

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA ĐÀO TẠO SAU ĐẠI HỌC

MÔN HỌC: HỆ THỐNG PHÂN TÁN

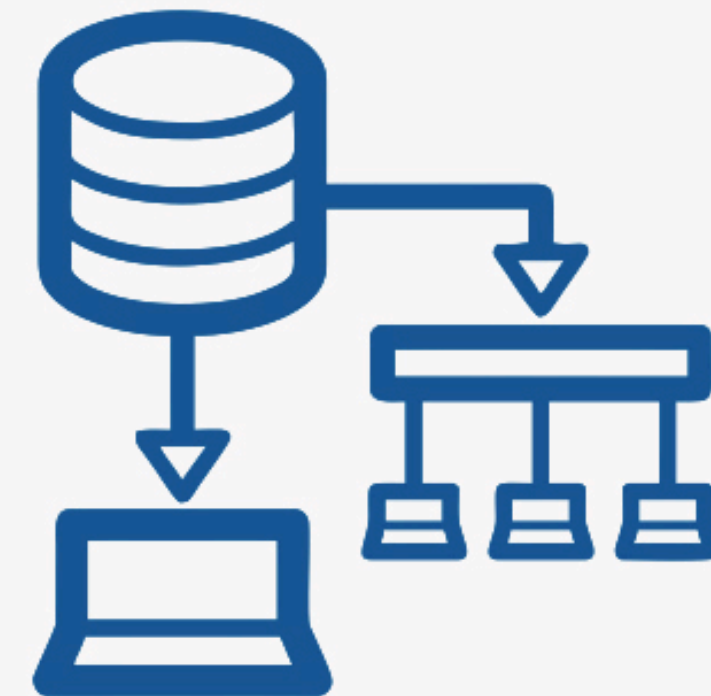
Đề tài: Xây dựng ứng dụng chat P2P

Giảng viên: TS. Kim Ngọc Bách

Học viên: Nghiêm Quốc Việt

Đàm Văn Trung

Mai Việt Hùng



Distributed Systems

PHÂN CÔNG NỘI DUNG TÌM HIỂU

Thành viên	Nội dung thực hiện	Đóng góp
Nghiêm Quốc Việt - B24CHHT100	Module định danh và xác thực	30%
Đàm Văn Trung - B24CHHT095	Module khám phá peer	40%
Mai Việt Hùng - B24CHHT077	Module gửi tin nhắn và đồng bộ tin nhắn	30%

