

# Quarashi Network whitepaper

## Abstract

Quarashi Network is a complete suite of solutions platform focused on providing the user with full privacy and anonymity. The core elements of the Quarashi Network ecosystem are the Quarashi Privacy/Anonymity Chat, Multi Crypto Wallet & Exchange, IDO/IEO Platform. All of them are powered by the Quarashi Network Token (QUA).

**Quarashi Chat** is the first decentralized, 100% private and anonymous chat application which doesn't store any data whatsoever about the user. The messages one user sends to another one are end-to-end encrypted (with a very powerful algorithm - in order to decrypt the messages you would need around 2 years and access to a supercomputer), and are self deleted from the server automatically 1 hour after reading.

Unlike other messaging apps which only pretend to be private, Quarashi Chat will never store your private info such as email addresses or phone numbers, contacts, and never ask you to grant access to the microphone, or the GPS location of your device. The only information stored is your username, which is not merged or connected with your wallet.

**Quarashi Multi Crypto Wallet & Exchange** is another feature of the Quarashi Network Platform and it is a complete multicryptocurrency and cryptoasset wallet solution which enables the users using Quarashi to safely manage, send & receive, exchange and buy crypto using Visa/Mastercard secure. Your assets are stored directly into the blockchain. Quarashi doesn't hold/store and will never ask you for information about any of your assets or private keys. The Quarashi Platform is created to respect and protect human rights, so you're in full control of your data.

**Quarashi IDO/IEO** completes the bundle. IDO listings prevent the issuer of the tokens from controlling how the fundraising round will go, giving fair chances to every investor. IDOs can be created for anything from cryptocurrency to a work of art or any form of digital asset. With Quarashi IDO Platform, we balance fairness and need of maximizing the capital, so our users get the best IDO experience.

Unlike similar applications which only promise to be private and anonymous, the Quarashi team sees privacy as the core aspect of the project. Quarashi Network will always be a 100% secure and private messaging application, and Quarashi Multi Crypto Wallet will always be a 100% secure and private cryptocurrency wallet. Privacy shouldn't be considered an extra feature. It should be the absolute foundation and the irrevocable core upon the rest of the project is built. Full and total dedication must be upheld to focus all of the available technology on user protection.

So, for the short version of this purposely simplified white paper, we add this: ***Quarashi is The Next Generation All in One Platform in your crypto journey.*** Secure messaging dApp, secure crypto wallet and exchange, for your assets and cryptocurrencies and IDO/IEO platform, for you to join new crypto projects in their early stages. We want to offer a real advantage for every crypto-enthusiast.

*Privacy - like eating and breathing - is one of life's basic requirements.*

— Katherine Neville

# Table of Contents

Abstract	1
Table of Contents	3
Background	5
Problems of the so-Called “Privacy” Apps	6
Problem 1: Individuals	6
Problem 2: Businesses	7
Market Overview & Direct Competition	9
Privacy Problem of Cryptocurrency Wallets	9
Challenge, Vision & Objective	10
The Challenge	10
The Vision	10
The Objective	10
Quarashi Network	11
Quarashi Network Features	12
No Phone Number or Email Address Required	12
Self-Destructing Private Messages	12
Hidden History	12
No Ads & No Trackers	12
No Backups	12
Private File Sharing	12
Secure Screen	12
End-to-End Encryption (E2E)	12
Quarashi Wallet	13
Quarashi IDO/IEO Platform	15
Quarashi Network Token	15
Token Summary & Tokenomics	16
Token Distribution	16



# Background

We're living In the age of Big Brother. Groundbreaking technology, fast internet, the ability to easily store and retrieve data - all of this is amazing, but unfortunately we pay for it by sacrificing our right to privacy.

The majority of social media platforms and messaging apps aren't really designed to fulfill the needs of their users. Instead, their purpose is entrapping the users, stealing as much of their private data as possible, and selling all of it to the highest bidder.

Because of that, privacy cannot be simply introduced as an extra feature - the entire architecture of most of the social media and chat apps is hostile to privacy on a structural level. And the users are very well aware of that - the number of users for the biggest social media platform have declined in the last two years, mainly because of their total lack of respect for the users' privacy.

