Homework 3 Answers

Answers

2. The Zokrates plugin rejects invalid inputs when creating the proof, but you can manually edit the proof, which should then get rejected by he verifier.

3. Because we are working on the Ethereum blockchain, we can have public inputs from other contracts, but the whole question of trusting data sources then becomes relevant.