NỘI DUNG TRÌNH BÀY



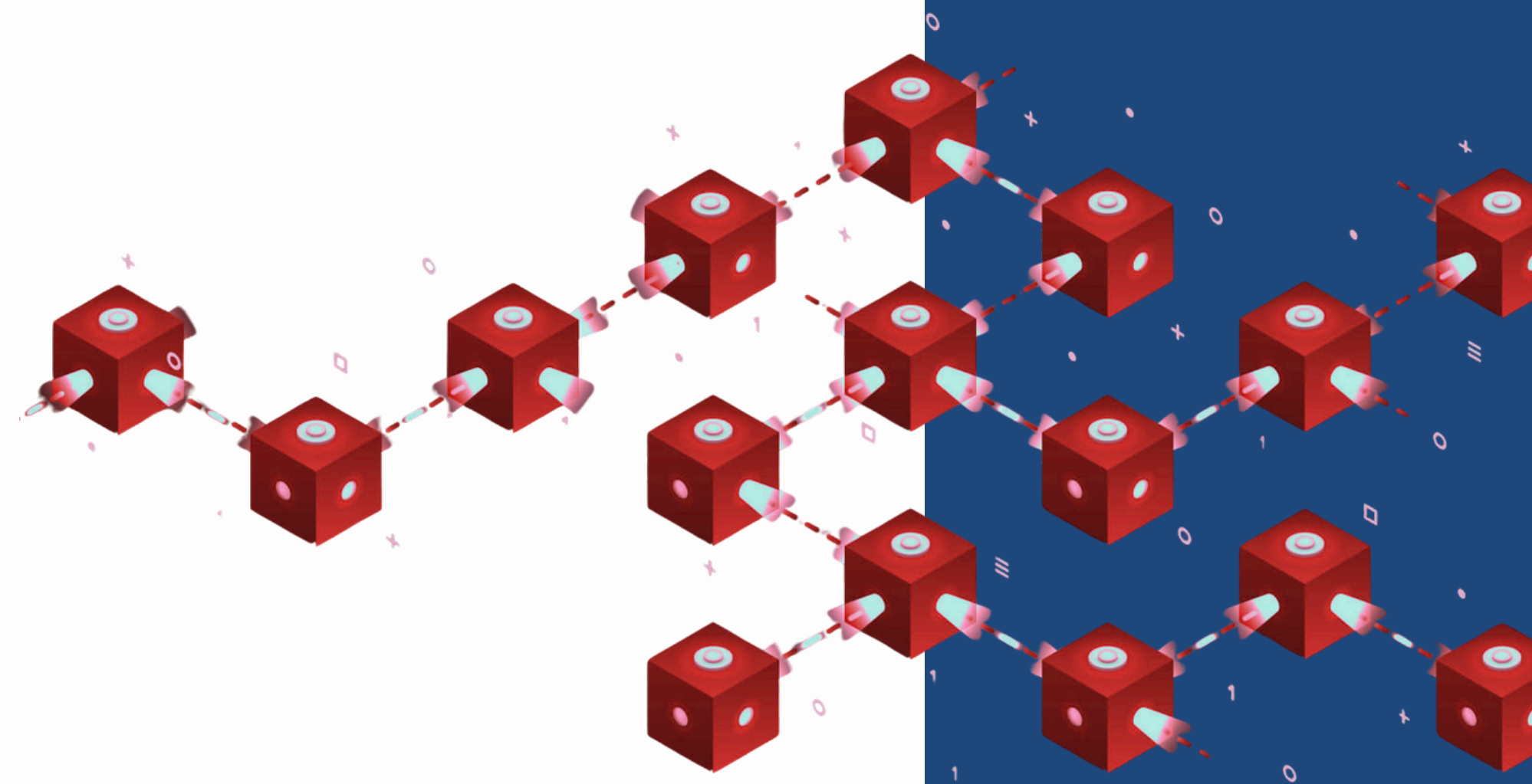
Giới thiệu về Mô hình Giao tiếp Phi tập trung