# Problems of the so-Called “Privacy” Apps

The facts are clear: most of the social media platforms and messaging apps advertising themselves to be more private than the competition are not really private at all. Both for individuals and business clients, these apps provide only an illusion of privacy instead of the real thing.

## Problem 1: Individuals

When numerous facts about companies collecting and selling their user data to private partners started to emerge, individuals felt betrayed - not protected by their service providers, but used and monetized as any other product.

Social media and messaging apps constantly improve their design and user experience, they improve their innovative technology, they create solutions which are constantly more appealing, addicting and easier to use. But instead of serving the users, the goal of all that is something else: transforming the users into goods which can be sold to the real customers - anyone who will pay for the access to people's private data.

Requesting access to numerous device features has become common. Because of that, social media platforms and messaging apps are able to monitor individuals 24 hours a day - even if they are not actively using the app. This translates to a total and complete loss of personal privacy. What's even worse, entities who purchase people's private information gain the power to influence people's decisions by analyzing the behavior and personality data.

The amount of data and metadata collected from an user allows the provider to fingerprint a person by unique identifiers. The data types collected are: network connections, contacts, Google service configuration, phone identity, user accounts, geolocation and many more.

For example, if the app is allowed to record video or audio, it WILL use that for recording everything it hears, digitize it using a built in voice recognition software and sending the conversation, in text format, to its servers. There, complex algorithms extract information and... voila! You get to receive highly customized and targeted ads, right after you talk about your new or future acquisitions. And this is just an example. Other apps will not use these features just for advertising.

Emails, electronic messages, voice or video calls and other forms of electronic communications are not like tangible mail written on a piece of paper and hidden in a sealed envelope. They can be collected, read, stored, analyzed by hundreds if not thousands of people other than the individuals who are actually sending and receiving the messages.

Access to Contact Databases is another service that is widely offered and abused. While often tied together with mass messaging services, these databases are also sold separately and often tailored to a specific audience. The most common databases on offer are commercially driven, including collections for gambling or online shopping.

The worst part is the fact that the users are never able to tell who exactly will have the access to their data - anyone from local and foreign governments, through hundreds of private companies, to malicious individuals can get a thorough insight into the private lives of ordinary people.

What people think is their private data is someone else's raw data.

## Problem 2: Businesses

Even for individuals, the complete and utter lack of privacy presented on all of the most popular social media platforms and messaging apps can pose a serious threat, but we often ignore that, because "we have nothing to hide". For businesses and professionals however, the danger is even greater.

Platforms which were not created from scratch with the purpose of securing people's privacy cannot be tweaked to protect it. Because of that, mainstream messaging apps are extremely prone to data leaks.

As much as 90% of data breaches occur due to human errors made possible by the lack of dedication to privacy. Actions such as downloading a file, or simply clicking a link, can easily open doors for successful cyber-attacks.

Social messaging platforms request practically full access to all the features on one's smartphone, such as microphone, camera, and the Global Positioning System (GPS) location. Each of these on its own would be problematic - combined, they result in a total loss of privacy and full disclosure of entire data the device ever had access to.

Not only messaging apps, but social media platforms as well are also vulnerable in this way. What employees of a company post in their free time on their personal social media accounts can be used to target their professional life, and vice versa. And if they are using the company's devices to access their accounts, the danger is even greater.

It's essential to acknowledge that none of the threats described above are just potential threats - they are actual dangers that businesses face every day, as social media and messaging apps have been turned into tools of mass-scale surveillance and industrial espionage.

For example, between April and May 2019 the Israeli spyware tool Pegasus was allegedly used by some governments to undermine the security of around 1,400 phones which belonged to lawyers, journalists and human rights activists. Most of the devices were hacked through video- and voice-call requests on WhatsApp. Even when ignored or declined, the call requests would give the Pegasus spyware access not only to the users' WhatsApp activity, but also to their location and other data stored on the devices. Because of the poorly designed or the lack of real security features of WhatsApp.

The risk of such breaches has led international organizations such as the United Nations to ban its employees from communicating on WhatsApp<sup>1</sup>. WhatsApp is seen as the leading mobile messaging application used in 112 countries and with 1.5 billion active users - but other messaging apps have the same problems, even if they are not as targeted as it is WhatsApp.

---

<sup>1</sup> *Manipulation Ecosystem on social messaging platforms published by NATO Strategic communication Centre of excellence, April 2020*



# Market Overview & Direct Competition

Know-your-customer (KYC) and anti-money-laundering (AML) trends which originated in the banking industry are starting to be widespread and common in other sectors. KYC/AML is becoming a standard even in the areas where such regulations are most often unnecessary, such as the crypto ecosystem, social media and messaging apps.

Privacy used to be the standard, then it became optional, and soon it might be gone altogether. At Quarashi, we believe that the full and unconditional dedication to privacy is the only answer to numerous threats to the sensitive data of individuals and businesses.

## Privacy Problem of Cryptocurrency Wallets

One of the most important elements of the Quarashi Network ecosystem is the decision to integrate a cryptocurrency wallet and the ability to securely and privately send and receive cryptocurrency transactions.

While the privacy problem of messaging apps and social media platforms is commonly known, many people don't realize that cryptocurrency wallets face a similar degree of privacy threats.

In the quest to retain anonymity, privacy and security, it is important to understand that typical crypto wallets are designed only to provide the basic functionality of sending, receiving and storing digital assets. Privacy is at the best considered an extra feature, in the worst case scenario, it's something that just doesn't get addressed at all.

Almost all cryptocurrencies on the market don't have in-built privacy, so unless the user's wallet is privacy-focused, all transactions can be effortlessly tracked by hostile third parties. Naturally, there is an increasing demand for privacy-oriented wallets to defend against transactions being followed by bad actors.

Our direct competition extends to platforms enabling private deposits of Ethereum by using smart contracts (such as Tornado Cash), anonymous wallets (such as Incognito), or even semi-private, but not anonymous wallets (such as Metamask). The success of our competitors reassures that the demand for privacy-based transactions is as high as ever - though we also see clear competitive advantages that Quarashi brings to the market.

Contrary to traditional markets, the cryptocurrency ecosystem is not a zero-sum game and lacks the "winner takes all" mentality. Different solutions, blockchains, exchanges and cryptocurrencies coexist together, which results in an ever-expanding, organically growing, healthy and user-oriented market. In other words, crypto is a community, and the demand for integrating private crypto transactions into a private messaging app is massive.

# Challenge, Vision & Objective

## The Challenge

Is it possible to design a completely private messaging application that would provide the full functionality enabled by today's technology, but without storing any data and without creating any fingerprint identifiers of the user?

An application like that would have to be totally dedicated to protecting users' privacy. All the private data would have to be owned exclusively by the user, but the entire network would have to be built as a community-owned, decentralized, transparent, public infrastructure. This would guarantee that the application remains fully resistant to hostile takeovers and outside manipulation, while also providing additional incentives to out-innovating and out-competing entrenched incumbents.

We strongly believe that Quarashi has the potential to fully answer this challenge.

## The Vision

The Quarashi vision is focused on total commitment, consistency and respect for its users' privacy, data and identity. Our mission is helping individuals and businesses in regaining their rights to privacy and anonymity.

Quarashi aims to be the world's most private, most secure and most anonymous chat application providing its users with untraceable identity while sending and receiving both traditional messages as well as cryptocurrency transactions.

Privacy shouldn't be "opt-in", rather it's something you could occasionally "opt-out" on your free will. Utilizing blockchain technology in Quarashi will allow us to greatly enhance the privacy standards prevalent in the current messaging apps.

*If crypto succeeds, it's not because it empowers better people. It's because it empowers better institutions.*

- Vitalik Buterin, Creator of Ethereum

## The Objective

To sum up, the objective of Quarashi Network is creating an ecosystem enabling sending and receiving communications and transactions in a truly private way.

Most of the messaging apps and cryptocurrency wallets on the market consider privacy an extra feature. We believe that privacy is the feature to begin with.

# Quarashi Chat

Quarashi Chat is the first messaging app that is fully privacy oriented. Encrypted chat apps aren't something new, but they only give you an illusion of security.

