**Distributed System**

**Project Report**

Distributed Chat Application



Table des matières

[I. Project description and requirements 3](#_Toc171290391)

[II. Architecture Design/Theory 4](#_Toc171290392)

[A) Authentication 4](#_Toc171290393)

[B) Messaging 7](#_Toc171290394)

[1. Private Message 7](#_Toc171290395)

[2. Broadcast Message 7](#_Toc171290396)

[C) Fault tolerance 7](#_Toc171290397)

[III. Implementation 8](#_Toc171290398)

[A) GitHub of the project 8](#_Toc171290399)

[B) Send Broadcast Message 8](#_Toc171290400)

[C) Receive Broadcast Message 8](#_Toc171290401)

[D) Send Private Message 8](#_Toc171290402)

[E) Receive Private Message 8](#_Toc171290403)

[F) Fault tolerance 8](#_Toc171290404)

[IV. Test 9](#_Toc171290405)

# Project description and requirements

The application to implement is a peer-to-peer distributed chat application. With this application, the user should be able to send broadcast messages up to 9 different chatters (connected users) and he should be able to send private messages to a specific chatter.

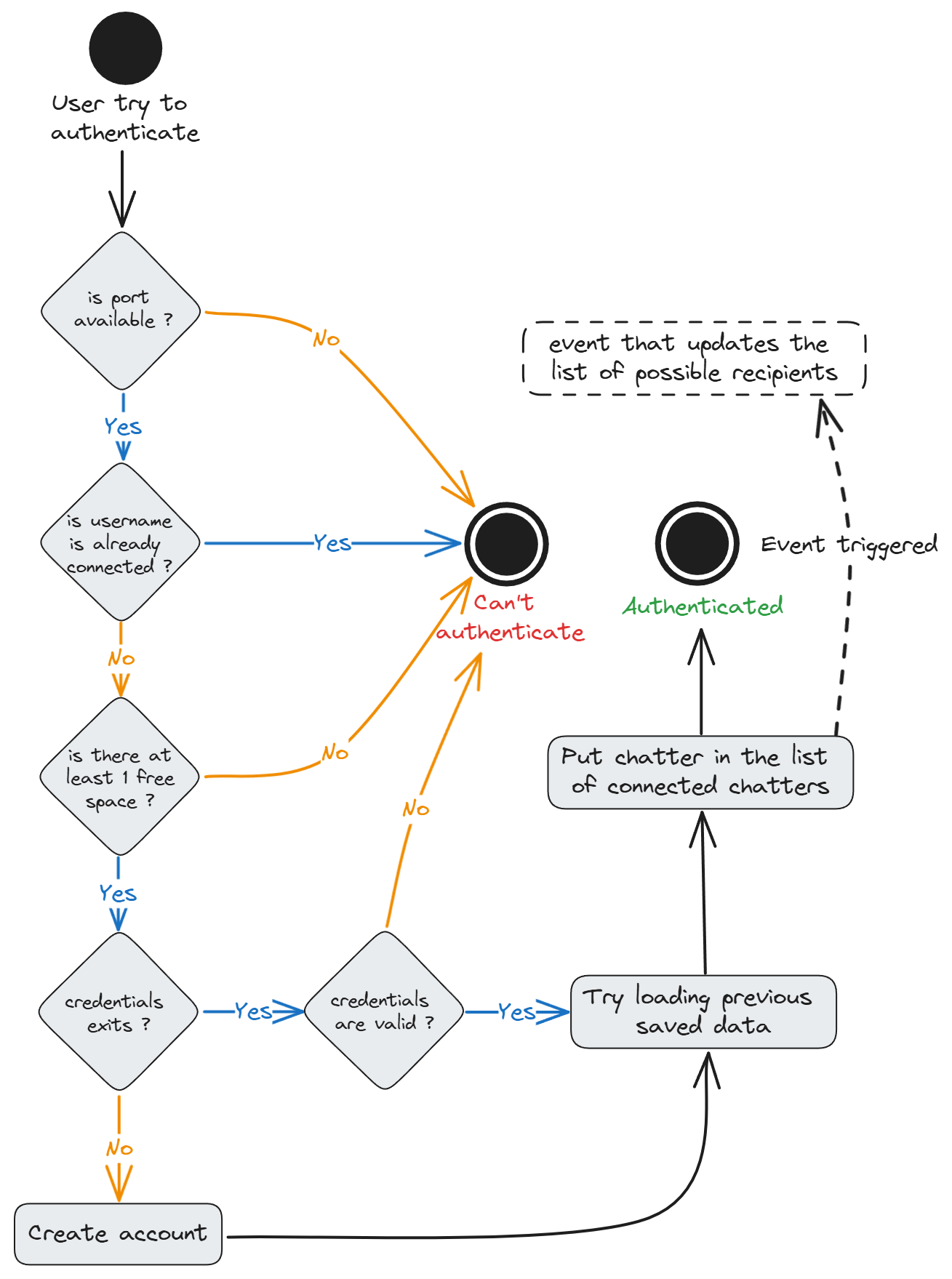
There is few constraints and assumptions made for this project. The maximum of connected chatters at the same time is 10. Communication between chatters should use UDP which means that **messages are unreliable and unordered** when sent (we must find solutions to address these problems). Broadcast messages should be received in a logical order (find the best algorithm to manage that). Private messages should be received in order (we need define which order).

