Here is a pretty scary attack one can do on ETH2 (or any other proof of stake PoS network)

An opensource developer can include a malicious piece into code of geth (or openssl or another part of the Linux stack) that intentionally creates a double sign transaction. The same can be done by an employee of a major cloud provider such as AWS.

Then the malicious code could be used to create a double sign evidence for ALL staked funds on all or a significant portion of nodes. The attacker could then either kill the entire network by submitting the evidence, or use the evidence for blackmail.

Note that the malicious code can be anywhere starting from Linux drivers and ending with the microcode executed by the CPU, so diversity of clients such as geth vs parity wont really help much.