PRESTO: A Systematic Framework for Blockchain Consensus Protocols

Stefanos Leonardos[1], Daniël Reijsbergen[1], and Georgios Piliouras[1]

[1]Singapore University of Technology and Design, 8 Somapah Rd, Singapore 487372, SG
stefanos_leonardos;daniel_reijsbergen;georgios@sutd.edu.sg

The rapid evolution of the blockchain technology has brought together stakeholders with fundamentally different backgrounds: software developers, startup enterpreneurs, corporate executives, investors and academics of various disciplines. The result is a diversified ecosystem, currently exemplified by the implementation of a wide variety of different blockchain protocols. This raises questions for decision makers in blockchain-based products and applications: How do different protocols compare? What are their trade-offs? Existing efforts to survey the area reveal a fragmented terminology and the lack of a unified framework to reason about blockchain consensus protocols.

In this paper, we work towards bridging this gap. We evaluate protocols as points in a five-dimensional design space: *Optimality*: does the protocol achieve its basic goals? *Stability*: are its participating agents properly incentivized? *Efficiency*: does the protocol maximize its output with minimum waste of resources? *Robustness*: can it cope with perturbations in its operational assumptions? *Persistence*: can it recover from catastrophic events? Based on the relevant literature, we divide these axes and sort properties of existing protocols in subcategories of increasing granularity. The result is a dynamic scheme – termed the *PRESTO* framework – targeted to the managerial practice. Its scope is to aid the communication between groups of different backgrounds and to allow the identification of research challenges and opportunities for blockchain protocols in a systematic way. We illustrate this via use cases in a first step to understand the blockchain ecosystem through a more comprehensive lens.

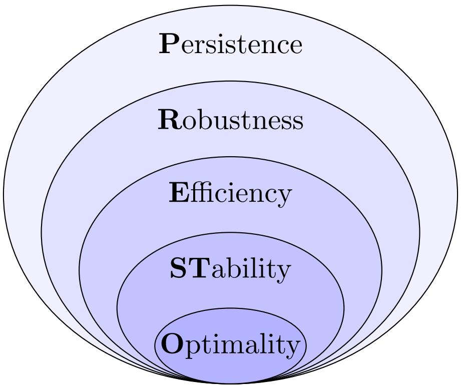

Figure 1: Understanding the PRESTO framework as a nesting doll of goals.

Acknowledgements

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2016NCR-NCR002-028) and administered by the National Cybersecurity R&D Directorate. Georgios Piliouras acknowledges SUTD grant SRG ESD 2015 097, MOE AcRF Tier 2 Grant 2016-T2-1-170 and NRF 2018 Fellowship NRF-NRFF2018-07.