**Project Specification**

**Title**

Peer to Peer ChatSDk with distributed hash tables

**Student(s)**

Benedikt Kaiser BSc.

**Project Advisor**

Alexander Palmanshofer MSc.

**Date and Time**

Hagenberg, 27.06.2023

Version: 03/2023

Table of Contents

[1. Overall Goal and Motivation 3](#_Toc139628332)

[2. Project Description 3](#_Toc139628333)

[2.1 Initial Technical Situation 3](#_Toc139628334)

[Currently, various distributed products, such as Matrix, are available. However, these products require you to set up a server at home with the necessary software to host the chat. While this setup offers security, it comes with the significant drawback of requiring a server at home and having the necessary knowledge. 3](#_Toc139628335)

[2.2 Realisation Concept 3](#_Toc139628336)

[2.3 System Context 4](#_Toc139628337)

[2.4 User Interfaces 4](#_Toc139628338)

[2.5 Functionality 4](#_Toc139628339)

[2.6 Technical Data 5](#_Toc139628340)

[3. Development Conditions 5](#_Toc139628341)

[3.1 Software 5](#_Toc139628342)

[3.2 Hardware 5](#_Toc139628343)

[4. Impact 5](#_Toc139628344)

[4.1 Target Groups 5](#_Toc139628345)

[4.2 Areas of Application 5](#_Toc139628346)

[4.3 Estimation of the Market Chances 5](#_Toc139628347)

[A. Appendix 5](#_Toc139628348)

# Overall Goal and Motivation

The goal is to develop an open-source Chat SDK for iOS that leverages distributed hash tables to create a decentralized communication system.

Motivation:

**Privacy and Security in Strict Countries**: Decentralized communication systems offer secure and private communication channels for individuals in countries with stringent internet regulations, bypassing centralized servers that can be subject to surveillance and censorship.

**User Empowerment**: Decentralized communication systems empower users by providing greater control over their personal data, mitigating concerns about data ownership and privacy that arise in centralized architectures.

**Network Resilience**: Decentralized systems demonstrate resilience by adapting to network disruptions and maintaining connectivity through alternative routes, ensuring uninterrupted communication even when parts of the network are compromised or unavailable.

**Trust and Verification**: Trust and verification mechanisms are crucial components of decentralized communication systems, enabling secure interactions and fostering confidence among users through cryptographic techniques, consensus algorithms, and robust trust models.

Also, the technology is pretty interesting

# Project Description

## Initial Technical Situation

Currently, various distributed products, such as Matrix, are available. However, these products require you to set up a server at home with the necessary software to host the chat. While this setup offers security, it comes with the significant drawback of requiring a server at home and having the necessary knowledge.

## Realisation Concept

I want to start by developing a simple udp communication class which handles every request. As soon as this works I will start implementing Kademlia. I will then develop a small example implementation and start testing how good it works and see what problems I face.

## System Context

The whole project has no dependency what so ever. It uses the swift networkListener for the communication and the official Kademlia paper will be used for the actual Kademlia implementation.

## User Interfaces

The actual master project implementation will not have a user interface but for testing purposes there will be an example implementation with a primitive user interface. This will mainly consist of necessities and will not implement eye candy.

This semester project has a small user interface to start the udp sockets and to request data from another device.

A screen shot of a phone

Description automatically generated

Figure 1 user interface

The ui for this example app can be seen in Figure 1

## Functionality

< Mentioning of all important functionalities respectively properties of the intended product; derived from Use Cases >

## Technical Data

< Standards, regulations, etc., if applicable >

# Development Conditions

## Software

XCode

## Hardware

Macbook, iPhone

# Impact

## Target Groups

The chatsdk will be open source and targets other iOS developer who want a safe communication but doesn’t want to implement it on their own. This package can just be used, they need to write a proper ui for it but the communication will be out of their hands.

## Areas of Application

Ios App development

## Estimation of the Market Chances

This project is going to be an open-source project. There is no point in making a closed source project and just say that it is secure. The developer needs to be able to check it if they want to.

# Appendix

Kademlia:

https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf