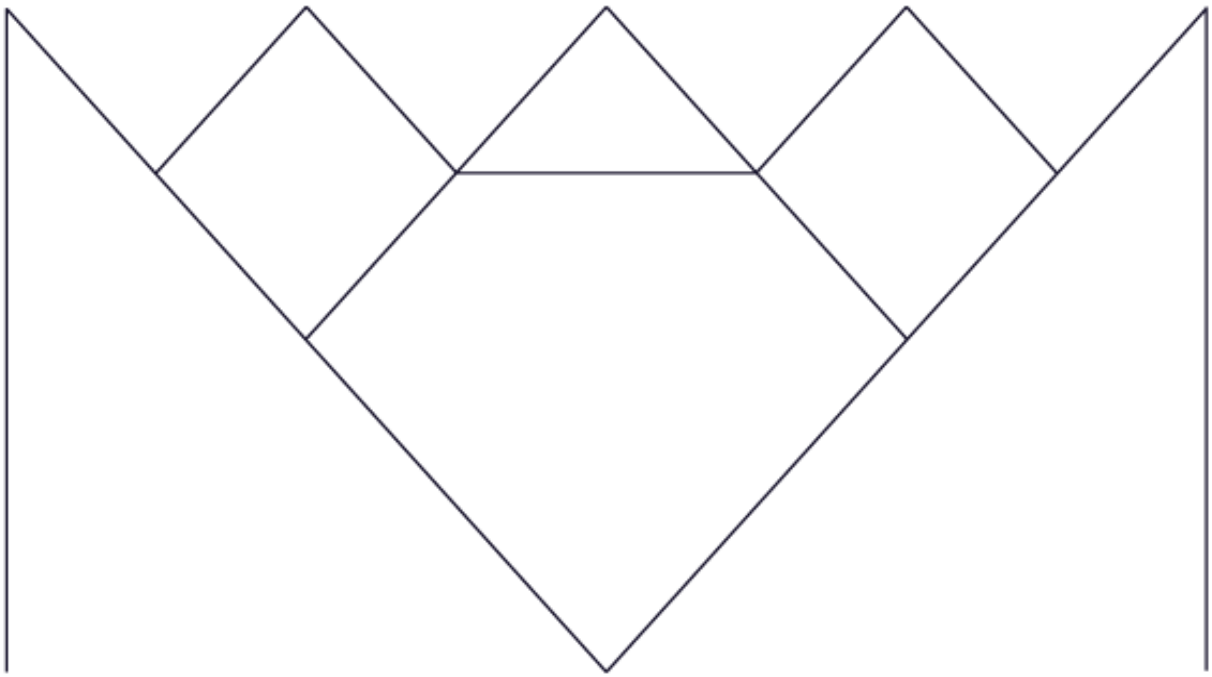


WorldWide Anonymous Messaging

TABLE OF CONTENTS

SUMMARY

Privacy over the internet is a growing problem, more so over the last few years. Search engines like Google, Internet Service Providers (ISP), the websites we visit and the mobile applications we download, are all tracking every move you make online. It is no secret that there is big money being made by violating our privacy.

Big internet companies are paying huge sums of money to learn more about their clients activities. Despite the precautions users employ to avoid being tracked, Internet Service Providers (ISP) can still monitor them. It may seem harmless to some people, but most users are resigned to it, and accept it as a necessary evil in this modern world.

To most of these companies, users as nothing more than a statistic to be exploited. Even though they are not standing behind you, and watching every click you make, your browsing history is being stored somewhere on their servers. This could lead to serious problems and consequences should there be a data breach.

Most internet users have no idea how their data is used or processed. What is encrypted, saved or deleted. Their main focus is communication, but this is where the most sensitive personal information is mined. Email clients, chat applications and messaging software identify you by using a remote server. In most cases, every communication between users passes through a central server.

It may be fine with the average user, but what about you? Do you appreciate your internet usage being tracked by your Internet service provider (ISP) and service providers? Are you interested in anonymous communication, without any central authority storing your data, contacts and messages?

We present to you WWAM. An anonymous, decentralized and safe protocol that enables instant and delayed communication between two or more users. This document seeks to highlight the privacy issues users face daily on the internet. It will also explore how WWAM will help users resolve these issues for a safer online environment.

This section is a general and simplified presentation of WWAM, for a more in-depth description of how WWAM works please see the technical section.

1 – THE MESSAGING PROBLEMATIC

1.1 – Anonymous messaging

This section is a general and simplified presentation of WWAM, for a more in-depth description of how WWAM works please see the technical section.

