CS 236r Problem Set 2

Due: Monday May 6, 2019

1 Introduction

In this assignment, you will provide a critical review of the paper "Incentive Compatibility of Bitcoin Mining Pool Reward Functions." However, this is not going to be a summary of the paper. Instead, we will provide detailed instructions about how to review the paper and how to comment on various aspects of the paper.

2 General Instructions

Here are some basic instructions on how to critically review a paper, particularly for this paper. Most of the instructions are taken from Prof. Michael Mitzenmacher's note, How to read a research paper.

- Expect to spend a few hours reading this paper. This paper also has appendices which includes the proof of the main results and some generalizations and details of the experiments. You are supposed to go over them as well.
- We advise you to go over the paper several times to get the complete picture. At a first reading, skip all the proofs and try to get an overview of the whole paper. Try to answer the following questions ? what is the main problem the authors are trying to solve? On subsequent readings, try to go over the proofs but most importantly get the main idea behind the proof.
- Critical reading : You should ask the following questions : (1) what are the assumptions made in the paper, are they reasonable? (2) are the authors solving the right question? (3) was the setup of the experiment sufficient? Did they interpret the data in a correct manner?
- Creative Reading : (1) How is this paper different from all the past papers in this field? (2) When are the assumptions made in the paper realistic? (3) What are the good ideas in this paper? Can they be generalized further?

3 Problem 1 (3 points)

This paper's main model assumes that there is only one mining pool and there are no other mining pools or solo miners (i.e. $\sum_{i=1}^{n} \alpha_i = 1$). Under this assumption, it shows that (1) the proportional reward function is not incentive compatible (2) the new reward function introduced in Section 5 is incentive compatible and (3) the pay-per-last-N-shares reward function is also incentive compatible for large enough N. Then, in Appendix C, the authors analyze the lack of incentive compatibility of the proportional reward function by allowing the existence of other mining pools or solo miners and show that (1) still holds qualitatively. Do you think allowing the existence of other mining pools or solo miners will affect results (2) and (3)? Why or why not? Provide a brief argument.

4 Problem 2 (3 points)

The paper introduces incentive compatibility rather informally in Section 2.3. Typically, the term incentive compatibility refers to dominant-strategy incentive compatibility, that is, in the context of this paper, for every miner i in a mining pool, for any given strategy profile of other miners, the best strategy of miner i is to report a full solution (as well as any share) that she finds immediately. There is a weaker notion of incentive compatibility, incentive compatibility at an equilibrium, that is, if for every miner i, if every other miners report a full solution (as well as any share) that they find immediately then the best strategy of miner i is also to report a full solution (as well as any share) that she finds immediately. Which notion of incentive compatibility is used in this paper? Please provide an explanation for your answer. (Hint: You may need to check the derivation in Section 3, proofs of Lemma 1 and Lemma 3 and Appendix B to convince yourself one way or the other.)

5 Problem 3 (2 points)

The new incentive compatible reward function will lead to a payment stream that is less steady compared to that of the proportional reward function. The authors argue theoretically that this is not too bad because about 63% of reward under this new function is still allocated based on shares (Lemma 6). Then, in Section 7, the authors further use simulations to show that using the new reward function there is only a modest delay in the time it would take miners to reach a minimal amount of bitcoin. Do you think the simulation sufficiently support that the new reward function is still good at achieving steady streams of payment for minders in a mining pool? Why or why not?

6 Problem 4 (2 points)

If you were a reviewer for this paper for a computer science conference, would you argue for accepting or rejecting the paper? What's your argument?