TOPIC: SECURITY

A DECENTRALISED CHAT WEB APP

SECURECHAT

Sahil Gangurde

sahilgangurde08@gmail.com

https://github.com/lostmartian/securechat

Addressing the issue

- There have been many issues regarding data leaks in top multinational tech companies which have data of millions of users. This data leak may happen due to many factors in which one of the factor is insecure server or a failure in backend programming.
- The solution for this problem which I am proposing is the use of blockchain to store information of users which will be available to everybody but still nobody could access it.
  - If anybody tries to break in the private data of other user then that would disturb the whole chain of system and we would get to know the data which is being leaked and also that would only happen with a small number of accounts because tampering 1 data on blockchain requires a LOT of effort.

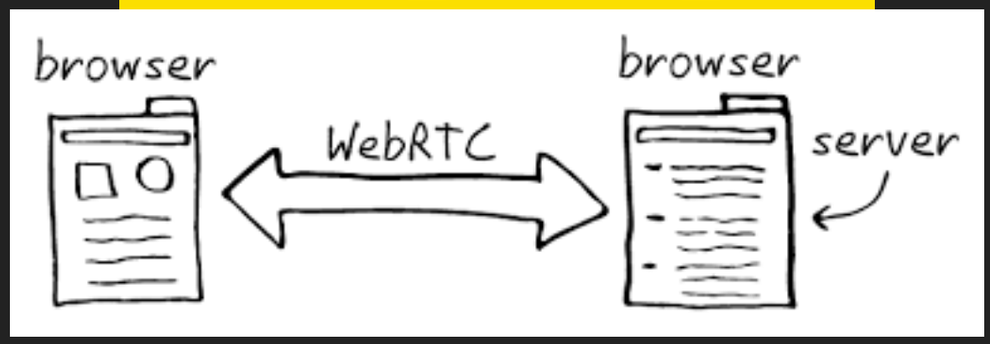
This bigger issue can be addressed via a small chat application where every user's data is protected and is anonymously chatting with people from a particular chat room

HOW “SECURECHAT” PROVIDES SECURITY ?

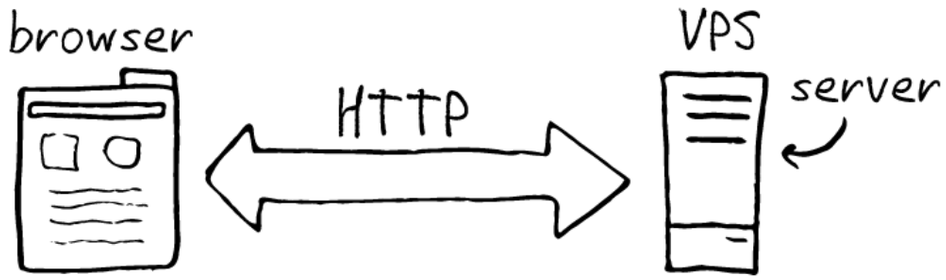
- It works on the principle of blockchain technology. Each time a user enters in a chat room a unique token is assigned to that user having a public key which looks like kind of a bitcoin key. This key is unique for every user and the user cannot modify in his/her details through these keys. A new contract is created as it is done in blockchains.
- At every refresh the user is given new tokens so user tracking is near to impossible.
- Also if any person want to hack user’s account during the live session then he has to mine the cryptocurrency which is a heavy task as it involves lot of machine power(almost a mini supercomputer) and is also very very costly.
- No servers or hosting platform is involved in it. The messages are send to each other via p2p (peer to peer) protocol. Hence, the messages travel from your device to other person’s device without being stored into any database.

