# Decentralized Chat System

Ann Sarah Babu
S3-A

# Relevance of topic

- A decentralized application for communication and resource sharing is need in today's world, where keeping data on a centralized server can be risky and costly experience.
- By implementing Blockchain technology, we can create a secure and reliable messaging application that overcomes the drawbacks of traditional messaging applications.
- As the name suggests, a decentralized application does not have a centralized server, control is distributed between participants in the system.
- In our application all the user data is stored on a block which is connected to other blocks forming a chain.
- Also the data that is stored in block is almost impossible to view as a very secure encryption and hashing functions (256 bits) are used, if a hacker tries to make changes to the information in block then, he/she will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible.

# Description

- Decentralized application make use of peer-to-peer networks, this ensures that no network failure can occur.
- Blockchain serves as an immutable ledger(the ability to remain unchanged).
- The decentralized application is implemented on Ethereum blockchain network.
- Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority.
- Ganache is used for setting up a personal Ethereum Blockchain for testing your Solidity contracts.
- MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

- Ethereum platform allows you to send encrypted messages through smart contract.
- Only you and the recipient of a message can decrypt it.
- Every Ethereum account has a private key and a public key associated with it.
- The private key is what you have to keep in secret (or your wallet software will keep it in secret for you).
- The public key will be shared on the blockchain network (so that other people can interact with your account).
- If someone got your private key, they will be able to control your Ethereum account and able to decrypt all your messages.

# Objectives

- To provide more secure environment for chatting and resource sharing.
- To provide more efficient system that works even if a node in the network fails.

# Existing System and Proposed System

- WhatsApp, WeChat, etc, these traditional applications have taken all over the internet. There is a centralized server which stores all the information including identity to chats. Generally, these chat applications based on the following:

- Centralized Management: In this management system, entire correspondence goes through the company's server which can govern its rules.
- Centralized Architecture: In this architecture, there is only single server which is maintaining all the services.
- Confidentiality: Confidentiality of a user can be compromised on the request of government.
- Single Point of Failure (SPF): If a single node fails then whole application can be compromised.

- The above encouraged us to build an application where, we can have all the features like: Decentralized storage, Data security and Data immutability.

- In our application, we are using the approach of decentralized application (DApp).
- All the user data is stored on a block which is connected to other blocks forming a chain. It is a peer-to-peer network.
- And, tampering the data which is stored on the blockchain is quite impossible because, of the encryption algorithm.
- If malicious user tries to make changes to the information in block then, he/she will have to make changes to all the copies of that block on whole blockchain network and that can be quite impossible.
- Though blocks are on all nodes, they cannot access the information in it, only the person for whom the information is concerned, they can only access.

# Modules/Sub-tasks

1. Environment setup

   We have to install all the needed dependencies and environements.

   Here is a list of the dependencies we need to install:

   • node.js

   • metamask

   • truffle

   • ganache

2. Deploy  smart contract

   2.1: Connect metamask to the browser

   2.2: Create the smart contract

   2.3: Deploy the smart contract

3. Send message

   3.1: connect to all the available wallet addresses available in Ganache

   3.2: send messages between these addresses

   3.3: monitor the state of the blockchain in real time when the transactions are executed

# Front end, Back end and Algorithm

- The front-end of Decentralized application is built on NodeJS.
- The backend of the decentralized application is Ethereum network.
- SHA-256 algorithm

  In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key.