WWAM aims to be the leading global, anonymous, decentralized messaging protocol with zero knowledge of its users. We want users to be able to communicate with each other, without registering their private information. WWAM will negate the need for a central server, and will not store the users contacts, preferences, messages and history.

Our goals are extensive, but achievable. Man will benefit individuals and corporations that deal with very sensitive information. It will also be useful for the average user, with concerns about their data being exposed or breached when using traditional messaging protocols.

Imagine having your personal information broken down into different parts, and stored in a separate safes. It will be visible to the public, but each safe will have its own key, and would require considerable effort by anyone attempting to access it. This is better than having all your information stored in one big safe, with just one key to access it.

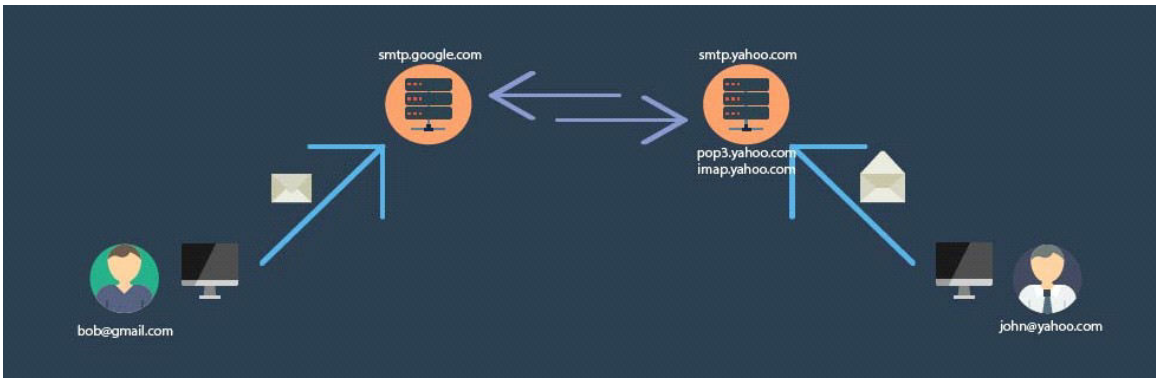
We are already witnessing multiple use cases of this type of protocol. It will be applied here and used for instant messaging, with the scope to replace emails or act as a means of spreading immutable messages worldwide. Messages will be written in the blockchain, encrypted, and cannot be changed. A good example is the Bitcoin blockchain, which is free of censorship.

1.2 – Current protocols

In this section, we will discuss the more popular and widely used messaging protocols on the internet. We will also focus on non-proprietary protocols since they are popular all over the world, and have better documentation.

1.2.1 – POP3/IMAP/SMTP (E-mails)

Electronic mail replaced postal mail with a system, accessible to every human being with access to an internet connection. It also reduced the time it takes to deliver written messages by posting them.



This diagram illustrates what happens any time Bob sends an email to John. Bob signs in by authenticating on Gmail's Simple Mail Transfer Protocol (SMTP) server as bob@gmail.com, which then transmits Bob's message. To process this, Gmail's Simple Mail Transfer Protocol (SMTP) server communicates with John's Simple Mail Transfer Protocol (SMTP) server. In this case, John's Simple Mail Transfer Protocol (SMTP) server is smtp.yahoo.com.

The email is passed on to Yahoo's Simple Mail Transfer Protocol (SMTP) server, which then dispatches the email to the corresponding Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP) server. To read his messages, John connects to Yahoo's Post Office Protocol (POP3) or their Internet Message Access Protocol (IMAP) server. He signs in and authenticates as john@yahoo.com, then reads the email sent by Bob.

The Post Office Protocol (POP3) keeps emails until the user reads them, and the Internet Message Access Protocol (IMAP) keeps remote copies. Both store emails and personal data on a remote server.

Potential vulnerabilities of the protocol

- Communication between users and servers are potentially vulnerable to man-in-the-middle (MITM) attacks. Industry giants like Gmail and Yahoo use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) these days. However, it is not mandatory.

- Emails are stored on remote servers. Simple Mail Transfer Protocol (SMTP) is not mandated to encrypt content. This means that the server can read email content in plain text, and so can anyone with access to the server.

- Communications between servers are also vulnerable to man-in-the-middle (MITM) attacks. The big companies like Google and Yahoo use Secure Sockets Layer (SSL) or Transport Layer Security (TLS). However, it is at their discretion to use them or not.

