Homework 7

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only one homework per email. Work in pairs and submit a single solution! CC the email to your partner. Please also submit only ASCII text or PDFs (no .docs etc). Every solution should be preceded by the corresponding question, like:

Qn:	**…a difficult question from me…**
A:	**…an answer from you …**
Q$n+1$	**…another difficult question…**
A:	**…another brilliant answer from you…**

Solutions will only be accepted until 20th December!

1. How can the hardness of the proof-of-work puzzles in Bitcoins be adjusted? What is parameter that determines how the hardness is adjusted?
2. What is the main data that is stored in Bitcoin's blockchain?
3. What is is the purpose of the proof-of-work puzzle in Bitcoins?
4. The department has large labs full of computers that are pretty much idle over night. Why is it a bad idea to let them mine for Bitcoins?
5. Is it possible that Bitcoins can get lost (be irretrievable)?
6. **(Optional)** This question is for you to provide regular feedback to me, for example what were the most interesting, least interesting, or confusing parts in this lecture? Is there anything you like to have improved or explained in the handouts? Please feel free to share any other questions or concerns.