Reading Questions for Tuesday, April 9, 2019

We ask you to submit comments on the following paper by midnight Monday April 8:

- Formal Barriers to Longest-Chain Proof-of-Stake Protocols.

Your comments should include both answers to the specific reading questions and generic response about the paper. You are welcome to include any questions you have about the paper 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. Give an example of a predictable Proof-of-Stake protocol as well as an unpredictable one, and explain what makes them predictable/unpredictable.

2. How is the Globally-Predictable Selfish Mining strategy a more serious vulnerability than the selfish mining strategies we saw for Proof-of-Work protocols?

3. Why does a D-recent (i.e. unpredictable) Proof-of-Stake protocol guarantee that the Undetectable Nothing-at-Stake strategy will indeed announce extra deviating blocks?

2 Generic Response

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