Zcash got a huge upgrade: NU5, which uses Pasta curves as a basis for Halo proving system. These are two curves (Pallas & Vesta) with very interesting relation between them. Using these allowed ZEC to ditch trusted setup altogether.

In ETH2, BLS12-381 pairings are used to verify aggregate signatures for effective beacon chain communication. However, the need for trusted setup makes it deficient for apps that use circuits / zk-SNARKs.

Since neither EIP-2537, nor EVM384 precompiles have been implemented on mainnet, I would strongly suggest to focus on Pasta curves instead. Right now most zk apps on eth are using bn254, because it has its precompile. However, it's pretty bad, the approximate security level can be just 100 bits, or even lower. Some time in the future, folks will start switching to new technologies. If we act early, folks won't need to do bn254 => bls12-381 => something w/o trusted setup

, they would be able to go straight to step 3.

Some readers would think adding BLS precompiles is fine, since “we can always add new tech later”, however this will require all

EVM implementations to implement pairings on BLS curve and keep it forever, because VM code would still need to be executed in the future. That's why I think it's necessary to drop “bls in ETH apps” idea altogether.

We can keep using BLS12-381 for beacon chain, there won't be any need for switches / upgrades.