

# bChat

Plaintext Letters ... and Nothing But

Luke, Sam, John, Matt

# What is bChat?

- **About:**

- bChat is a chat platform which allows users to create simple and secure self-deleting chat sessions

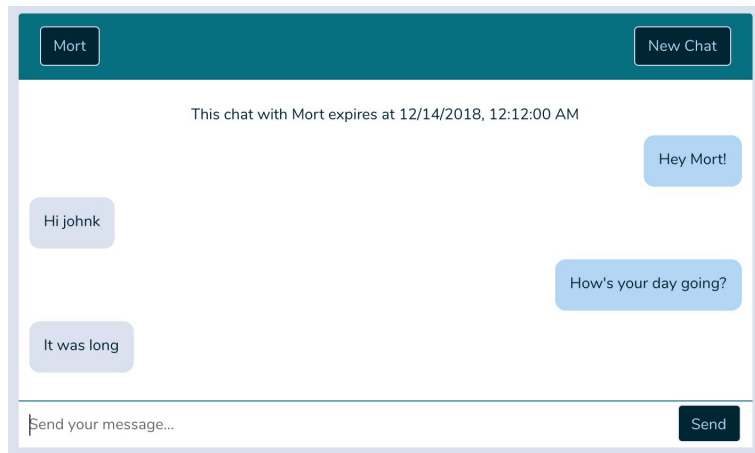
- **Mission Statement:**

- We wanted to fill the desire for simplicity and security in users who have grown weary of convoluted modern communication software by providing a fast, simple, and secure solution.

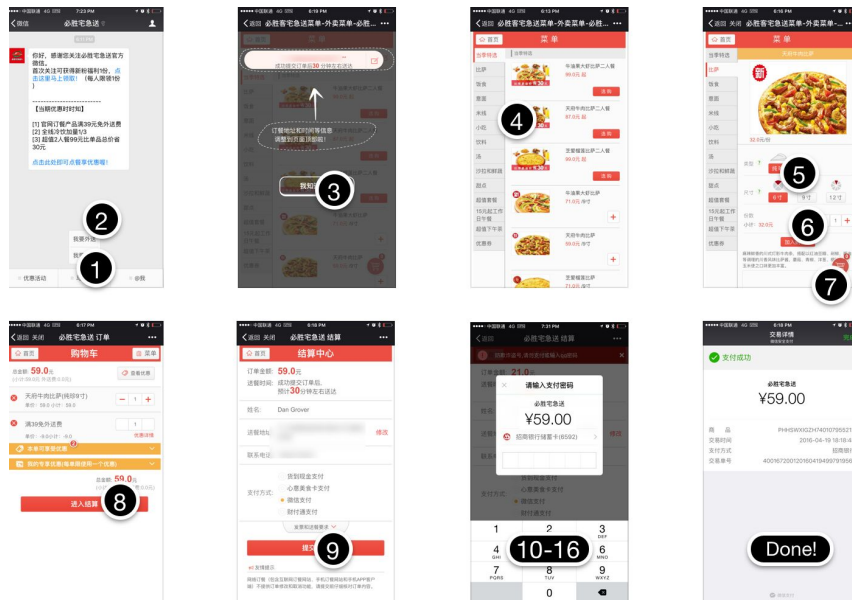
- **Security Features:**

- End-to-end encrypted chats
- Timed deletion of chats

# bChat



All interactions are a click away, and if you want to order food, go to the store's website



16 interactions through a terrible user interface for something which should **not** be in a chat

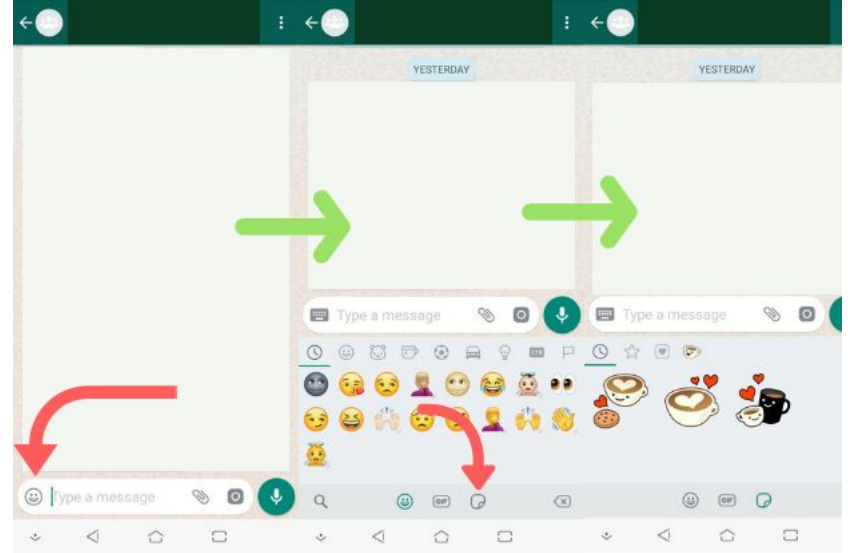
# bChat



Plain text all day. No emoticons, and any sent will be blocked. Nobody wants their conversations cluttered with smiley faces.



