At SKL we are impelementing on a Threshold-Encryption based protection mechanism for MEV.

While we working on it, one of our engineers@D2 came up with a simpler scheme.

Essentially you execute transactions in a block according to ordering specified by a Common Coin - an unpredictable, random number.

In our case, since each block is already signed by a Threshold Signature, which is a Common Coin, implementing this mechanism is really simple.

For other blockchains, Common Coin can be derived through VDF, which may delay execution a bit …