TECH STACK

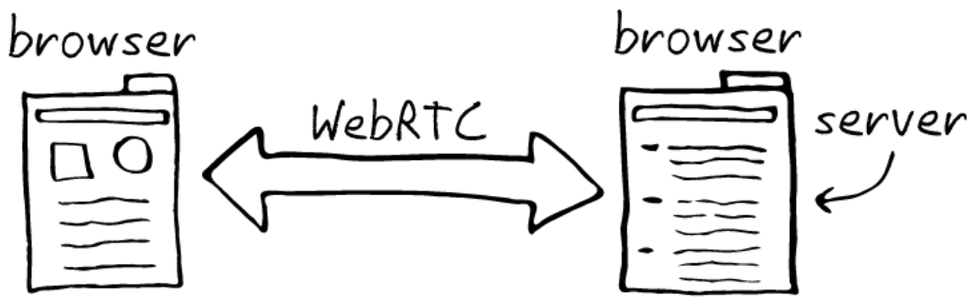
- HTML5, CSS3
- BootStrap
- NodeJs
- Vanilla Js
- WebRTC
- BlockChain



Backend Features

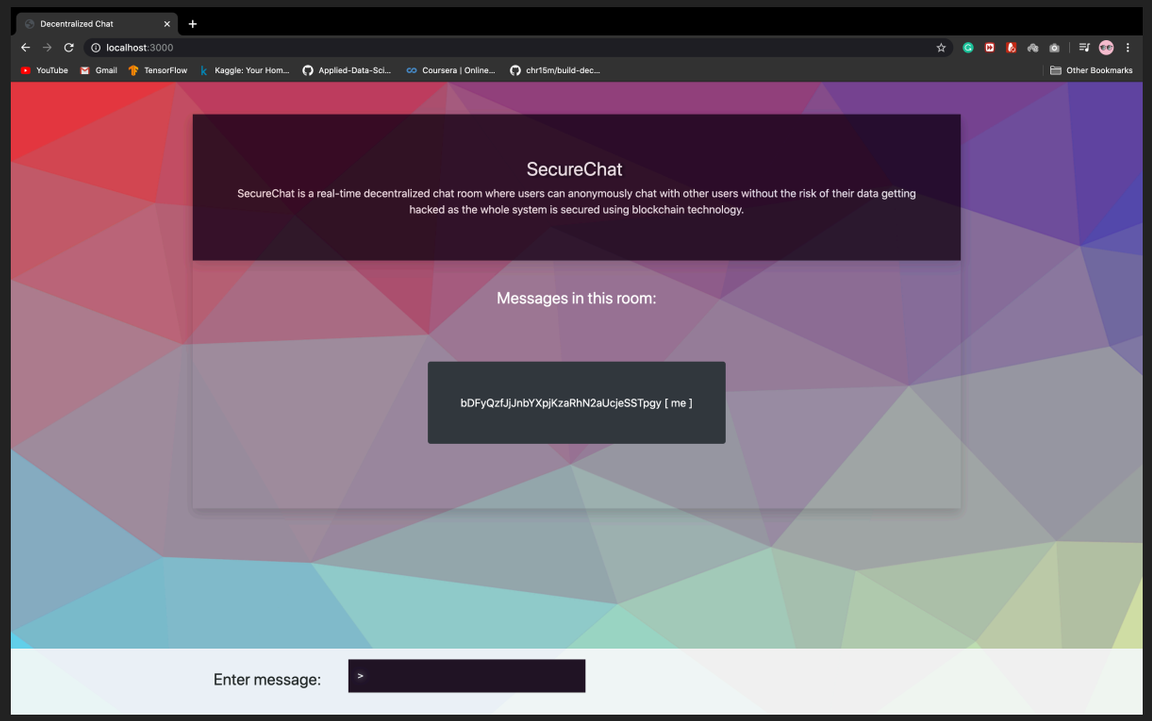


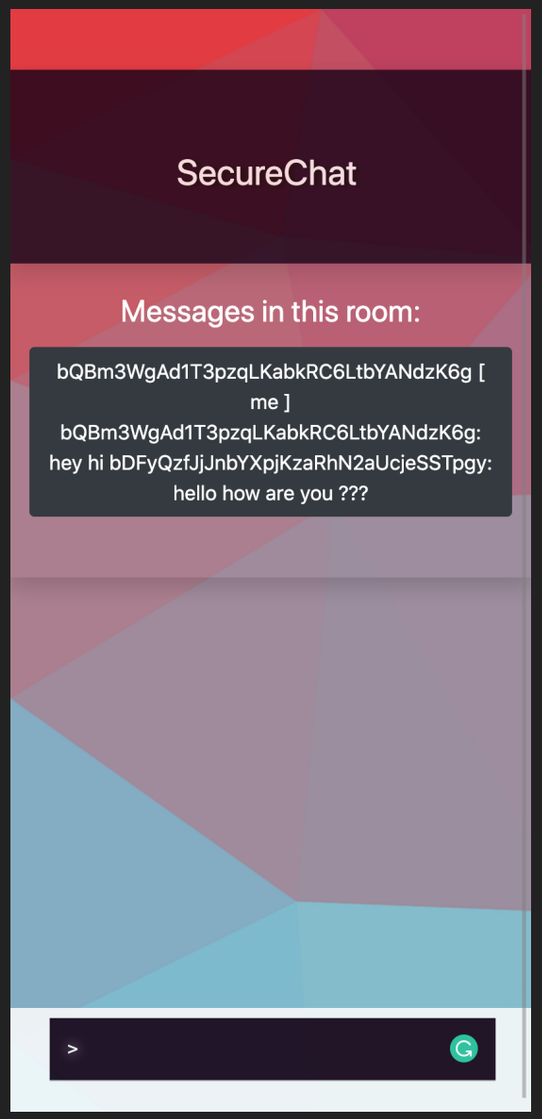
Old Method



New Method

- Easily send messages directly between browsers.
- Write servers that run in a browser tab.
- Host backend services without a VPS, domain or SSL cert.
- Easy to deploy & "self-hosted" servers by leaving a browser tab open.
- Client-server over WebRTC instead of HTTPS.