In the whole report, chatters are defined as clients or users.

# Architecture Design/Theory

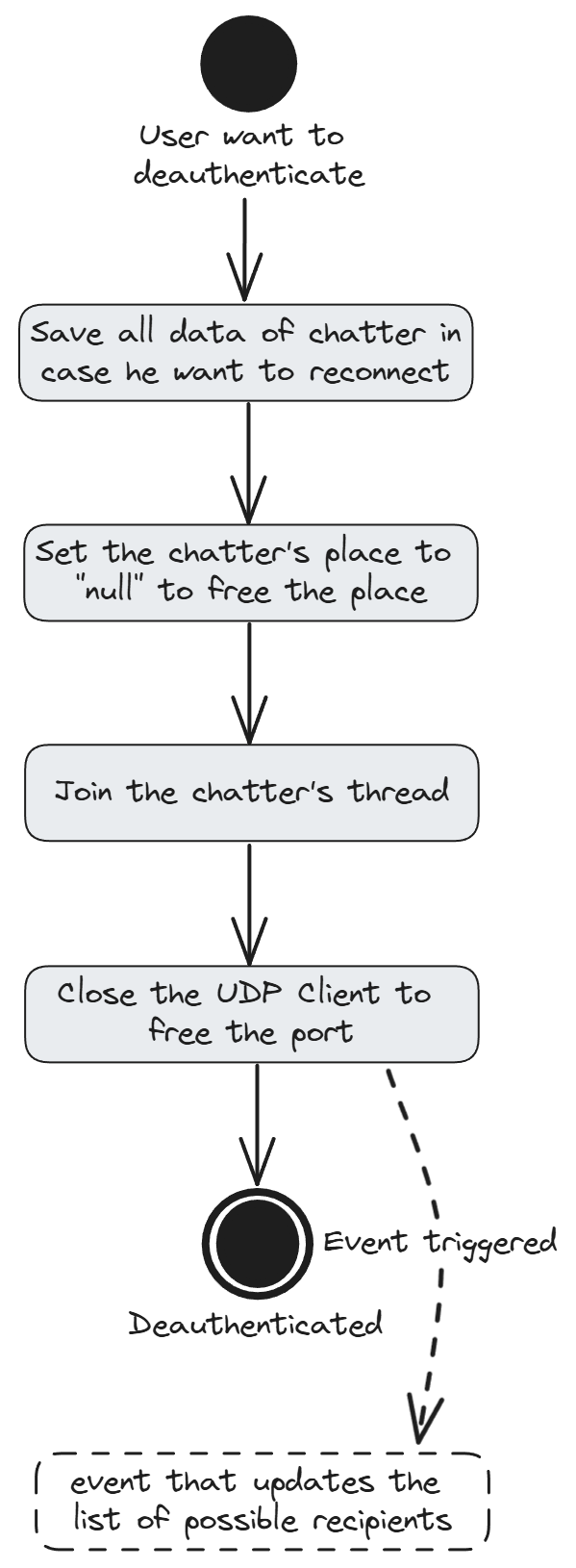
## Authentication

The first step is to authenticate users who wish to use the application. If the user has never logged in, an account must be created. If an account already exists, you need to check the user's login details to make sure they match. However, these are not the only checks to be carried out. Below is an