Kiến trúc Hệ thống chat P2P



Kết luận



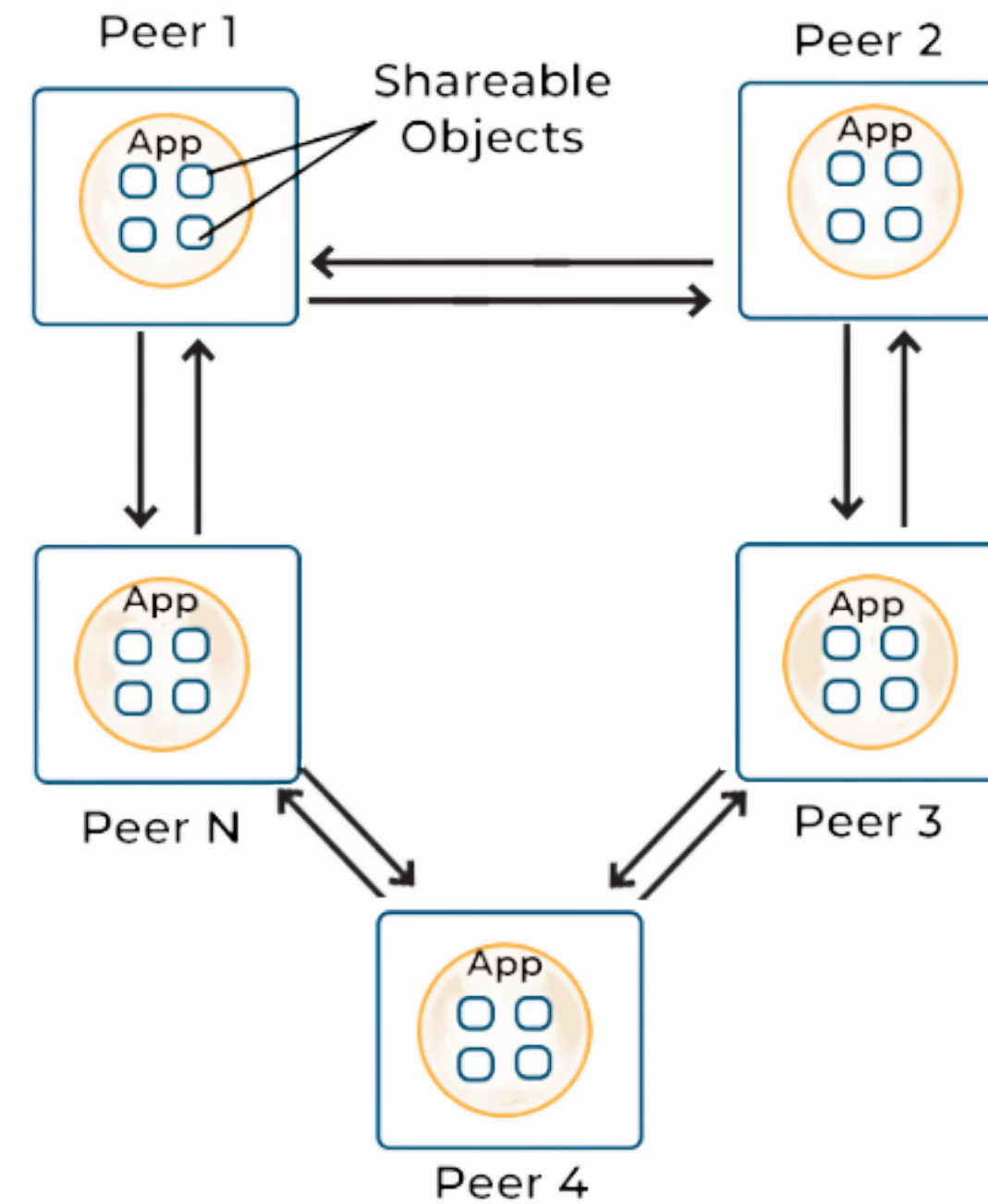
1. GIỚI THIỆU VỀ MÔ HÌNH GIAO TIẾP PHI TẬP TRUNG

1.1. Bối cảnh Chuyển dịch: Từ Client-Server đến Mạng ngang hàng (P2P)

1.2. Định nghĩa và Nguyên tắc Cốt lõi của Ứng dụng Phi tập trung (dApp)

2. KIẾN TRÚC HỆ THỐNG CHAT P2P

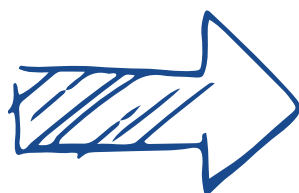
PEER-TO-PEER ARCHITECTURE



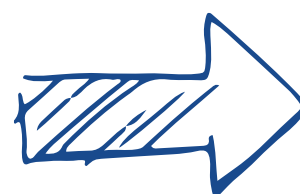
2.1 CÁC MODULE CHÍNH TRONG KIẾN TRÚC HỆ THỐNG



