# Research proposal on Heterogeneous Paxos 2.0

Together with @isheff we have been working on the heterogeneous consensus protocol, and developed a new version of the consensus algorithm called HPaxos 2.0. The main improvements of our proposed algorithm compared tothe original version are summarized below.

## Advantages of HPaxos 2.0

1. Explicit broadcast

primitive

We assume a broadcast primitive, which sends each message to each acceptor and learner. For liveness, this primitive must provide the guarantee that each message received by one honest (safe and live) acceptor is eventually received by all acceptors. To guarantee this, the original Heterogeneous Paxos had each acceptor echo well-formed messages to all other acceptors. Instead, we leave the exact implementation of broadcast out of the Heterogeneous Paxos 2.0, allowing multiple possible implementation options. While echoing all messages would work, so would (for example) explicitly requesting unknown refs from a received message, which would (likely) require much less bandwidth.

1. Optimized sending of 2a messages

Instead of sending a 2a message for each learner, as per the original algorithm version, we send a single 2a with a set of learners. Conceptually, this is similar to sending a set of 2a messages, but in practice, it is more efficient, both to send and to track with message references.

1. One message in, at most one message out

Given the broadcast primitive and the 2a messages, we substantially simplify our protocol as follows. We remove all recursion and broadcast at most one message for each message received. Thus, instead of each actor receiving its own message in the same atomic action that it sends it (messages are broadcast, so actors receive their own messages), they receive them in some future action, just like any other message.

1. Improved Byzantine behavior detection

The original protocol assumed the comparison of transitive history sets. In the new version, we ensure that each message specifies the previous message from the same sender. This makes it much easier to detect and implement certain kinds of Byzantine behavior without sacrificing any guarantees.

## Formal verification of HPaxos 2.0

We have formally verified the newly introduced HPaxos 2.0 and proved the safety of the algorithm using theTLAPS proof system of TLA+.

## Shortcomings

Since the introduced algorithm operates on the graph structure of messages, when implemented naively unfortunately it has rather high complexity of single message processing.

More specifically, in the worst case, the complexity is $O(l \cdot n^5)$

, where $l$

is the number of learners (i.e. chain ids) participating in the heterogeneous consensus and $n$

is the number of messages processed so far.

While our HPaxos 2.0 algorithm improves the complexity of the original HPaxos (which is $O(l^2 \cdot n^5)$

), clearly more efficient versions are desired.

## Ongoing and future work

We have an idea on how to further reduce the complexity of HPaxos 2.0 to $O(l \cdot n)$

, and started working on our idea already.

Our results achieved so far are scattered across the following three resources:

1. the overleaf writeup

2. SML algorithm implementation and
3. HPaxos 2.0 ART report

In Q4, our plan is to finalize the development of the new optimized version of the protocol HPaxos 2.0 ^{\text{eff}}

with the complexity of O(l \cdot n)

, and formally verify the algorithm to demonstrate its safety. We are also planning to provide the first version of the implementation in the Anoma node and test the liveness of the algorithm within the Anoma infrastructure.