Correct the answer if see any error.

## Question 1

### Part a

### 

1. b
2. c (*Re-entrancy attack is related to smart contracts*)
3. b

Iv. In the slide:

+ no order book maintenance.

+ simple implementation of CP AMM.

+ low gas fees

- Danger of impermanent loss/ coin de-peg.

- high slippage for low liquidity market.

- user is vulnerable to sandwich attacks

### Part b

1) .

The main formula is (noting that we have a *constant* product market maker)

Simplifying,

2) Let x,y be the amount of ETH and DAI after arbitrage, respectively.

X: Y = 1:200 (exchange rate after arbitrage)

X \* y = 10000 (constant product after all)

Hence, x = 7.0711 ETH () and y = 1414.2 DAI.

Before: 10 eth + 1000 Dai = 10\*200+ 1000 = 3000 USD.

After: 7.0711\*200 + 1414.21 = $2828.4

Loss = 171.57

## Question 2

A. I) All – see slides.

II)

a.F (*it should be* p *instead of* p – 1)

b. T (False – MEV is a concern for consensus because it incentivises miners to fork the chain, not for the reason stated in the q)

c. T (bookwork)

d. F (while it is *harder* to back-run due to the element of luck that is required in ordering, it is still easy enough)

e. T (bookwork, slide 90)

f.F (bookwork, slide 90)

g.F (bookwork)

h. F (bookwork)

I.T (bookwork)

j.F (bookwork; network layer actually)

b.

I) see slides

ii) Slide 89, Security (bookwork). The link between the searchers (third party crawling the for MEV) and the miners – *relays* the BEV transactions between the two groups. The third party bribes the miners for that.

c. see slides.