activity diagram showing the algorithmic logic to be applied for server authentication.

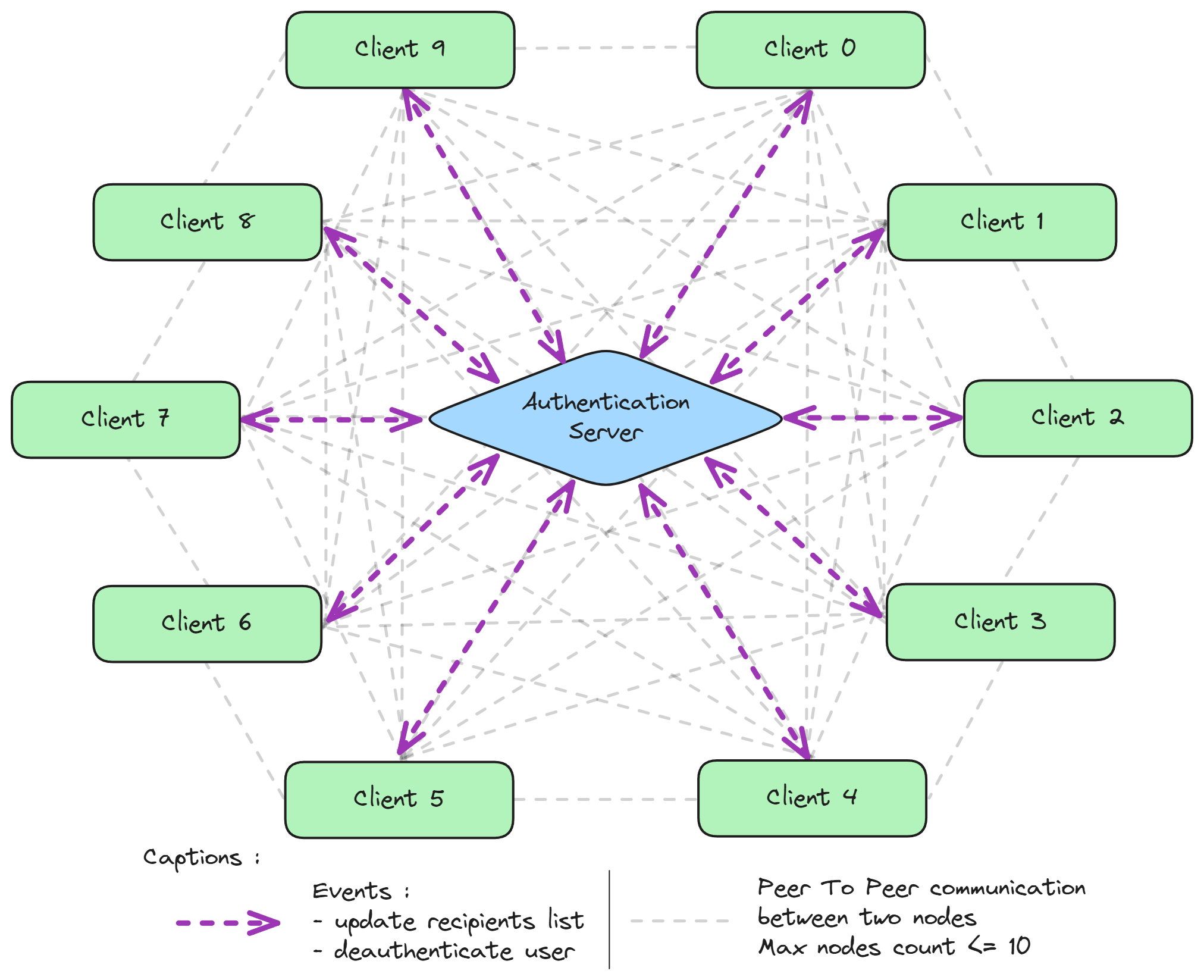


Scheme 1 : Activity Diagram for chatter’s authentication on the application

In fact, if authentication is the most important part of the Authentication Server, the user might also want to log out without causing data loss and/or errors for other users and future users. Below is a diagram of the user logout activity.



