

The problem of multi-block txns could even be made simpler, right now most builder payments are actually at risk. I outlined a payment from builder to proposer that was reorg'ed out a block and ended up in the mempool here [Builder->Proposer Payment Transfer Unbundle - HackMD](#).

A single rogue employee at one of these block relays could easily drain the builder of their entire collateral

In theory yes, but in reality most of the relays I have spoken to restrict access to their relay infra to data sensitive infra members. Your point still stands of course, but commenting to make the risk a bit more realistic.

1. A consensus layer verification of a signature directly from the block.coinbase address.

I believe this would stop builders from setting a validators EOA as the coinbase which often happens if there's no MEV in the block. It's probably not the worst scenario if we force this. I don't immediately see any issues with this approach, I need to think more about the implementation though.