SuiChat

Mysten Labs

Team Name: Sui Squad
Project Name: SuiChat
Company: Mysten Labs

Team Lead: Sophia Weiler
Scribe: Bonnie Huynh

Team Members:

- Sophia Weiler (sophiaweiler@ucsb.edu)
- Chloe Ta (cqta@ucsb.edu)
- Ben Richardson (bwr@ucsb.edu)
- Bonnie Huynh (bonniehuynh@ucsb.edu)
- Ashton Wong (ashton@ucsb.edu)

Mentors:

- Deepak Maram (deepak@mystenlabs.com)
- Alberto Sonnino (alberto@mystenlabs.com)

Project Overview:
SuiChat is a messaging app prototype that circumvents the need for intermediaries in contact discovery and message transmission. Utilizing blockchain technology, the app will facilitate the establishment of end-to-end encrypted sessions and message transmission, mitigating the censorship and coercion risks present in current messaging platforms. By decentralizing the access and providing strong integrity to both the client software binaries and the process of discovering contacts, the app addresses concerns related to binary and key transparency, enhancing user privacy and security.

Problem Significance:
Current messaging applications have become indispensable tools for global communication, but there are many concerns regarding the centralized control and operation of these platforms, specifically regarding censorship, coercion, binary transparency and key transparency. Centralized control of messaging platforms permits selective censorship, potentially leaving users without access to their chat history, contacts, or means of communication, essentially exposing businesses to the risk of market manipulation due to user overreliance. This centralized platform is also vulnerable to government coercion to censor certain parties, including disabling

encryption services or installing backdoors for communication monitoring across platforms. As messaging apps typically operate as closed-source entities, platform manipulation deprives users the ability to verify privacy and security claims made by these services. Despite the use of open-source encryption solutions, users must trust that the client software has not been crafted maliciously or with possible exposure to surveillance or data breaches. Furthermore, end-to-end encrypted channel security relies upon the exchange of public keys, but centralized key distribution leaves way for malicious actors to hijack said keys and intercept communications passing through the channel.

Existing Solutions:
Currently, there exist other messaging applications, such as Whatsapp, Signal and Telegram, that offer end-to-end encrypted messaging, however, they are limited to centralized interactions. For example, it is impossible to fully verify these platforms are using encryption as claimed, user verification requires in-person contact and users lack full control over their messages as apps can censor and delay private messages.

Project Outcome:
The culmination of the SuiChat project will be an encrypted messaging app prototype that utilizes blockchain technology, accessed through a CLI client. If time permits, the CLI client will be updated to a full-stack web application.

Technologies:

- Move
- Typescript
- Sui
- Git
- Blockchain

Milestones:

1. **Familiarization with Sui:** Review Sui documentation to gain a solid understanding of how to send transactions to the Sui testnet using the Sui client binary.

2. **Write a Smart Contract:** Leverage the knowledge from the Sui documentation to write a basic smart contract. Use Sui's SDK to craft personalized transactions.

3. **Cleartext Messaging Prototype:** Implement a simple smart contract that mediates cleartext messaging between users. Maintain a mapping of all users' keys within the smart contract, allowing for identification and routing of messages.

4. **Event-Driven Messaging and Encryption:** Use Sui's event system to avoid storing messages directly in the smart contract. Implement message encryption using an open-source cryptographic library to ensure privacy and security in communication.