Scheme 2 : Activity Diagram for chatter’s deauthentication on the application



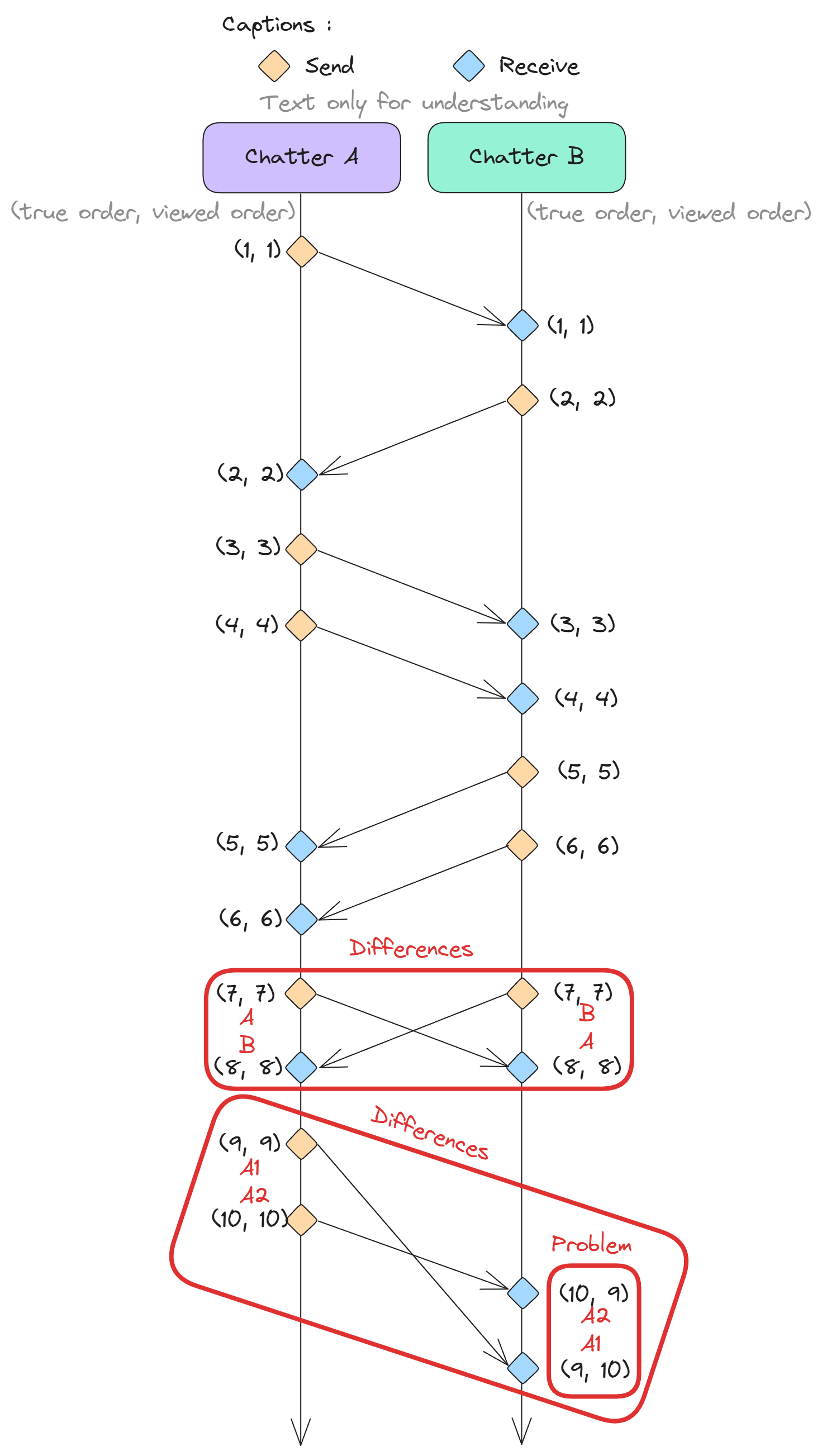
Scheme 3 : Diagram focusing on peer to peer with Authentication Server

