Decentralized Chatting App

***Abstract-* The present software technology aims on the security of apps or any other software platforms due to the modern days cryptographical threats. A decentralized application (dApp) is a type of distributed open-source software application that runs on a peer-to-peer(P2P) blockchain network rather than on a single computer. DApps are visibly similar to other software applications that are supported on a website or mobile device but are P2P supported. Decentralized apps more secure than centralized as it does not get to store the data in a particular server rather it directly deals with only two parties-sender, receiver. As the decentralized apps are open source required changes can be done by other users when the codebase is available to all users for evaluation. Peer-to-peer is a decentralized communication model which only includes only two nodes. The peer-to-peer philosophy and network architecture eliminate the direct top-down relationship between clients and their servers in favour of linking each connected individual as a peer, eschewing the centrality of traditional networks by placing the focal points at each individual computer.**

**INTRODUCTION**

In application like messaging apps and data mining, security is the first and foremost thing to be concentrated necessarily. Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the “chain,” in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a ‘digital ledger’. Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure. In simpler words, the digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which, the transactional records are stored based on actual purchases. The fascinating angle is that anybody can see the data, but they can’t corrupt it. Technologically, Blockchain is a digital ledger that is gaining a lot of attention and traction recently. Record keeping of data and transactions are a crucial part of the business. Often, this information is handled in house or passed through a third party like brokers, bankers, or lawyers increasing time, cost, or both on the business.

LITERATURE WORK

Blockchain avoids this long process and facilitates the faster movement of the transaction, thereby saving both time and money. It uses a digital signature feature to conduct fraud-free transactions making it impossible to corrupt or change the data of an individual by the other users without a specific digital signature. Conventionally, you need the approval of regulatory authorities like a government or bank for transactions; however, with Blockchain, transactions are done with the mutual consensus of users resulting in smoother, safer, and faster transactions. It is programmable and can generate systematic actions, events, and payments automatically when the criteria of the trigger are met. Blockchain is a combination of three leading technologies:

1. Cryptographic keys.
2. A peer-to-peer network containing a shared ledger.
3. A means of computing, to store the transactions and records of the network.

Cryptography keys consist of two keys – Private key and Public key. These keys help in performing successful transactions between two parties. Each individual has these two keys, which they use to produce a secure digital identity reference. This secured identity is the most important aspect of Blockchain technology. In the world of cryptocurrency, this identity is referred to as ‘digital signature’ and is used for authorizing and controlling transactions. The digital signature is merged with the peer-to-peer network; a large number of individuals who act as authorities use the digital signature in order to reach a consensus on transactions, among other issues. When they authorize a deal, it is certified by a mathematical verification, which results in a successful secured transaction between the two network-connected parties. So, to sum it up, Blockchain users employ cryptography keys to perform different types of digital interactions over the peer-to-peer network.

There are four different types of Blockchain Networks. They are as follows:

* Private Blockchain Networks
* Public Blockchain Networks
* Permission Blockchain Networks
* Consortium Networks

## Private Blockchain Networks:

## Private blockchains operate on closed networks, and tend to work well for private businesses and organizations. Companies can use private blockchains to customize their accessibility and authorization preferences, parameters to the network, and other important security options. Only one authority manages a private blockchain network.

## Public Blockchain Networks:

## Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularizing distributed ledger technology (DLT). Public blockchains also help to eliminate certain challenges and issues, such as security flaws and centralization. With DLT, data is distributed across a peer-to-peer network, rather than being stored in a single location. A consensus algorithm is used for verifying information authenticity; proof of stake (PoS) and proof of work (PoW) are two frequently used consensus methods.

## Permissioned Blockchain Networks:

Also sometimes known as hybrid blockchains, permissioned blockchain networks are private blockchains that allow special access for authorized individuals. Organizations typically set up these types of blockchains to get the best of both worlds, and it enables better structure when assigning who can participate in the network and in what transactions.

## Consortium Networks:

Similar to permissioned blockchains, consortium blockchains have both public and private components, except multiple organizations will manage a single consortium blockchain network. Although these types of blockchains can initially be more complex to set up, once they are running, they can offer better security. Additionally, consortium blockchains are optimal for collaboration with multiple organizations.

