School of Electronics and Computer Science
University of Southampton

COMP6212 Computational Finance 2018/19

Assignment 3, Bitcoin Protocol (25%)

Issue	26 March 2019
Due	9 May 2019 10:00AM

---

1. You are expected to answer the first seven questions fully. The last three questions require in-depth understanding and further exploration. This assignment contributes 25% to your final mark of this module.

   (a) What is the maximum number of Bitcoins? How to calculate it? [6 mark]

   (b) If, on average, it takes 10 minutes to mine a block, when will the last Bitcoin be created? When will 97% of Bitcoin be mined? [8 marks]

   (c) What are the desired security properties of a Hash Function in designing the Bitcoin Proof-of-Work protocol? Briefly explain these properties. [10 marks]

   (d) What is a stale block? What is a Soft Fork? What is a Hard Fork? [9 marks]

   (e) What is double-spending? How does the Bitcoin network achieve consensus? [10 marks]

   (f) What are the routine tasks of a Bitcoin miner? What strategic considerations would a miner have? What is a 51% attack? [9 marks]

   (g) What are the bottlenecks of the Bitcoin system? [8 mark]

   (h) Explain the interconnection between block size, block generation interval, number of stale blocks, number of forks, length of forks, and block propagation time. [12 marks]

   (i) Describe the advantages and disadvantages of mining pools. Describe three possible ways that a mining pool distributes the block reward to individual miners. What are their advantages and disadvantages to the pool, and to the miners? Would there be any strategic behavior in these reward-sharing mechanisms? [14 marks]

   (j) When the transaction fees dominate the block reward, what changes would it bring to the Bitcoin ecosystem? Any potential risks? [14 marks]

   The Handin submission link will be opened on the 3 May. Please upload your answers in PDF format, font size 12 and no more than FOUR pages by the deadline.