The events that update the list of possible recipients on clients’ UIs (User Interfaces) allow to each client to select the communication channel he wants to use. All chatters must use the Authentication to instantiate an UDP client that allows for peer-to-peer communication using UDP. Closing the client must automatically call the deauthentication function of the Authentication Server. Since the scope of the project is focusing on private messaging and broadcast messaging, the Authentication is a shared static class that will not communicate with clients using UDP.

## Messaging

Once a Chatter has logged in through the authentication service, the user then has two options. They can either send private messages to another connected Chatter or send a broadcast message.

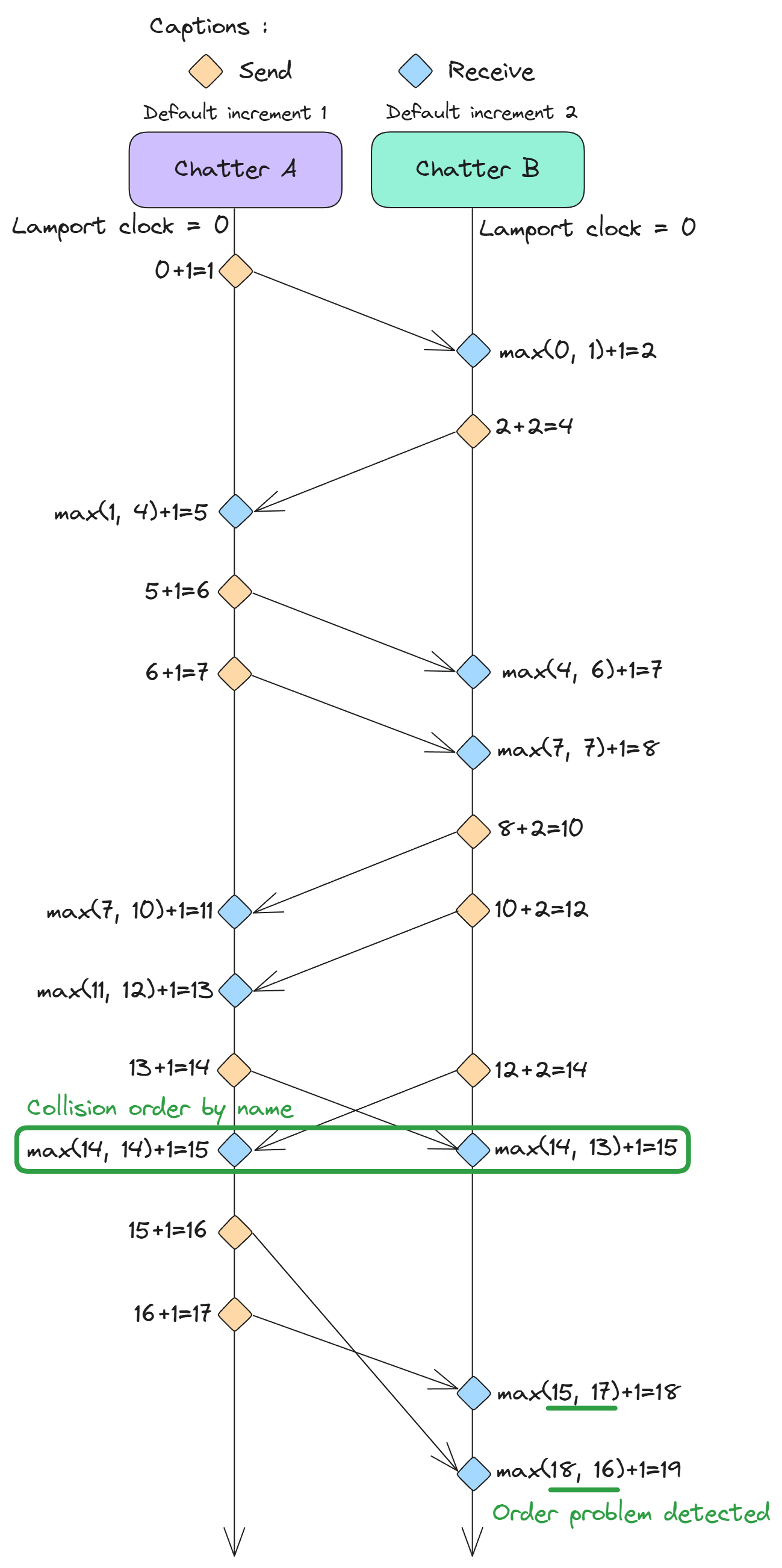
### Private Message



Scheme 4 : Naïve message sending using UDP (no order)

In the diagram above, the UDP messages are naively sent without any system to ensure their ordering. The displayed numbers are there to highlight the various issues that can arise. Two possible problems can be observed in this approach. If the messages are sent at the same time, the order of message display will be different between Chatter A and Chatter B. Additionally, a lost message will not be detected. Finally, if the delay between two messages causes the first one to arrive second, it will be impossible to retrieve their correct order.

That is why I chose to implement the Lamport Clock Algorithm. It allows for managing situations where two messages are sent simultaneously. We can manage their display based on the chatter's username in alphabetical order. Additionally, if a message is not received, this can be detected thanks to the counters which will show a large offset.

