ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

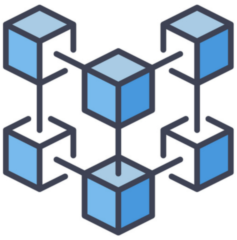
Distributed
Computing

Protocol Labs
Research

Prof. R. Wattenhofer

Building Practical Longest Chain Protocols

From traditional cloud computing and datacenter management to peer-to-peer applications, all the way to modern permissionless blockchains: state machine replication is an important building block of modern digital systems. Consensus algorithms can be seen as the engines that power these large systems.



Some of the most used consensus algorithms today fall into the category of longest chain protocols. Be it through proof-of-work (e.g., Bitcoin) or proof-of-stake (e.g., Ethereum), these protocols are at the core of modern blockchains. Sadly, these protocols are sometimes complex, hard to reason about, and even harder to implement.

Mir is a novel framework that makes implementing, debugging, and analyzing distributed protocols much easier. In this project we aim to leverage Mir to build longest chain protocols that allow researchers, developers and students alike to gain additional insights into current implementation. Additionally, we believe that through this implementation, we will have the potential to significantly support the development of new longest chain protocols, by allowing faster prototyping, and modelling. Eventually, other benefits of Mir, such as visualizations and debugging tools could be leveraged too. Moreover, our implementation could be used in teaching, both during lectures and hands-on exercises.

In a first phase we shall reason about the core abstractions and software building blocks needed, while in a second phase we will focus on bringing these protocols to life. Finally, extensions towards modelling the effects of particular tweaks or the behavior of potential adversaries are possible.

Requirements: Knowledge of the Go programming language and blockchain systems is a plus. We will have weekly meetings to discuss open questions and determine the next steps.

Interested? Please contact us for more details!

Contact

- Matej Pavlovic: matej.pavlovic@protocol.ai, Protocol Labs
- Yann Vonlanthen: yvonlanthen@ethz.ch, ETZ G97