Final Project Report
Name: Li Kaixu
Stu Id: 1155180259

(a) advantages:

[1] better transparency: all the transactions are recorded on blockchain, these transactions are transparent and traceable to all users and can better avoid cheating

[2] save cost: an online retail shop does not have a intermediate platform or real-world rental fee, so it requires low payment for one transaction. It saves the cost of booth seller and buyer.

[3] better security: blockchain is a decentralized system with cryptography tools to ensure the validity and purity or a transaction. It is hard for attackers to make fake data or temper with data on chain.

(b) problems and potential solutions

[1]

Problem:

The management of balance is not very good. The reason is we do not set strict limit to donation and punishment. The seller can continuously set high price product and the users can set 0 score to an ongoing transaction multiple times to 'steal' balance from the contract. This is not what we want.

Solution:

We should set more detailed limit to avoid abuse of punishment and donation, like limit the times of punishment when users set score 0 or limit the address who sends donation. And we can think of set a trusted public third-party address store the punishment money and decide who to give. If both seller and buyer cannot get real money from the punishment, it is better to manage the balance of a deployed transaction. But it seems not be liked by someone in a blockchain, so it still needs more thinking how to carefully design the punishment.

[2]

Problem:

The security is not very good. We allow all users to register and we mainly check the address to ensure the integrity. We do not have encryption or hash to ensure it is not maliciously modified.

Solution:

We can use encryption tools, hash or Merkle tree to store the transaction data and user data. We can get better security and integrity through this and better avoid malicious ones,

[3]

Problem:

This system has no requirement for buyer registration and it gives the buyer a bit too much power by scoring(since only the buyer can change it and punish seller). Malicious users can easily create zombie account to attack the contract.

Solution:

We can see requirement for users. For example, they need to pay at least 1 ether to enter or we require some certain format of personal information like names and address. We can tighten the rules.

[4]
Problem:
We do not really complete the function of event signal like EventTransactionInitiation, EventTransactionComplete. We give the event function but they are all empty.

Solution:
I learned from TA that it is complex and require frontend code, so I do not complete it. I give the format of event and emit for future use if someone really want to do it. The potential solution I think is a function directly send a signal to the address of seller when something happens.