled mining impossible. Instead of using hash functions, we use Verifiable Random Functions (VRFs) for proof-of-work-based consensus. As VRF binds the authorship with hashes, a pool operator should reveal his private key to outsource the mining process to miners, and miners can easily steal cryptocurrency in the pool operator's wallet anonymously.

Please find the details here https://hackmd.io/@ZcwjuAe3RUCFVPrXtvriPQ/S1YM1KZWI

This idea is co-developed by Runchao Han (me) and Haoyu Lin (@haoyuathz). We thank Jiangshan Yu and Omer Shlomovits for their valuable feedback.