

# Reading Questions for Thursday, February 21, 2019

We ask you to submit comments on the following papers by midnight Wednesday February 20:

- Majority is not Enough, Bitcoin Mining is Vulnerable.
- Optimal Selfish Mining Strategies in Bitcoin.

Your comments should include both answers to the specific reading questions and generic response about the papers. You are welcome to include any questions you have about the papers in your comments. After submitting your own comments, you'll be able to see others' submitted comments. You can comment on others' submissions and answer raised questions on Canvas. Discussion on Canvas is strongly encouraged.

## 1 Reading Questions

1. "Majority is Not Enough, Bitcoin Mining is Vulnerable": What are the consequences of selfish mining attacks, and what is a proposed solution? Can you think of any others?
2. "Majority is Not Enough, Bitcoin Mining is Vulnerable": How much mining power is necessary to successfully perform selfish mining? In particular, why is the threshold less than  $1/2$ ?
3. "Optimal Selfish Mining Strategies in Bitcoin": What is "uniform tie breaking" and what impact does this have on would-be selfish miners?

## 2 Generic Response

Respond to the papers following the guidelines in the course syllabus (under "Submit Comments and Presenting Papers").