

Due to the advent of the internet, the issue of privacy has become ever more prevalent. Large companies use the lack of technological literacy most citizens possess to their advantage by convincing them to opt into giving up information they didn't even know could be used against them. Google, Amazon, Apple, Facebook, and even some big box retailers like Walmart collect vast amounts of data that they sell off or abuse which Bruce Schneier discusses in his book *Data and Goliath* [?]. This abuse comes in many forms but one of the most common is using your data to target you with ads or media to increase your use of their services [?]. Multiple types of technologies have risen to help bring some control back to the average citizen. The Onion Routing project (Tor), an internet networking system, uses algorithms and information hiding techniques to deliver information to websites across the internet without them knowing where the data came from [?]. This keeps websites from tracking data about users. Multiple blockchain technologies like Ethereum have also taken advantage of cryptographic technologies to validate transactions anonymously. Allowing users to pay for items or make exchanges of data securely without the personal information of either party being known, skipping the bank all together. Both of these systems work using a similar principle called decentralization, which allows for large computer networks to work securely with each other to accomplish a goal. These examples are also open source as well, allowing anyone to connect and run a computer to help grow or use the network.

With Facebook, Google, Microsoft, Apple, and Amazon being responsible for almost all of the online communication channels we use today, it is only a matter of time before they start pulling data from private chats. This would be a huge breach of privacy but does already happen when the governments request information from these organizations such as with Amazon who co-operates with police when asked for Ring doorbell data [?]. This shows that they have the capability to access this data as well as the motive. Noctua seeks to solve this problem before it starts, implementing peer-to-peer messaging in a secure and decentralized way. By combining the Tor network and blockchain technologies like Ethereum, it can securely move data between devices on the internet without a centralized middle man. This peer to peer structure allows for you to be in complete control of your data, with no entity to step in the middle. Only people you know and have given permission to can message you using proven cryptographic techniques that encrypt your data with personal keys that you can change. Data, stored locally, gives you the agency to completely delete if you feel it's necessary, giving you complete control.