# WhatsApp



Ugly stickers and emoticons which makes conversations confusing and silly

# Development Stack (Architecture)



Nginx web server (deployment)



Laravel PHP Framework (back end)



MySQL database



Vue.js (front end)







































Redis server (queuing notifications)

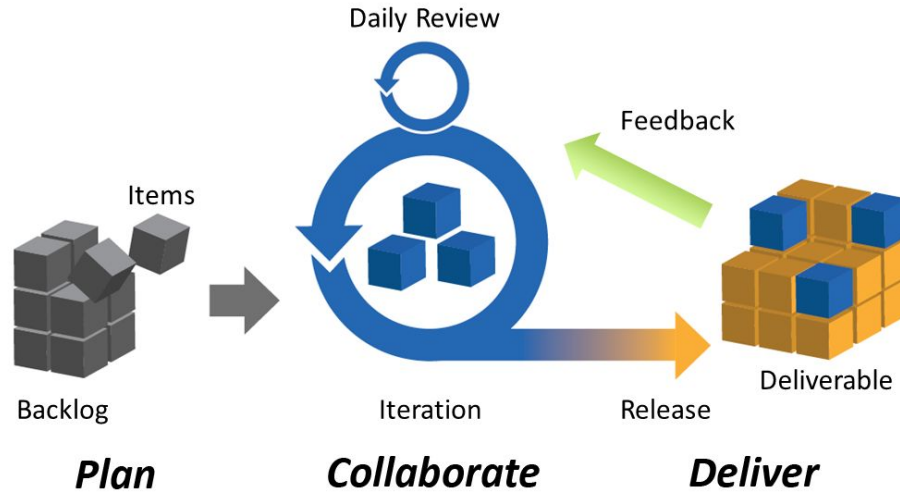


Socket.io (web sockets)

# Tools

Project Tracker:		    
Communication Platform:		    
VCS Repository:		    
Database:		    
Testing Tool:		    
Deployment Environment:		    

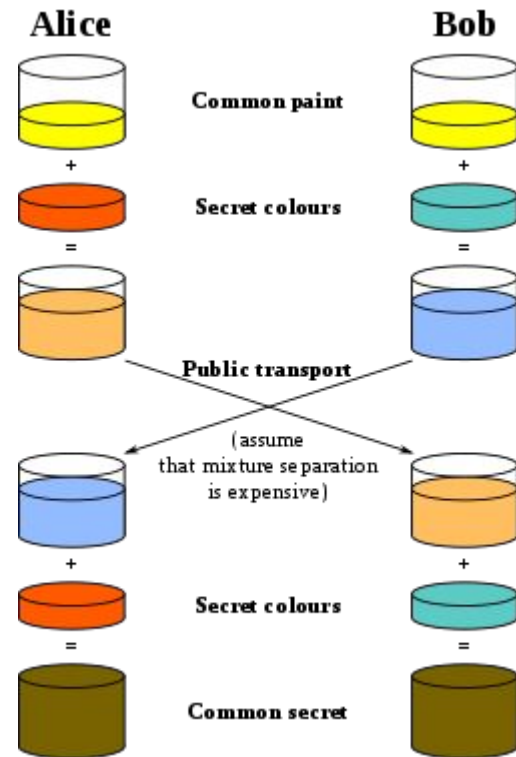
# Project Management Method: Agile



But...

# Let's Talk Encryption

- bChat utilizes end-to-end encryption
  - If the server is compromised, the messages are undecipherable
  - Users exchange a shared secret using ECDH, converted into an AES-256 key using HKDF
  - Encryption keys stored on the client



id	chat_id	message_content
1	1	c0519f327f9b4bda92a79474566755b4d04881f8101dc4ec7ee03a517de685dd32e160856c2bdf0b529b2a8ab48c7469ecdaa318cf9815cadcd3ed4f
2	1	c0519f327f9b4bda92a79474567849b9cc1181f8101dc4ec7ee03a517de685dd32e160856c2bdf0a5a992b8fb28c7469ecdaa318cf9812dcdcd4bc41be7d98



# Lessons Learned

- Make the scope of your project, and each sprint, reasonable enough to accomplish in order to provide a deliverable.
- Ensure frequent communication to allow for strict collaboration.
- Thoroughly understand frameworks and tools in order to make the most effective use of them.
- Survey strengths and weaknesses of team members to allow each member to make maximum contributions.

*Demo*

*Questions?*