No. AbdelRahman Adel
Date. 17012296

Assignment 4

① it would create more branching, which is vaulenerable to attacks, and also would allow someone with less than 50% of the hash rate to be able to manipulate the chain.

② - if SHash 256 (P) == h then spend else Not honest Transaction

- if he password is revealed then all of Bobs funds are indanger

③ ECDSA requires less space than RSA
ie: if it's 256 bits secure RSA needs → 15360 bits
& ECDSA needs → 512+ bits
$\frac{1}{30}$ of RSA size

④ P2PK ⟹ Public key directly included in output
P2PKH ⟹ Hashed Public key included in output

Advantages:
- Improved privacy since the Public key is not known
- Improved Security
- Reduction of size

⑤ No it's not fair, it would be more fair if it was proportional to the hashing rate of each person

(6) The best ~~to~~ time theoratically is to wait until you have 6+ Blockes, which means there is no longer chain since each Block takes 10 mins to mine, but it would not be wise since the network can detect it and mark it as an dishonest branch

(7) if it doesn't pass then she might lose her funds and not get her refund

(8) As long as one player is honest it will affect the sum which means that it will affect the result after the modulo then it is fair and random.

I acknowledge that I am aware of the academic integerity guidelines of this course, and that I worked on this assignment independently without any unauthorized help

عبد الرحمن عادل عبدالفتاح