Here, in our app we are using “Public Blockchain Networks”.

## OVERVIEW OF MESSAGING APPS:

There are lot of difficulties while using instant messaging or other Application based messaging because we don’t know what’s happening the two parties-sender, receiver. The message is sent to the server obviously the trust of the server is based on the app we use for messaging. There’s a lot a server can do right and that’s what the signal protocol uses and by association. The sender sends a few things to the server along with the public key which is his/her identity. This is going to be the public key on an elliptical path. It also sends a private key or a private component associated with it which will remain only with himself. There will be an exchange on the pre key bundle. The only way we can verify the identity of the parties is only to verify each other’s public keys by our identity keys. This works in a way that both the identity public keys are combined using a hash function into a safety number, this safety number means we are having a conversation with the text. Overall, same two identity keys, we are having a same conversation that’s the idea. In signal you can press this a verified button which says we’ve looked at these out-of-band communication because we’re not using the normal encryption to verify our keys. So now actually when we send messages it will show as verified. So, in whatsapp it is known as security code.

## DECENTRALIZED MESSAGING PROCEDURE:

Decentralisation is exactly what it sounds like: the polar opposite of centralisation. Control is distributed between participants in the system, rather than being held by a central authority. The government of a democratic country is a centralised authority, but the people put that government into power through a decentralised process: voting. In decentralised computing, instead of a network being governed by a central server — and controlled by a central authority — control is held by a distributed network of nodes (servers). These nodes make democratic decisions about the network, with all (or some, depending on the protocol) nodes “having a say”. This collective works together to handle tasks like data traffic routing and maintaining network security. The most secure decentralised end-to-end encrypted messaging apps send messages by routing them through a random selection of nodes on the network.

The set of nodes being used changes with every new message. If a malicious node was trying to collect data about users’ messaging activity, it could only do so for messages relayed directly through it — a tiny fraction of the total message traffic on the network. Onion routing protocols add additional layers of security by encrypting a message multiple times, once for each server it passes through on its way to the destination. If onion routing is in use, malicious servers can’t even track messages passing directly through them, as they are only aware of the node before and after them in the chain. A decentralised, end-to-end encrypted messaging app is trust less because you do not need to place your trust in anyone when using it. You know that your conversations are anonymous and secure — no trust necessary. Decentralisation makes it impossible for third parties to compel the network’s creator to provide information about users, because in a fully decentralised system, the entity which created the network does not have the capability to collect that information. Decentralisation also significantly limits the data a malicious third party could collect if they attempted to hack into the network.

An attacker would need to gain access to the vast majority of nodes on the network to collect any specific user’s conversation data — much more challenging than just hacking into a central server. Centralised encrypted messaging apps are trusted systems. Users have to trust that the central authority won’t act in bad faith by collecting conversation data for themselves or for third parties. Centralised systems are vulnerable to software or hardware bugs and other failures. If a disaster takes down the central server, the whole network goes down. Central servers make it simpler for malicious third parties to hack into the network. And as if that wasn’t enough, centralised systems are vulnerable to censorship. If the central authority decides to ban you — or if a third-party pressure them to do so — there’s nothing anyone can do to stop it.

Decentralised encrypted messaging apps are trust less systems. You don’t need to place your trust — or your privacy — in the hands of a controlling entity when you use a decentralised messaging app. There is no central authority to collect, sell or give away your conversation metadata, and if the messaging app is using onion routing, the decentralised servers can’t collect any data either. Decentralised systems can tolerate losing servers to software bugs, hardware failures or natural disasters. Finally, decentralised networks are censorship-resistant by design. There’s no central authority making decisions about who can use the network — so there’s no chance of users, groups or countries being blocked, banned or censored. You can never trust centralised networks to be private, secure, or safe from censorship. Decentralised networks remove trust from the equation completely.

**CONCLUSION**

Thus, the decentralized chatting app we develop is ensured for security, privacy. The decentralized networks don’t rely on a central server, the network is unaffected if unforeseen circumstances cause nodes to go offline. The network will simply route messages through other, unaffected nodes. This makes decentralized networks far more resistant to natural disasters and power outrages.