Have been reading a bit about side-channel attacks on Intel SGX recently and am consistently confronted with hacks that breach privacy. A lot of them are architecture specific and after their discovery are patchable but the sum of them seems to have a pretty significant surface area and all it takes is a single, new vulnerability to undermine the privacy of a system. I also know this is a highly unoriginal concern and am sure the Flashbots team and collaborators have a good position on this that they've answered in the past but… Curious as to why confidence in SGX justified for such a high-stakes use-case (private block building)?

Perhaps y'all are taking proper precautions or have some other reason not to worry, but am curious to learn why!