Reading Questions for Thursday, March 28, 2019

We ask you to submit comments on the papers on Plasma and Casper by midnight Wednesday March 27.

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

Plasma:

1. What main functionalities does MVP (Minimum Viable Plasma) have and what problems remain? In particular, please discuss how invalid transactions are settled or stay problematic in different scenarios of withdrawals/exits.

2. Explain the high-level of idea of Plasma Cash: what problem does it attempt to solve? How does it track a coin?s full history? What are its advantages and challenges that remain?

Casper:

1. How does PoS prevent malicious attacks such as a double spending attack? Why are attackers deterred from doing so?

2. Explain why theorems 1 Accountable Safety and 2 Plausible Liveness hold, and describe the example shown in figure 3. Suppose there are three validators with equal stake, Alice, Bob, and Chris. If Alice and Bob behave honestly, why can?t there be two conflicting checkpoints finalized?

2　Generic Response

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