Log inference on the Ripple Consensus Protocol

Author: Marijn Roelvink, Supervisors: M. Olsthoorn, A. Panichella, V. Prasad

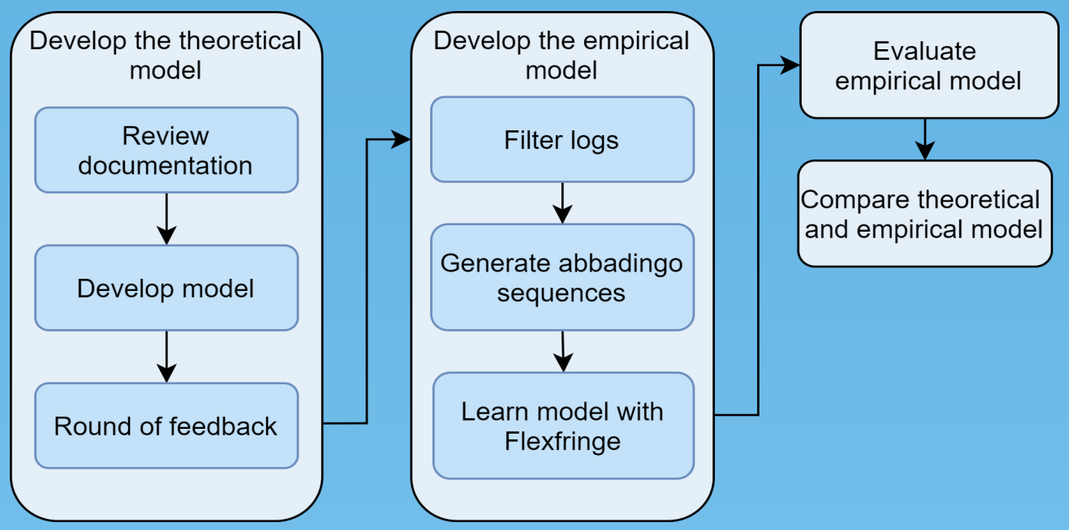
Problem

- **Ripple** is an up-and-coming **payments network** that aims to unite infrastructure of current financial system
- It functions as a **distributed ledger**, which is maintained by Ripple's **consensus protocol**
- To **verify** it is working as specified, we have applied **log inference** on this consensus protocol

Research question

Does the empirical model of Ripple's consensus algorithm, as produced by conducting log inference, match the theoretical model?

Methodology



Results:

- A **theoretical state machine** to compare with the empirical model.
- An **empirical state machine** with a **recall** of 99.8% and a **precision** of 97.4%.
- One **notable difference** between the empirical and theoretical model.
- This concerns the different behaviour of a validator during the ***wrongLedger* mode**.

Conclusion

- Whether this difference has significant implications remains to be researched.
- Thus, sofar the Ripple Consensus Protocol seems to be working correctly.
- For future work, a guarded DFA can be used to build a more specific model, and more data should be used to cover more irregular execution paths.

TU Delft ripple

20-05-2019, CSE3000