We’re considering whether or when Arbitrum should support BLS signatures, on the BLS 12-381 curve, on transactions.

The main advantage is that this allows the sequencer to aggregate signatures so that an entire batch of transactions can carry a single (probably) 48-byte BLS signature, rather than a separate 65-byte ECDSA signature on each transactions. This would lower costs by reducing the L1 data footprint.

The main disadvantage, at this time, is that this would require defining a new transaction format which would not be supported by wallets and other tooling, at least at first. Ethereum may eventually standardize on such a format, but that seems unlikely to happen soon. So we would be implementing in advance of any Ethereum-wide standards process.

Perhaps other teams are willing to work with us on a jointly proposed standard.

This isn’t difficult to implement as a feature in Nitro.

Thoughts on whether and how to proceed?