Hi everyone,

I am not a BLS expert. But this scheme seems to be pretty new and therefore could potentially contain bugs and exploits. Is there a way to recover from potential exploits in phase 0? How is security guarenteed?