II. Literature Review

To adequately prepare for the coming solutions discussed in this paper it is necessary to go over several primary technologies. These being Blockchains and Tor which will be used in the implementation of the proposed decentralized messaging application.

Blockchains are a subsection of cryptographic techniques that chain data together using hashes that prevent unauthorized changes being made to the chain []. In the context of this paper blockchains are most often used to share information between large networks of anonymous computers. This allows for a distributed database with high data integrity that only allows for the original owners of the data to change it []. This can simulate peer to peer data transfers but is often **too slow** for large amounts of data to be sent or stored.

Blockchains used for distributed computing are described in the Ethereum yellow paper[] as a "simple application on a decentralised, but singleton, compute resource". The Ethereum blockchain takes this idea and uses it to create a generalized block chain that works as one distributed computational resource. Resources are managed via transactions that are signed off on using cryptographic techniques that verify their authenticity []. The method that the Ethereum network uses is known as a Blockchain []. The Ethereum blockchain is a ledger of information with each entry being tied to particular account known as a "wallet". Each time this ledger is updated all computers on the network verify the authenticity of the update with proof of stake algorithms. Computers are motivated to update the ledger via payments of a token called "gas" [] and updates being known as transactions. When a transaction is made the user who initiated it will pay a small fee in gas depending on the size of the transaction and the load the network is under. The nature of the block chains cryptography allows for near absolute certainty of the validity of a transaction []. Another well known blockchain is Bitcoin, which differs from Ethereum in that is can only store information relating to how much bitcoin a wallet owns. Ethereum allows for the storage of many different types of information such as code, which the network is able to use to run decentralized apps. This ability to store predefined behavior that operate securely on a distributed network is why it is the choice blockchain for this paper. The major downside of Ethereum however is its greatest strength. Due to the open nature of the ledger every computer on the network is able to see all the data in the ledger. Transactions can also be limited based on how much stress the network is currently under as well. To complement Ethereum a second technology discussed below.

Tor is a networking protocol that anonymizes internet traffic. It works via encrypting data which is then sent through the tor network. The network is made up of many peer to peer connections that bounce your data around preventing any one sever from knowing where your data is going and where it came from []. Tor is an open source project that was originally created by the US navy to hide secret communications []. Since then it has seen wide adoption by the greater public for accessing network resources like websites anonymously. The core interest of this project in tor is its ability to host resources anonymously. Using Tor nodes as rendezvous servers (Severs that allow clients behind network address translators to communicate) it is possible to host servers located behind firewalls []. This secure true peer to peer behavior would allow each user on a communication network to be their own message server. Combining Tor and the Ethereum network allows for decentralized anonymous network traffic to be directed by a decentralized authority that can verify users securely and anonymously. Several other projects have attempted to create similarly secure apps which will be discussed below

D.I.M Or Decentralized Instant Messenger is a software that uses the GunJs framework to implement a distributed messaging app []. GunJs provides tools to create distributed databases (DDB) across many nodes []. This allows for network of self hosted server nodes that store user information. Client nodes on the network are able to read information from the DDB which allows for user verification and logins from any device. The main benefit of this model is that it is easily used by users who just need to install the app or access the web portal. However, This structure lacks several features due to the server node client node model, it is not truly peer to peer even though it is distributed. However this model has no single point of failure communication besides access to the web portal or app and uses encryption methods to maintain and ensure transactions on the DDB are legit. Making it secure and easy to use. The next project that will be discussed in this literature review has the most similar structure to the proposed solution of this paper.

Muhammad S. A.[] proposes a solution not for a chat app but a way for patients to transfer data from smart sensors to their doctors securely and without a middle man. In [] two technologies are focused on to allow for a secure peer to peer architecture. [] states that they use the Ethereum block chain for "a medium for negotiation and record keeping" and that tor is used for "Delivering data from patients to doctors". This architecture is favorable for the medical setting due to its ability keep data in the hands solely patient and the doctor. [] uses the blockchain for identity management and thus is able to securely transfer the data between doctor and patient using tor rendezvous servers. This is true peer to peer communication and since its using tor it has the added benefit of hiding user metadata such as origin IP.