There’s a simple way to make an atomic swap between a smart-contact chain and any POW chain.

For example for Ether <-> BTC:

- Alice sends some Ether to the swap smart-contact which locks this money. While doing that she specify her BTC address and Bob’s ethereal address.
- Bob sends BTC to Alice.
- Bob shows the proof of this BTC tx on to the smart-contract and unlocks his Ether.

Bob’s proof is a signed transaction and SPV proof which lead to the valid Merkel root inside the block header. So smart-contact should either believe that proof is legit because it has sufficient level of work (number leading zeros in the hash of the block header, so it’s very costly to fake it) or there are oracles who send time to time these BTC block’s headers to the contact and the smart contact takes the chain with larger PoW as the legit one.

The question: is it possible to design a similar system where the second chain is POS?

The immediate problem with POS is how to verify that the block header is a legit one. Perhaps people who are building POS for Ethereum can give advice? As I understood this is also the problem for the lite client?

thanks.