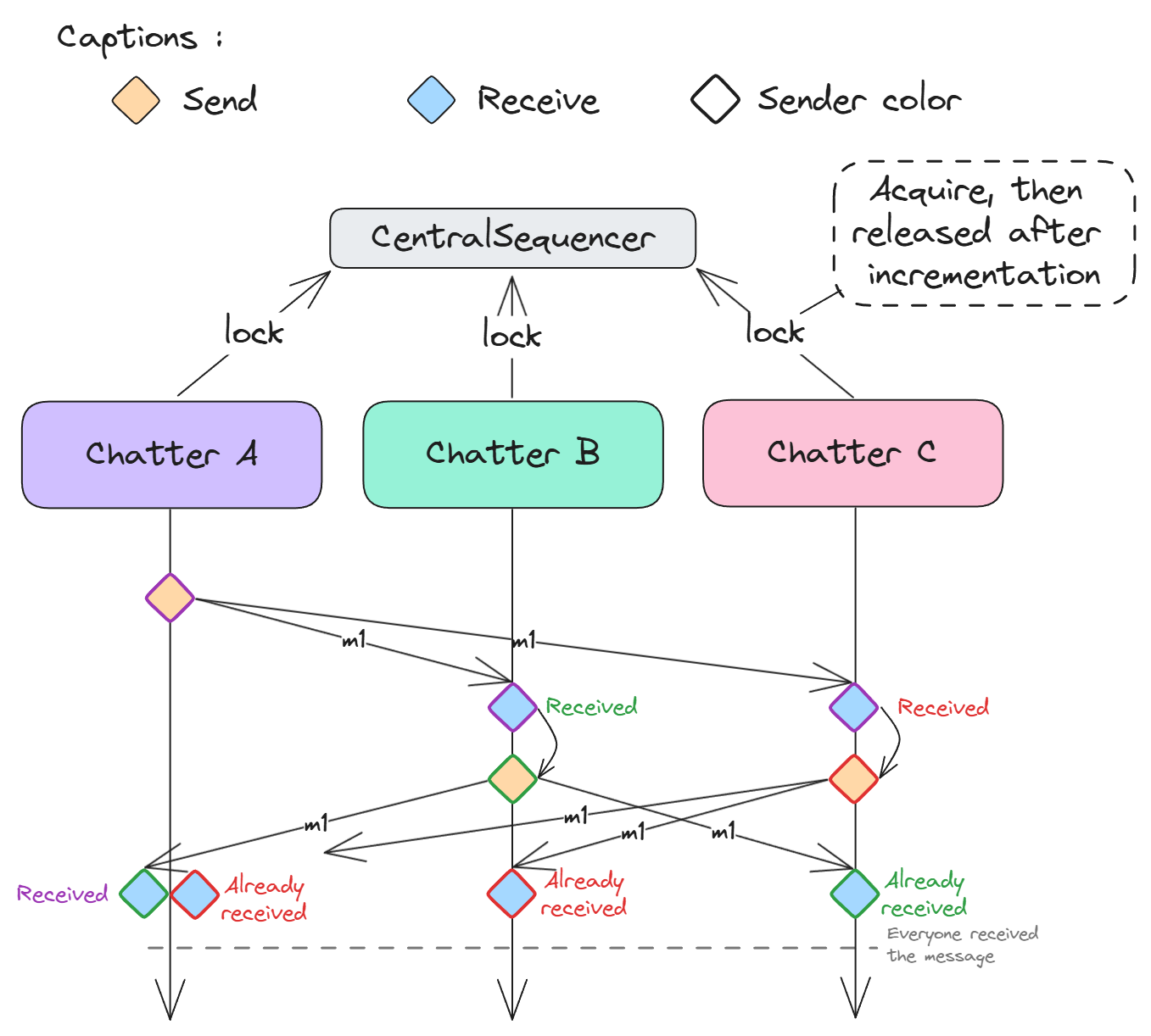


Scheme 5 : Lamport Clock System

### Broadcast Message

For broadcasting messages, I had several algorithms to choose from. While some of my peers decided to implement complex systems, I kept in mind that the maximum number of nodes (chatters) is 10. The eager reliable broadcast is a resource-intensive algorithm with a complexity of O(n²). Although this could be problematic for an application with a large number of chatters, it is important to remember that we have a maximum of 10 users. Additionally, the second advantage of this system is that message loss is less likely as more users are connected.

However, this algorithm alone does not allow for ordering messages. That is why I coupled it with the Total Order Broadcast, which I slightly modified. Since all users must go through the authentication server, I decided that the "leader" would be the authentication server. Instead of serving as a relay to the other chatters, we use a shared variable acting as a central sequencer. This would ensure message order is always maintained by adding a lock on the sequencer whenever a new message is to be sent.



Scheme 6 : Eager Reliable Broadcast

Message order is kept thanks to the central sequencer. This allows to know if a message as been lost or if the message received is a duplicate.

## Fault tolerance

As mentioned in the course and in the project topic, the simplest way to reduce the likelihood that a chatter does not receive the message intended for them is to send the same message multiple times.

To maintain good performance, I differentiated between private messages and broadcast messages in how the same message is sent multiple times. For private messages, I broadly estimated a message loss rate of 20%. Therefore, to ensure that the user's message is transmitted in the vast majority of cases, I send the user's message 10 times.

With a simple probability calculation, we find that the probability of the message being received at least once is 99.99998976%. This leaves little room for bad luck.

Nevertheless, if this same logic is applied to broadcasting messages, we will seek to correlate this repetition of sending based on the number of connected chatters. Indeed, if only 2 chatters are connected, the probability that message delivery will be problematic is high when 20% of the time the message does not reach the recipient. In the situation where 10 chatters are connected, message loss is less of an issue because there are 10 message sendings that will be rebroadcast by our Eager Reliable Broadcast algorithm. Thus, I arrived at the following conclusion:

Number of repetitions = 10 - (Number of connected chatters - 1)

This creates a reasonable balance and ensures that the message is delivered regardless of the number of users, while keeping the total number of messages sending reasonable.

# Implementation

## GitHub of the project

## Send Broadcast Message

## Receive Broadcast Message

## Send Private Message

## Receive Private Message

## Fault tolerance

# Test