Scriptless Scripts enable us to use digital signatures in order to enforce execution of smart contracts off-chain. Here, we define a smart contract as a trustless multiparty cryptosystem. They were originally introduced by Andrew Poelstra in the context of Schnorr signatures and MimbleWimble. In 2018, Moreno-Sanchez and Kate developed scriptless scripts using ECDSA, the signature scheme currently used in Bitcoin and Ethereum.

Naturally, one might think to attempt to figure out Poelstra-style scriptless scripts using BLS signatures. If this could be done, it would enable some forms of DApps such as atomic swaps in ETH2.0, potentially as early as Phase 0 (with some modifications of course).

So, I spent the past few weeks undertaking this endeavour. I have finally come to the conclusion that due to the properties of BLS signatures, Poelstra-style scriptless scripts may not be possible. A few Grin core developers have arrived at this conclusion several months ago and have written up a document that goes into details about why.

I would like to note that even though my attempts have been futile, I think pursuing pairing-based scriptless scripts is an interesting research problem. In fact, I might continue pursuing it.

If anyone is interested in working on developing pairing-based scriptless scripts, feel free to reach out.

UPDATE: I emailed Andew Poelstra about this. He seems to agree that is may not be possible to do this using BLS signatures for the same reasons outlined in the Grin dev's article.