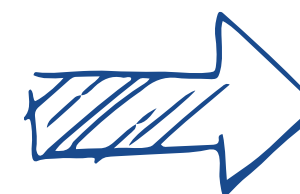
**Định danh &
Xác thực**



Khám phá Peer



**Giao tiếp & Lan
truyền Tin nhắn**



**Đồng bộ hóa
Trạng thái**

2.1.1. ĐỊNH DANH & XÁC THỰC NGƯỜI DÙNG

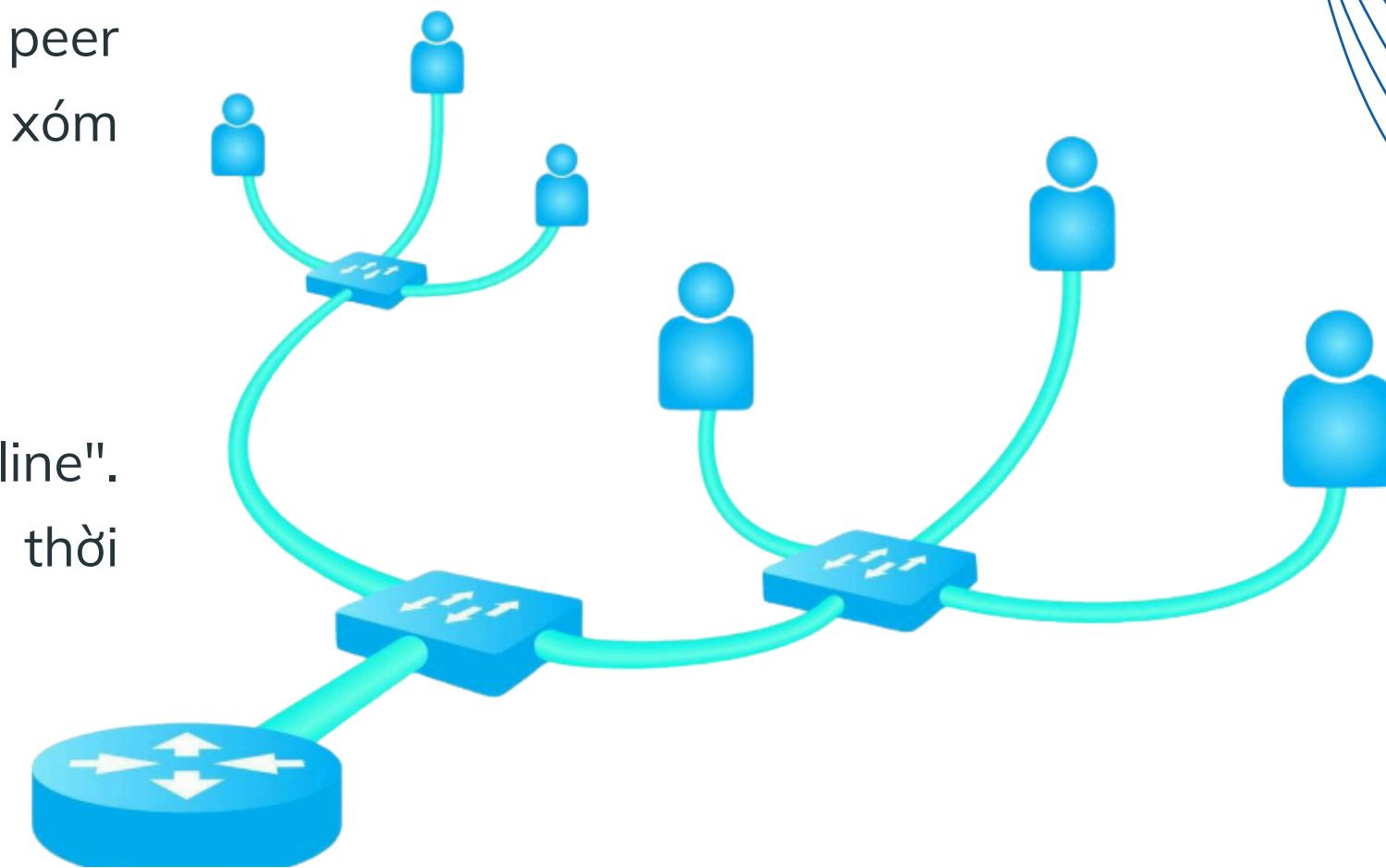
- **Công nghệ cốt lõi:** Mật mã hóa Khóa công khai để tạo ra Định danh Phi tập trung.
- **Quy trình Xác thực:** Dựa trên Chữ ký số.



