EE 374: Blockchain Foundations **Stanford, Winter 2023**

Lecture 19: PoS protocols: Possibilities and Impossibilities

May 16, 2023

Lecturer: Prof. David Tse

1 Introduction

We have discussed two PoS protocols so far: PoS longest chain (PoSLC) and Streamlet. In this final lecture, we will turn to a comparison between these two protocols. We will also ask the question: is there a possibility to improve upon these protocols to get the best in both worlds, capturing the best properties of these protocols?

2 Comparison between PoSLC and Srteamlet

PoSLC	Streamlet
secure under honest majority	secure under honest supermajority
slow confirmation	fast confirmation
partition intolerant	partition tolerant
dynamically available	not dynamically available
not accountable	accountable

Figure 1: Table comparing five properties between Proof-of-Stake Longest Chain and Streamlet.

3 Possibilities and Impossibilities

By observing the table, we see that neither Streamlet or PoSLC dominates in all 5 properties being compared. Streamlet has fast confirmation, partition tolerance and accountability, but requires a honest supermajority and is not dynamically available. On the other hand, PoSLC only requires a honest majority, is dynamically available, but is not partition tolerant and not accountable and has slow confirmation latency. Is it possible to design a new protocol that has the best of both worlds and dominates Streamlet and PoSLC in all 5 properties?

The answer is no. There are *impossibility* results which show that certain pairs of properties cannot be achieved by *any* consensus protocols:

- Safety under partition and liveness under synchronicity requires honest supermajority: this is a classical result due to Dwork et al [2].
- Partition tolerance and dynamic availability cannot simultaneously hold. If a protocol is partition tolerant, than it must halt when the number of parties have dropped a lot, because

they may be building another fork. On the other hand, a dynamically available protocol would retain liveness because the implict interpretation underlying that protocol is that the other parties have just gone offline. This *availability-finality* dilemma is discussed in more details in Neu et al [4]

- Accountability and dynamic availability cannot simultaneously hold. Accountability requires a sufficient fraction of *all* the parties to vote to confirm a block, but this would say that the protocol needs to halt when there are few parties online. This *availability-accountability dilemma* is formalized in [5].
- Accountability with $n/3$ parties held accountable when there is a safety violation and liveness under a honest majority is not possible. The former property implies that a honest supermajority is needed for liveness. This result is proved in [6].

These impossibility results show that Streamlet is *Pareto-optimal* in terms of these 5 properties: one cannot reduce the honest supermajority assumption or make it dynamically available without sacrificing at least one of the other properties. On the other hand, the impossibility results do not say anything about confirmation latency. So it is still possible to find a protocol that improves upon PoSLC in terms of making the confirmation fast while retaining the other positive properties (honest majority and dynamic availability). Indeed, a recent work by Momose and Ren [3] constructed a new protocol that does just that. So this shows that PoSLC is not Pareto-optimal and indeed we can so better.

PoSLC	Momose-Ren	Streamlet
honest majority	honest majority	honest supermajority
slow confirmation	fast confirmation	fast confirmation
partition intolerant	partition intolerant	partition tolerant
dynamically available	dynamically available	not dynamically available
not accountable	not accountable	accountable

Figure 2: Table comparing five properties between Proof-of-Stake Longest Chain, Momose-Ren and Streamlet. Both Momose-Ren and Streamlet are Pareto-optimal while PoSLC is not.

References

[1] B. Y. Chan and E. Shi. Streamlet: Textbook streamlined blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 1–11, 2020.

[2] C. Dwork, N. Lynch, and L. Stockmeyer. Consensus in the presence of partial synchrony. *J. ACM*, 35(2):288–323, apr 1988.

[3] A. Momose and L. Ren. Constant latency in sleepy consensus. Cryptology ePrint Archive, Paper 2022/404, 2022. `https://eprint.iacr.org/2022/404`.

[4] J. Neu, E. N. Tas, and D. Tse. Ebb-and-flow protocols: A resolution of the availability-finality dilemma. In *Symposium on Security and Privacy*, S&P '21. IEEE, 2021.

[5] J. Neu, E. N. Tas, and D. Tse. The availability-accountability dilemma and its resolution via accountability gadgets. In I. Eyal and J. Garay, editors, *Financial Cryptography and Data Security*, pages 541–559, Cham, 2022. Springer International Publishing.

[6] P. Sheng, G. Wang, K. Nayak, S. Kannan, and P. Viswanath. Bft protocol forensics. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, CCS '21, page 1722–1743, New York, NY, USA, 2021. Association for Computing Machinery.