Many messaging apps only provide you with end-to-end encryption (E2E). But even if an app is 100% encrypted, it doesn't mean that it is truly anonymous and private.

Quarashi Chat is a decentralized, community-driven, 100% secure and private messaging app in the Quarashi Platform which combines traditional end-to-end encryption (E2E) with a wide array of extra features massively enhancing users' privacy and anonymity.

Most of the chat apps on the market request you to disclose personal information such as your phone number or email address. Because of that, even though the messages might be encrypted, you are not anonymous and your real identity can be easily revealed.

Quarashi is different. No phone number or email address is required. You can send and receive encrypted messages while being absolutely certain that your personal information remains private, anonymous and fully untraceable. The only thing you need to know is **the username**.

# Quarashi Network Features

## No Phone Number or Email Address Required

Most of the so-called “private” messaging apps forfeit the user’s actual privacy before the user even starts to use them, as providing personal information during registration means that the user’s real identity can be easily traced. Quarashi is different: the user is never, under no circumstances asked to disclose any personal information, nor we store anything else from the user’s device.

## Self-Destructing Private Messages

If you want to have absolute certainty that nobody but the recipient will read your message, you can choose the self-destruction option. The message will be automatically deleted from all devices after a set period of time, leaving absolutely no trace.

## Hidden History

With typical privacy chat apps, someone who accesses your smartphone can read the entire chat history. With Quarashi Network, the messaging history is hidden, and even if your device is compromised the messages can’t be read by a third party.

## No Ads & No Trackers

Ads can compromise your privacy and anonymity by collecting data about you. That’s why Quarashi Network contains absolutely no ads and no trackers.

## No Backups

No sensitive data and personal information will ever be stored where it shouldn’t. Your data is not copied anywhere without your knowledge. If you delete something, it’s gone. So, use this powerful feature wisely.

## Private File Sharing

Privacy must not be limited to traditional text messages. In Quarashi, all types of messages are equally private and secure: transferring photos, videos and other files can be done 100% privately and anonymously.

## Secure Screen

In messaging apps which don’t provide full screen protection, messages can be easily captured and the entire content of the user’s screen can be revealed to a hostile third party. Quarashi offers a completely secure screen which cannot be captured, so the only thing you need to protect is your password.

## End-to-End Encryption (E2E)

For most messaging apps, end-to-end encryption is the only privacy-oriented feature. For Quarashi, it’s just one of many features working together to assure full privacy. Text messages

and other files use the military-grade protocol for end-to-end data encryption, as well as pre-keys optimized for mobile and multi-device messaging.

Privacy does not necessarily mean that you are hiding something, it is about protecting your information and just keeping it private. It's a fundamental right, and you don't need to prove the necessity of fundamental rights to anyone. That's why governments often seek to tighten data privacy laws to protect the personal data of their citizens. Moreover, staying safe online can help protect your identity and that of your loved ones, and keep you safe from any kind of risks.

Therefore, privacy should be the default setting for anything in today's digital space. That's why most online platforms would advise you to use strong passwords, such as those generated by and stored in a keychain, or two-factor authentication. But as it turns out, the idea of privacy from most organizations in 2021 it's a luxury, as there is a very thin line between staying totally private and sharing information about you with organizations or individuals online.

Here are the top 15 reasons why you should use Quarashi Chat App:

**The rising token value:** The QUA tokens that you will hold in your Quarashi Wallet/APP will gain value over time.

**Intuitive App:** The App is highly intuitive and easy to use.

**Wallet:** The dApp also doubles as a wallet; hence you don't need another wallet that may expose your personal data to fraudsters.

**Sell/withdraw tokens anytime:** With the dApp, you have the liberty to sell or withdraw your tokens anytime.

**No phone number or SIM card needed:** You don't need a phone number or a SIM card to use the dApp.

**Offline capability:** The dApp can also be used as an offline wallet without SIM. You can also use it on your WiFi only tablet.

**Automatic message deletion:** The dApp is designed to enable the disappearing of messages (automatic deletion of messages) from the server one hour after reading it. This happens even if you forgot to burn the message.

**No special permission from the Quarashi team:** We will never ask you for special permissions, such as personal information, in order to allow you to use it. You don't need to share your location, contact access, or recording audio, or any other special access queries sought by most apps.