USER AUTHENTICATION

2.1.2. KHÁM PHÁ PEER

- Giai đoạn 1: Khám phá Ban đầu (Mạng Cục bộ)
 - Cơ chế: Sử dụng UDP Broadcast.
 - Hoạt động: Peer mới gửi một gói tin đến toàn bộ mạng cục bộ. Các peer khác nhận được sẽ phản hồi trực tiếp, từ đó xây dựng danh sách hàng xóm ban đầu.
- Giai đoạn 2: Duy trì Trạng thái Hiện diện
 - Cơ chế: Gửi Heartbeat (Nhịp tim) định kỳ.
 - Hoạt động: Mỗi peer định kỳ gửi một gói tin nhỏ để báo hiệu "tôi vẫn online". Nếu không nhận được heartbeat từ một peer khác trong một khoảng thời gian, peer đó sẽ bị coi là offline.



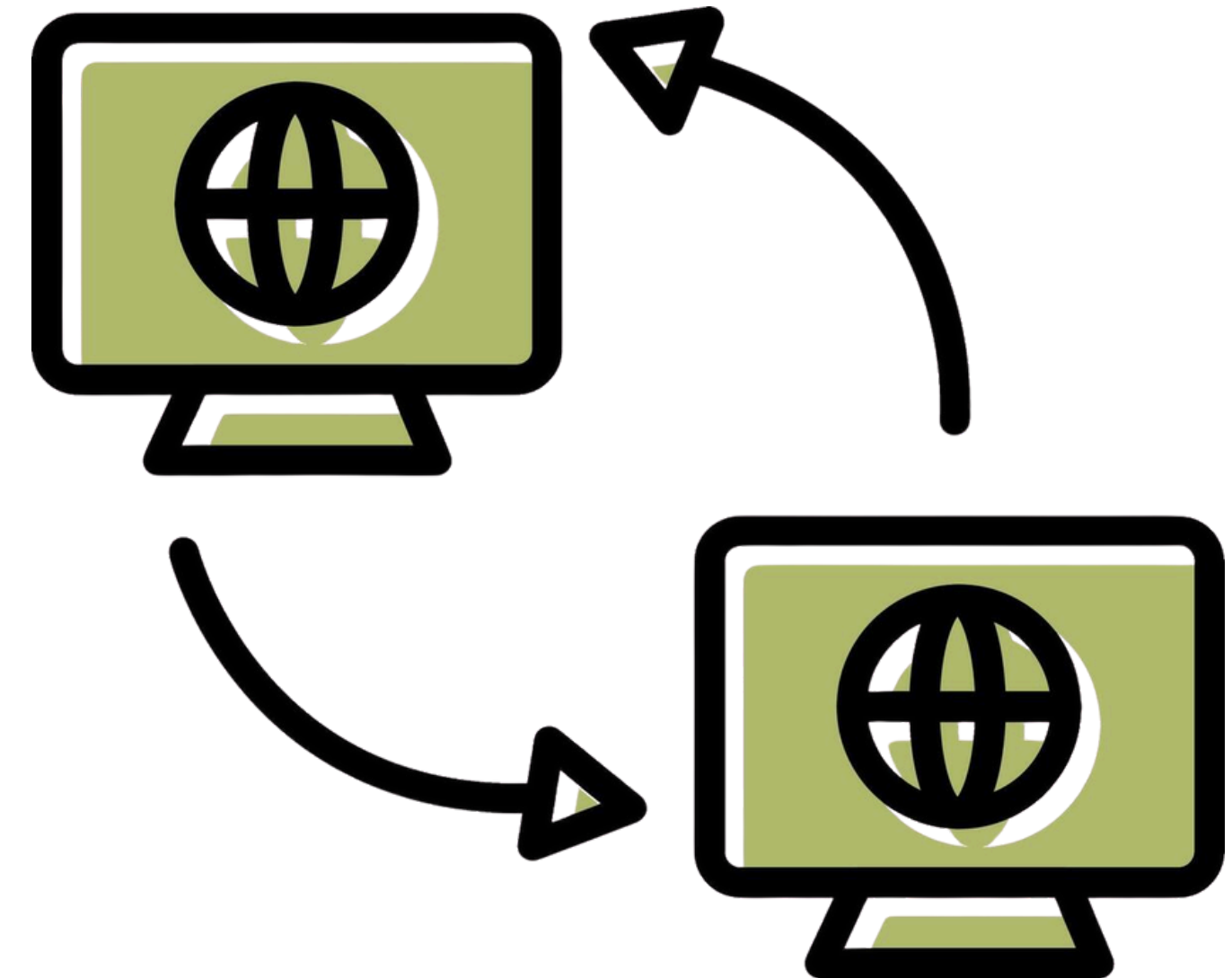
2.1.3. GIAO TIẾP & LAN TRUYỀN TIN NHẮN

- Phân phối Thông tin Hiệu quả với Giao thức Gossip
- Nguyên lý Giao thức Gossip (Epidemic Protocol): Mô phỏng cách tin đồn hoặc dịch bệnh lây lan.
 - Khi có tin mới, một peer chỉ gửi nó cho một số lượng nhỏ các peer ngẫu nhiên trong danh sách hàng xóm ("fanout").
 - Các peer nhận được tiếp tục lặp lại quy trình, tạo ra sự lan truyền theo cấp số nhân.
- Đặc tính:
 - **Ưu điểm:** Khả năng mở rộng cao , chịu lỗi cực tốt do có nhiều đường truyền song song.
 - **Nhược điểm:** Chỉ đảm bảo Tính nhất quán Cuối cùng (Eventual Consistency) , có thể gây ra thông điệp trùng lặp.



2.1.4. ĐỒNG BỘ HÓA TRẠNG THÁI

- **Thách thức:** Làm sao để một peer offline lâu ngày có thể cập nhật lịch sử chat mà không cần tải lại toàn bộ dữ liệu?
