Chime: A Distributed Peer-to-Peer Social Communications Network

ALegendsTale (Brandon)
brandon@jollybandit.com
x.jollybandit.com

Abstract. Chime is a distributed network that allows for direct communication with peers. Users can login using a web3 compatible wallet and Chime will fetch the appropriate encrypted messaging private key (MPK) from the Ethereum blockchain. The MPK will be decrypted and allow for the user to access the application while their wallet is connected. Messages are encrypted (using a variation of the signal protocol's double ratcheting algorithm), sharded, and then they are accessible from OrbitDB nodes that have pinned the Data. When the user disconnects their wallet, the application will clear the MPK that was gathered locally during runtime, keeping your messages safe.

OrbitDB

Messages from previous sessions will be displayed if the message meta-data shows that it belongs to that wallet address & if the MPK matches. This allows every user to send private messages.

Login & Profile Retrieval

Profiles can be retrieved after the MPK is successfully validated for that particular wallet. The application will load the user's personal information such as last login, name, and profile picture. Additionally messages & message meta-data will be loaded provided they haven't been deleted.

Settings

- Delete data (messages will require owner address to read. Can only be read after successful validation of address & MPK)
- Set profile picture
- Application appearance modifiers
- Localization support (additional languages)
- Notifications
- Read receipts [default]
- Disappearing messages
- Data settings for toggling when to connect to the network (maybe not needed)

Future Improvements

- VOIP calling feature
- Video calling feature
- Typing indicators (Possible?)
- Money Transfer (crypto)
- Show-off NFTs in messages
- MPK brute force prevention