**Safe & Secure:** The dApp is backed by a special end-to-end encryption. It will take around 2 years with a supercomputer to decrypt it, and the messages are deleted permanently in just 1 hour after reading.

**Anonymous membership:** You've got the option to use the app anonymously, a feature that's not available with other chat apps.

**No backups:** Our app doesn't perform any backups, so you can be sure that no one will ever access your chat information by breaking into a backup server tucked somewhere across the globe.

**No monthly fee:** We do not charge the users of our app any monthly/yearly fee, in order to use it. All you need to do is store just 100 Quarashi tokens in your wallet (lifetime), and you're good to go.

**Cheap & affordable:** The Quarashi app is the cheapest chat tool you will ever find with the level of cutting-edge technology it runs on. The free apps will not hesitate to sell your information, because if an app or service is free, then you're the merchandise they are really selling.

**Ad-free App:** Quarashi App is an ad-free app, so don't expect any ad or tracker on your app.

**No selling of user information:** We don't collect any data, so we don't have anything to sell.

**Easily recovery of your wallet:** The Quarashi wallet is connected directly to the Ethereum Blockchain. It means that even if you lose your password, you can restore it anytime on MEW, Metamask, or any other Quarashi accounts.

**Data control:** At Quarashi, you control all your data because you own it. We're just a platform that facilitates your own usage of data.

**Quarashi App is what the world needs, and you know it.**

The ease of information sharing in today's digital space has exposed us to random identity thefts, manipulation through ads, discrimination based on your personal information, cyberbullying, filter bubble, and many other ills that may arise from invasion of our privacy.

Data privacy is critical for anyone, and you need it like never before in this information age. Keep your privacy under lock with Quarashi App.

# Quarashi IDO/IEO Platform

An **initial DEX offering**, or IDO, is a new and exciting type of decentralized and permissionless crowdfunding platform, which is opening up a new way of fundraising in the crypto ecosystem.

Participating in a IDO is not always simple or transparent. Joining the project right at the beginning is reserved for those advanced users, focused and passionate about decentralized finance (DeFi) and non-fungible tokens (NFTs). With Quarashi IDO/IEO Platform we will simplify that and will also offer a solution for early access investors, in a transparent and fair way for all our users.

IDOs provide instant liquidity, as the tokens sold start trading on the host DEX immediately. This is a particular benefit over ICOs and IEOs, which are effectively at the mercy of centralized exchanges free to list (or not) tokens at their discretion. Also, IDOs don't attract the very severe fees levied on ICOs and IEOs by exchanges.

Another big factor is investor fairness. In both ICOs and IEOs, the tokens being launched are pre-mined and often pre-sold, which essentially locks small investors out of the early stages of trading, when successful launches often see the greatest price gains. With Quarashi IDO Platform, we balance fairness and the need of maximizing the capital, so our users get the best IDO experience.

The Quarashi IDO platform gives fair chances by using a lottery system. For every 3000 QUA you get one ticket for that IDO. You need exactly 3000 QUA for every ticket. More tickets, more chances to buy the IDO project you want.

## Quarashi Network Token

The entire Quarashi Network ecosystem is powered by a native digital asset: Quarashi Network Token (QUA).

Quarashi Network Token is an Ethereum-based (ERC-20), deflationary, fairly issued and fully transparent digital currency.

QUA is a multi-functional token utilized both in the Quarashi messaging app and in the Quarashi cryptocurrency wallet & exchange, IDO/IEO Platform . Thanks to the application of the QUA token, Quarashi Network is able to be the first 100% private and anonymous solution on the market combining the functionality of a traditional messaging app and a crypto wallet, allowing the users to send all kinds of data with total privacy - including cryptocurrency transactions.

## Token Summary & Tokenomics

**Blockchain:** Ethereum

**Symbol:** QUA

**App Code:** Kotlin, Java

**Max Supply:** 1,000,000,000 QUA

## Token Distribution

**Platform Development:** 15%

**Marketing / Reserves:** 27%

**Listing:** 10%

**Team:** 13%

**Public Sale:** 35%