Sealed Glass:

1. SGX performs the verification on the seller input, e.g. in the case of PoR the
2. Since it assumes that SGX does not provide confidentiality, it cannot support privately verifiable PoR, as in this case the knowledge of a secret is needed to do the verification. Instead, it has to use publicly verifiable PoR that is costly. Note that the buyer cannot commit its verification key in the SGX and then open it, as this is one-off, and for next verification it has to download the entire data and re-generate the tags.
3. SGX is always involved in the protocol.
4. It assumes SGX original signature scheme (i.e. EPID signature) and its related secret key remains secure and not revealed to the host.

Drawbacks:

1. It also does not provide the privacy of payment similar to zkCSP.
2. It is only feasible in theory. The reason is that the smart contract needs to verify the messages signed by SGX using EPID signature scheme. However, EPID signature scheme is not supported by Ethereum. One may let the verifier define its own signature scheme using a secret key. However, this is against the protocol assumption that such secret is leaked to the host, i.e. prover.
3. Because the smart contract cannot verify SGX signature in practice, the sealed-glass implementation does not support ‘’guaranteed fulfilment’’ property**. Thus, it suffers from the sames issues as fair-swap and zkCSP suffer from (i.e. coin transfer is public and immediate, and coins transfer require client’s engagement).**