Vitalik recently posted an article titled Don't overload Ethereum's Consensus - which is about external applications borrowing the economic security of Ethereum blockchain. Light client bridges are one such application but it was not covered in the article, so I have added my own analysis here.

Let me start by saying first of all that a PoS blockchain like Ethereum offers two layers of security ⇒ first is the economic security provided by the ETH staked on the Ethereum network. This type of security is supposed to be "fast" and objective. Any bad actors loose their stake (money) for malicious actions. The second layer of security is the social security layer. This layer provides a guarantee that if the economic layer falls apart due to any reason, then the community as a whole can come together and decide which fork is correct and recover the chain through informal coordination. Since the consensus process is quite objective, this kind of social recovery works because it's easier to agree on facts.

Light client bridges borrow the economic security but not the social consensus security

For a Light Client bridge between Ethereum (sending chain) and another PoS chain (receiving chain), the basic idea is that in order to attack the bridge, the bridge relayers (all of them), must collude with 51% Ethereum validators to sign malicious blocks that get submitted only to the PoS chain but never to the canonical Ethereum chain. This way, the bridge would be tricked into accepting transactions that never actually happened.

However, notice that this is akin to 51% attack by Ethereum validators. If we assume that the malicious blocks from the bridge somehow get broadcasted to the canonical Ethereum chain by some community members, as a result, this would trigger the social consensus layer to kick in on Ethereum. Post the recovery, the malicious blocks from the bridge will get rejected and the original canonical chain will again emerge as the winning fork.

If 100% relayers were dishonest, and no relayer reports the ongoing social recovery to the PoS chain, then, the bridge would be successfully tricked into accepting malicious blocks. However, please note, that in this situation, even though the attack was successful on the bridge, the attacking validators still loose all of their economic stake (~$18 billion). As a result, it would make sense to conduct this attack only if you can steal more than $18 billion from the bridge. By limiting the bridge TVL to less than staked ETH, we can ensure that the incentives to conduct such an attack never arise. Overtime, as the Ethereum economic stake rises, the maximum bridge TVL can increase accordingly.

Here, we have assumed the existence of an accountable Light Client for Ethereum, and assumed that the transaction is going from Etheruem to the PoS chain.

Not just bridges, securing external applications using Ethereum Social consensus is hard

While we have analyzed this strictly from a bridging perspective, if we think carefully, this constraint applies to all situations where we are securing value outside

the Ethereum blockchain, while using Ethereum security. By "outside the chain", I mean anywhere

that is not on Ethereum. This could include cloud execution environments, other blockchains

or TradFi like NASDAQ, etc

Hence, the current blockchain security model is reliable only if we assume that the assets being secured by a blockchain primary have value within the ecosystem of the chain itself. If we are securing any assets that carry value outside the chain as well, then we do not get any social consensus security from the underlying chain, and instead we only get the economic security. Quoting Vitalik - "dual-use of validator staked ETH, while it has some risks, is fundamentally fine, but attempting to "recruit" Ethereum social consensus for your application's own purposes is not"

So how do we fix this?

Since we cannot rely on social security, we must make sure that the economic security is very high. As such, it would be better if the value of the Ethereum stake were to increase significantly. The current value of $35 bn is good, but in future, if this value can cross $1 trillion, it will give confidence to applications that wish to borrow Ethereum security.

This of course does not solve for the case where the external applications have a negative impact on the economic security itself, as discussed in some of the cases in Vitalik's article. Solving this issue would require new consensus algorithms that don't rely on honest majority assumptions.

So conclusion?, is this high risk or low risk according to the analysis done by Vitalik in his article?

By my analysis, I consider this Low-risk

, since it makes use of the Ethereum economic consensus but does not depend on the social consensus layer of Ethereum.