

BBM 443 homework 1 - Deadline 12.11.2018 by midnight

- 1- In class we have demonstrated that there are online client side Bitcoin wallet generators such as <https://www.bitaddress.org>
Using the above website, I created a wallet that includes public key / private key pairs where the bitcoin address is 139sa8tvAQ4hyoYupWpRSWEvY3gwFeqspn
There are also websites to check the balance and transactions of a wallet on the bitcoin network such as <https://www.blockchain.com/explorer>
Immediately after creating the wallet, I can check the balance of the wallet on the explorer page, which, of course, shows a balance of 0 BTC.
<https://www.blockchain.com/btc/address/139sa8tvAQ4hyoYupWpRSWEvY3gwFeqspn>
If I change the last character of the wallet address from 'n' to 'a', the explorer page reports it couldn't find it.
<https://www.blockchain.com/search?search=139sa8tvAQ4hyoYupWpRSWEvY3gwFeqspa>
The question is although the bitaddress.org is a client side page which doesn't suppose to send any information to outside world, and I haven't shared the wallet address with any one yet, how does the blockchain.com/explorer page know if an address is included in a wallet?
 - 2- In slide 39 of the 3rd lecture, slide shows the content summary of a sample block. One information in the block is the timestamp.
 - a- Explain in what step the timestamp is used and how?
 - b- It is hard to establish a consensus on time in a distributed environment. Thus, an attacker can try to attack the Bitcoin chain through this ambiguity. Propose an attack that can be done to the Bitcoin and explain what you can achieve with this attack? Explain what kind of mechanism does Bitcoin use to prevent such ambiguity in time variance.
 - 3- Bitcoin depends on proof of work (PoW) consensus algorithm and PoW mining requires lots of energy consumption for block creation. Many claims the energy requirements of Bitcoin is wasteful. Give a counter example to disprove this claim.
 - 4- Find the gain of the miner in BTC who mined the block ID 547785? Hint: use web.
-

This is an individual homework. DO NOT SHARE your answers with anyone.

Submit your responses through Google Forms using the link below.

Resubmission through editing previous submission is allowed.

Write your answers in English

<https://goo.gl/forms/8rIDae1fZDSRvmZ33>

Deadline 12.11.2018 by midnight