We are thinking to implement BLS signature verification using the bn128 Ate pairing verification implemented in SNARK-related precompiled contracts.

The precompiled contract uses SNARK library, which in turn uses libff library. This library uses bn128 ATE pairing curve, which seems to be OK for BLS.

The description of the curve says: https://github.com/scipr-lab/libsnark

“bn128”: an instantiation based on a Barreto-Naehrig curve, providing 128 bits of security. The underlying curve implementation is [ate-pairing], which has incorporated our patch that changes the BN curve to one suitable for SNARK applications.

It is not clear what the patch is and whether it affects suitability of the curve for BLS signatures. Does anyone know what the patch is?