Probabilistic Chained Blockchain Consensus

André Santos, Hasan Heydari. Alysson Bessani

LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal

LASIGE dependable and secure decentralized systems

What Is Consensus?

Consensus refers to the problem in which several participants in a distributed system attempt to agree on a single common value.

Consensus

Agreement
All correct nodes agree on the same value

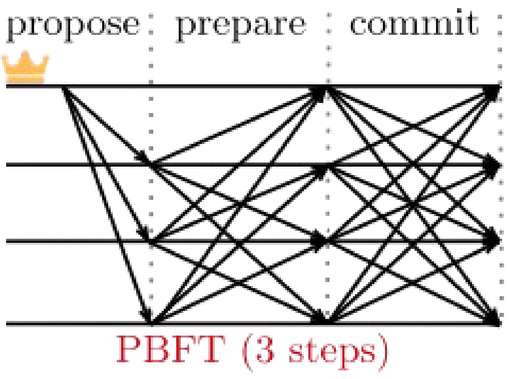
Termination
Every correct node eventually decides

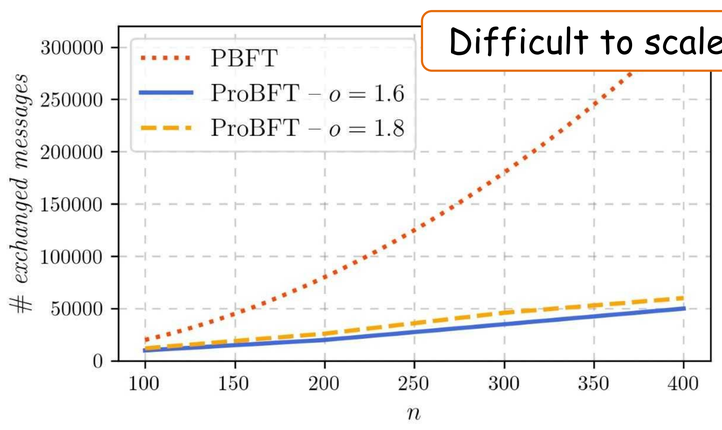
Validity
The agreed value was proposed and is valid

Probabilistic Consensus

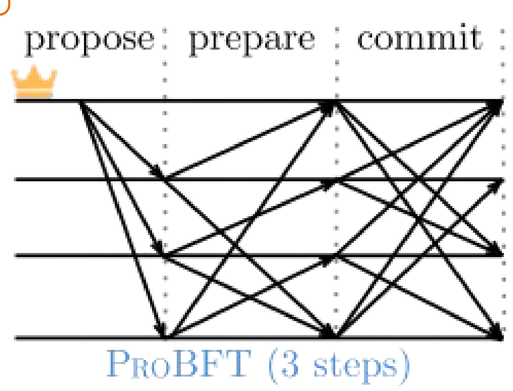
Probabilistic Agreement
All correct nodes agree on the same value with high probability

Probabilistic Termination
Every correct node eventually decides with probability 1





Difficult to scale!



ProBFT is a recently developed Probabilistic Consensus protocol at LASIGE.

Achieves sub-quadratic message communication by selecting samples of receptors randomly.

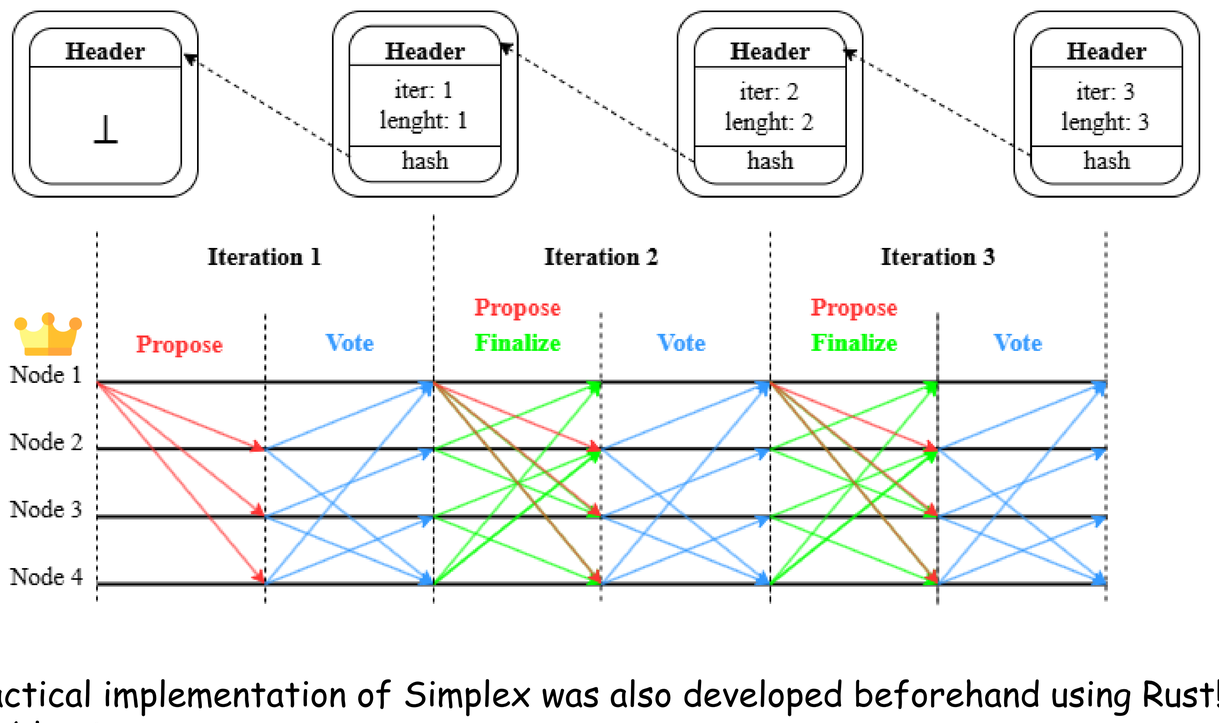
Problem!

ProBFT has never been implemented or evaluated experimentally and only solves the single-shot consensus problem.

Approach

1. Develop a SMR and Blockchain Probabilistic Consensus protocol capable of ordering blocks of transactions.
2. Integrate ProBFT's core mechanisms to a simpler and recent Byzantine Consensus protocol, Simplex.
3. Evaluate and compare this new protocol with Streamlet, Simplex and BFT-SMaRt.

ProSimplex



A practical implementation of Simplex was also developed beforehand using Rust!
Available at: https://github.com/AndreSantos0/Probabilistic-Chained-Blockchain-Consensus

Work Plan

Development
Integrate ProBFT's mechanisms into a practical implementation of Simplex

Evaluation
Evaluate and compare the newly implemented protocol with others

Document
Write protocol proofs

Patching and Improvement
Fix latency issues and bugs found with the current implementation of the protocol

Acknowledgements: This work was supported by the LASIGE Research Unit, ref. UID/00408/2025.
This work was supported by FCT through project SMaRtChain, ref. 2022.08431.PTDC, DOI 10.54499/2022.08431.PTDC (https://dx.doi.org/10.54499/2022.08431.PTDC) and the LASIGE Research Unit, ref. UID/000408/2025.