TrezarMessage

Oliver Ziegler, David Walton, Peter Bushnell

trezarcoin@chekaz.dev, david@waltion.io, bushsolo@gmail.com

Abstract

A big problem in today's society is trust, especially when it comes to personal data. Today's messenger apps all promise to be end-to-end encrypted, but it's hard to verify. In most cases, the data is stored on internal company servers. Furthermore, for secure encryption, an encryption key is needed, which in modern messenger apps is either unknown or is only known and stored on internal servers of the company in question (e.g. WhatsApp). It is therefore not guaranteed that the messages are ever securely encrypted or if there is a hidden masterkey which can decrypt any of these messages. TrezarMessage addresses exactly this point, seeking to fill this gap and present a decentralized, end-to-end encrypted messenger.

Preprint submitted to Trezarcoin *May 31, 2019*

1. User Data

TrezarMessage aims to be an application which ensures privacy at the highest level, therefore no user data is collected or stored. Registration only requires a pseudonym which will also act as the users MessageHandle or username.

2. Public and Private Keys

After choosing a pseudonym, the app will create a public and private key pair, which will be used for encrypting the messages as well as sending them. The user doesn't need to manage these keys, as the Pseudonym is pegged to this address-pair (your public and private key). To ensure the relation between the pseudonym and the public-key, we use a mechanism called Addressbook on the Trezarcoin blockchain.

3. Addressbook

The heart of TrezarMessage is the Addressbook on the blockchain. Each pseudonym gets registered on the blockchain along with the corresponding public-key. To ensure that the Handles are unique, we use the timestamp of the transaction, first come, first serve. With that Addressbook we eliminate a key security concern of an end-to-end encrypted System; the key exchange.

4. Signing Methods

There are two methods to register on the blockchain, the Signing Server and Self Signing. Both ways ensure that the pseudonym gets written on the blockchain.

5. Signing Server

The Trezarcoin team will provide Servers which will be usable for the Signing-Service. This method is the default, as it's the easiest way to register for TrezarMessage. The user simply chooses a pseudonym which gets sent to the SigningSever along with the corresponding public-key. The Server will then use that information to execute a transaction to sign it on the blockchain via TX-Comment (Comment left on the blockchain though a transaction). This is a centralized service but it bypasses the need to have knowledge of how the blockchain and especially the signing works. Also no Trezarcoins are needed for this method, the signing servers pay for the transaction to sign it.

6. Self Signing

The other option is Self Signing which provides a higher level of anonymity as the data doesn't go through a centralized Signing Server. Self Signing requires the user to load up Trezarcoin on the TrezarMessageApp and execute a transaction to sign him/herself on the Blockchain.

7. Message Layer

With TrezarMessage, Trezarcoin introduces the new Message Layer, which enables the ability to relay messages on the underlying Peer-to-Peer network of Trezarcoin. Messages won't be stored on the blockchain to avoid blockchain bloating, which would negatively affect the Trezarcoin blockchain. With this upgrade of the Trezarcoin-Core code, messages are stored on full nodes and can be requested from users.

8. Mobile Application

The mobile application is supported on Android and iOS. On first run, the app will ask for your pseudonym and connect to the signing server in order to register your pseudonym on the blockchain. Once that's done you're ready to start messaging.