The Perun research team is happy to announce the first lower bound on off-chain protocols. You can find our result at: https://eprint.iacr.org/2020/175.

Informally speaking, we prove that every Plasma system must have either large exits, or must suffer from a “mass exit problem” (or a variant of it) caused by data unavailability.

This provides a clean separation between Plasma-Cash-like systems (sometimes also called non-fungible Plasma) and Plasma-MVP-like systems (sometimes also called fungible Plasma). Our findings confirm that the best of both systems is not possible to achieve, and may guide the design of future construction of off-chain protocols. For example: one way to circumvent our impossibility result it to rely on the “defragmentation techniques”, or to use rollups. In other words: we show that some methods of this type are inherently needed if one wants to to avoid the problem of “mass exits”, and at the same time benefit from short exits (as, e.g., in Plasma MVP).

We are happy to discuss this result. One of us (Stefan) will also present it at the Stanford Blockchain Conference 2020 on Wednesday (the talk will be live streamed, please check https://cbr.stanford.edu/sbc20).

We thank the Ethereum foundation for their continuous support!

Best,

The Perun research team