[

](https://ibb.co/LtMxSBL)

Note to the reader: Due to the length of the post it is broken into three parts (sequential ordering). This is a working draft. It may contain errors, incomplete ideas, and incorrect concepts, in particular as it pertains the pseudocode examples. Please feel free to register feedback and / or complaints. I'd like to publish this on the Anoma blog. Feel free to discuss below (in the forums!) for specific questions or DM for out of the scope or more async dialogue.

- Ideas

by @cwgoes and many others!

- Writing and synthesis

by @apriori

- Inspiration

from conversations with @degregat @nzarin @tg-x @vveiln

Thank you to @cwgoes and @0x_Emperor for preliminary review and feedback, which is still being implemented. Review ≠ endorsement.

All errors, mistakes, omissions are my own.

Preface

Multichat is a concept for an Anoma application. The application can be thought of as a distributed chat network without

a central server operator. The history of chat applications is rich, spanning from the original Internet protocols like the Internet Relay Chat (IRC), Extensive Messaging and Presence Protocol (XMPP), AOL Instant Messenger (AIM), and Short Message/Messaging Service (SMS) to Slack, Discord, Discourse, Signal, WhatsApp and Telegram in present times. Multichat demonstrates the principle of separating protocols from operators by allowing developers to customize interfaces for particular types of communication, relying on user trust graphs to identify and maintain connectivity.

Multichat offers a minimum viable feature set that is competitive with existing messaging but can be forked and iterated over beyond a single hackathon event. Multichat's core feature set should include: (i) a messaging protocol, (ii) a user management system, (iii) complex permissioning (iv) message expiry (v) user presence and status (vi) notification system and (vii) end-to-end encryption.

References

It should be noted that this art stands on the shoulders of giants. Most of the ideas, references, phrases, and terminology used come from the following source materials. We recommend the earnest reader to visit these materials before engaging in this art.

[

](https://imgflip.com/i/8ka9ub)

- [The ecosystem is moving: challenges for distributed and decentralized technologies from the perspective of Signal development

](https://www.youtube.com/watch?v=Nj3YFprqAr8) by Moxie Marlinspike

- [Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform

](https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf) by Vitalik Buterin

- [A Federated Architecture for Information Management

](https://dl.acm.org/doi/pdf/10.1145/4229.4233) by Heimbigner and McLeod

- Matrix 1.0: Decentralized Communication at Scale by Matthew Hodgson

- [An Autonomous Ecologist's Guide to Namada and Anoma

](https://www.youtube.com/watch?v=OoS2_QT6_gc) by Christopher Goes

- [Blockchain Nodes are Heterogeneous and Your P2P Overlay Should be Too: PODS

](https://arxiv.org/pdf/2306.16153.pdf) by Zarin, Sheff & Roos

- [Sovereign Domain P2P Overlays, A brief intro to Anoma’s P2P Network

](https://drive.google.com/file/d/1AT9vc0P_ReitBwY3wq0V7L3T88BC9LzD/view) by Naqib Zarin

- [Towards an intent-centric topology

](https://anoma.net/blog/towards-an-intent-centric-topology) by Christopher Goes

- [Rise of the Resource Machines

](https://anoma.net/blog/rise-of-the-resource-machines) by Yulia Khalniyazova

- [How Slack built Shared Channels

](https://slack.engineering/how-slack-built-shared-channels/) by Sun and Demmer

- [Grassroots Flash: A Payment System for Grassroots Cryptocurrencies

](https://arxiv.org/pdf/2309.13191.pdf) by Lewis-Pye, Noar, Shapiro

- The Anoma: Undefining Money - Versatile commitments to valueby Goes, Yin & Brink

Introduction

Multichat is a concept for an Anoma application. The application can be thought of as a distributed chat network without

a central server operator. Multichat demonstrates the principle of separating protocols from operators, or operator - protocol separation. OPS speaks to the unbundling of an existing web 2 business model. For example, centralizing some of the original internet protocols has been a recipe for success. It’s what slack did with IRC, it’s what Facebook did with email, It’s what WhatsApp did with XMPP. Clearly, these companies did more than just fork something like IRC. However, they often used open-source software to bootstrap their product development and then created gated moats of value capture, leaving users with high switching costs while cementing a rent seeking model often referred to surveillance capitalism.

The Anoma Protocol is a distributed operating system on top of which applications can run. Anoma allows developers to rebuild these protocols agnostic of the existing operators on permissionless intent infrastructure. Anoma’s architecture affords developers a rich canvas for experimentation where many existing applications like X (twitter) can be rebuilt to be permissionless, interoperable and customizable for community or organization needs.

There are three common types of chat application networking architectures including (i) centralized server-based, (ii) federated, (iii) Peer-to-Peer (P2P). We’ll take a look at centralized server-based and federated architectures first, and then follow up by exploring P2P designs enabled by Anoma’s network architecture. In addition, we’ll examine Signal as a case study for centralized architecture and [Matrix] for federated architectures.

Signal and Matrix provide users many things they desire. One stated goal of this research is to understand if Anoma can offer anything beyond what already exists on the marketplace. With that said, Let’s begin with centralized architectures.

…