# **Possible attack on Private Messaging App based on Blockchain**

# 

One of the biggest problems of modern messengers is the lack of privacy. While many apps use secure technologies and strong encryption to make messages hard to crack, it does not mean that users’ private data are properly secured. This problem may be solved with blockchain.

**Messaging and privacy**

Nowadays there are literally dozens of messaging apps out there. Some of them claim to be secure and protected, but in practice not everything is that simple. This is due to several different reasons.

First of all, many popular messengers are owned by big corporations that want to collect as much information as possible. Facebook social platform which also operates its own Messenger, collects information and content provided by users, their connections, data about app usage, transactions and even information others provide to a certain user! This data is then used for advertising and other purposes.

Another important aspect is that most current communication tools are “closed source”, meaning that the code of these products is never published and independent researchers cannot audit it. This provides an opportunity for malicious actors to find security flaws and exploit security holes in order to steal personal information.

Finally, traditional messengers are centralized, which is also bad for privacy. Take Telegram, one of the most secure chat apps out there. It is centralized, meaning that the government can just block it, which has already happened to the service in Iran and Russia. Users in these countries are experiencing problems with access to Telegram, which may force some of them to switch to less secure alternatives. This also makes online communication less private.

**All these problems raise questions about how blockchain technology can be used to solve them?**

One of the possible applications is data storage. Blockchain can be used for distributed data storage. The main idea here is to distribute your data across a network of peers, all over the world instead of trusting your personal information to a centralized party like Facebook

# **What can go wrong?**

Some peoples are saying:

Storing all of your sensitive private messages to a permissionless blockchain might be one of the most stupid things

There is a reasonable point in this emotional comment. Translating this into more technical language, we can say that unlike **centralized messengers** that rely on the security of their servers, blockchain-based apps provide free access to encrypted data.

Therefore the **security is provided by cryptography**, and if it is weak, data could be hijacked.

The Blockchain saves messages forever.. What if later quantum computers come out? The encryption might be broken then? It is shallow thoughts:

* Blockchain cannot be decrypted entirely, as each account possesses its own key
* Even if a decryption method existed, it would take resources and time (money) even for quantum computers
  + Blockchain allows us to create chats that can be deleted with the help of side-chains (every chat is started as a side-chain and then removed)
* Blockchain has speed limitations as well. Even the fastest blockchain-based messaging tool will always be slower than traditional messengers with each message delivery time taking up to several seconds.