- **Giải pháp:** Sử dụng Cây Merkle (Merkle Tree).
 - Cấu trúc: Toàn bộ lịch sử chat được băm thành các "lá". Các cặp lá được băm lại tạo thành các nút cha, cho đến khi chỉ còn một nút gốc (root hash) duy nhất đại diện cho toàn bộ trạng thái.



2.2. LƯUỒNG HOẠT ĐỘNG TÍCH HỢP

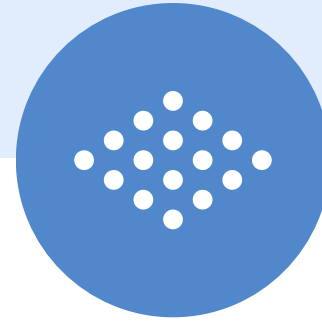
HÀNH TRÌNH CỦA MỘT TIN NHẮN TRONG HỆ THỐNG

- Tạo Danh tính (Module 1): Người dùng tạo cặp khóa Public/Private.
- Khám phá (Module 2): Peer gửi UDP Broadcast để tìm các peer lân cận.
- Xác thực (Module 1): Các peer xác thực lẫn nhau bằng cơ chế Chữ ký số.
- Gửi Tin nhắn (Module 3): Người gửi tạo tin nhắn và "gossip" cho một vài peer ngẫu nhiên.
- Lan truyền (Module 3): Tin nhắn được lan truyền khắp mạng lưới theo giao thức Gossip.
- Đồng bộ hóa (Module 4): Một peer vừa online sẽ so sánh Merkle Root với hàng xóm và chỉ tải về những tin nhắn bị thiếu.

3. KẾT LUẬN

KIẾN TRÚC CHO MỘT MÔI TRƯỜNG GIAO TIẾP BỀN VỮNG VÀ TỰ CHỦ

- **Bền vững (Resilient):** Loại bỏ điểm lỗi đơn, hệ thống có khả năng tự phục hồi.
- **Riêng tư (Private):** Giao tiếp trực tiếp giữa các peer và người dùng toàn quyền kiểm soát danh tính, giảm thiểu nguy cơ bị giám sát.
- **Chống kiểm duyệt (Censorship-Resistant):** Bản chất phi tập trung khiến việc kiểm soát hay chặn nội dung từ trung ương trở nên bất khả thi.



**THANK
YOU!**