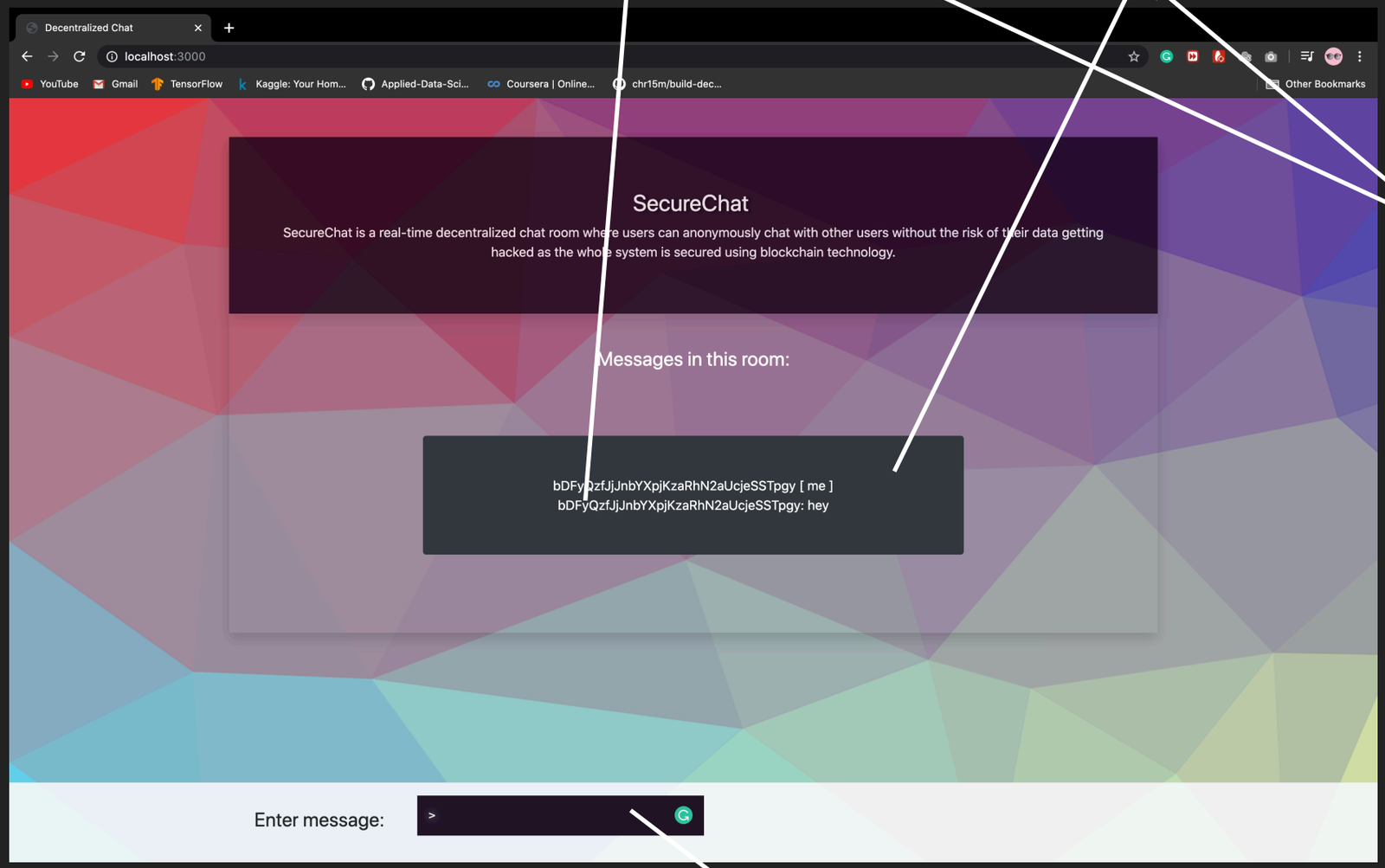
FrontEnd Features

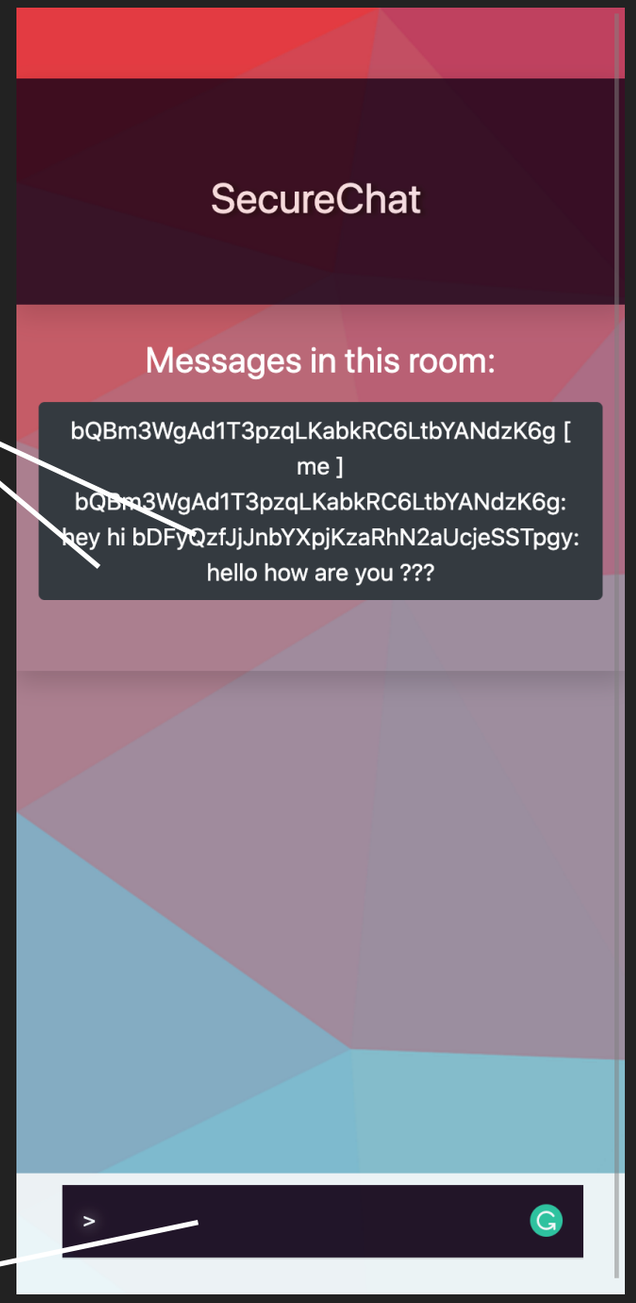
- Responsive Design mobile friendly
- Pleasant colour with good UI/UX
- Easy to use interface with minimalistic design approach

UI Explanation

Unique tokens of users

List of messages





Field to enter messages

HOW TO SETUP THE ENVIRONMENT TO RUN THIS SITE ?

- Offline
  Read the instructions given in the readme.md file on GitHub repo https://github.com/lostmartian/securechat.
- Online
  Visit https://chatchain.000webhostapp.com/