Olivier Bégassat, Alexandre Belling, Nicolas Liochon

Hi all, this note contains a specification for a rollup design with anonymity and scalability properties halfway between (transparent) rollups and (fully anonymous) zk-rollups. It can have full data availability (both for users and operators), leaks relatively little user information on chain (account activity is leaked through updated account state hashes but transaction details are opaque to anyone but the relevant parties). Operators know what they are doing and are auditable (whence the “partially anonymous” tag.) The rollup state has bounded size (two depth 32 sparse Merkle trees) and can fully hold in memory.

We would greatly appreciate any feedback you may have!

partially_anonymous_rollups_with_encryption.pdf (371.1 KB)