Since people here suggested using Truebit for several purposes, it is important that we understand security properties of the Truebit whitepaper

It seems that Truebit protocol is vulnerable to front running in the following way:

Truebit pays bounties to verifiers that successfully challenge incorrect computations.

The problem with the bounties is that parasitic verifiers can verify nothing, and simply wait for good guys to report errors.

Since everything on the blockchain is public, I can wait until the good verifier guy announces a challenge, see his transaction submitted to the blockchain, and challenge myself. Then we split the bounty, but the good guy did all the work.

See page 24 of the whitepaper

Verifiers who have posted minDeposit can challenge (the hash

of) solution until timeOut. Prior to timeOut, the Verifier must

broadcast the hash of an even integer to the blockchain in order

to commit to a challenge. Hashing an odd number in case of no

challenge is optional and may be used to camouflage real challenges

from other Verifiers (see Section 5.3). After timeOut, the

Verifier broadcasts to the blockchain this hashed number in the

clear to reveal her action.

Note that the good guy can “camouflage” the real challenge, but this “camouflaging” unfortunately does not work since the bad guy can simply broadcast the same hash as the good guy