The recent 51% attack on ETC made me think that this is not that far away from Ethereum, as renting 20X more hash power today is mostly about money (unlike Bitcoin, where the use of specialized hardware makes it harder to buy). Is there a way to make some transactions more secure (for example larger moves) until PoS comes?

One solution (that may already be implemented without me knowing about it) is to commit the transfer to a chain via hash reference. Lets say Bob gave me 100 ETH in block …56 in exchange for 100 of my magic ERC20 coin. If I transfer coins to Bob (say at block …57), he may be able to rearrange the chain so his transaction never happened. Now let me make my transaction include an IF statement, that makes it valid only if the hash of block …56 is as I saw it. If he rearranges the chain, he will not be able to use my transaction, as he cannot reproduce the original hash. How hard will it be to implement something like this?