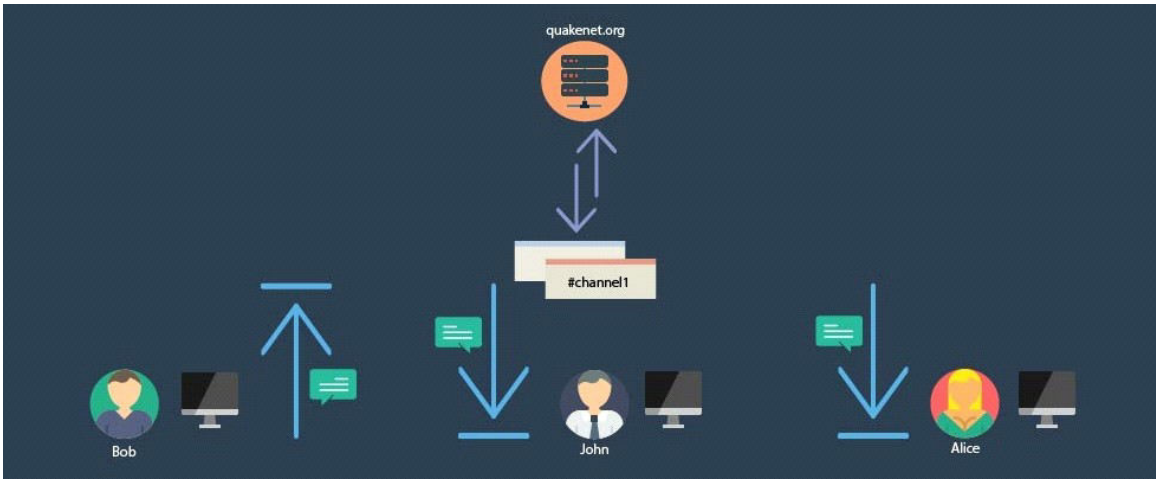
- Lastly, before assigning users an email address, they are required by most providers to register, and are asked for personal details. The provider's track Internet Protocol (IP) addresses each time an account is created and whenever users connect to use these platforms. Most internet companies provide web clients that are vulnerable to phishing and man-in-the-middle attack (MITM).

Resetting passwords is easy on these platforms. Most of them require very simple questions and answers, and someone with the right motivation, knowledge and determination could guess the right password. Using One Time Passwords (OTP) or Two Factor Authentication (2FA) are positive developments. However, they are not enforced by the providers and the user can decide to use or do without them.

1.2.2 – IRC

Internet Relay Chat (IRC), gained popularity in the early 2000s. It is a unified means of communication, especially for group channels. Users can sign in to a particular server and choose their preferred channel, to communicate with other users. They are very convenient and widely used, but they were not created with privacy in mind.

Users can communicate in group chats with just about anybody on the same channel, or send private messages to a specific user. Some applications use Internet Relay Chat (IRC) platforms as a communication frame work, mostly for malware and video games.



In this example, Bob, John and Alice have all joined Quakenet's Internet Relay Chat (IRC)server. They are all connected to #channel1. Bob sends a message to #channel1 and the message is relayed to the Quakenet server. In turn, the server checks to determine which particular channel is associated with the message, then contacts every user connected to #channel1. In this instance, John and Alice are the other users so the server relays the message to them.

Potential vulnerabilities of the protocol

- As messages are not encrypted, and Transport Layer Security (TLS) or Secure Sockets Layer (SSL) not mandatory, communication between users and servers are vulnerable to man-in-the-middle attack (MITM).

- The Internet Relay Chat (IRC) server can read and log the users messages in plain text.

- Users can use Internet Relay Chat (IRC) without registration. However, nicknames can be impersonated if they are not registered.

- Users Internet Protocol (IP) addresses, are logged by the Internet Relay Chat (IRC) server, and sometimes other users can see it too.

1.2.3 – XMPP (Jabber)

Extensible Messaging and Presence Protocol (XMPP), is a communication protocol for message oriented middle-ware, based on XML (Extensible Markup Language). It is arguably, one of the best decentralized and secure communication protocols and Internet giants like Facebook and Google use it. However, there are concerns about the privacy of communications between simple users.

Extensible Messaging and Presence Protocol (XMPP) is similar to protocols used by email providers, with the exception of Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). End-To-End encryption is mandatory and it eliminates the possibility of man-in-the-middle (MITM) attacks. It ensures that the server cannot read users' messages in plain text.

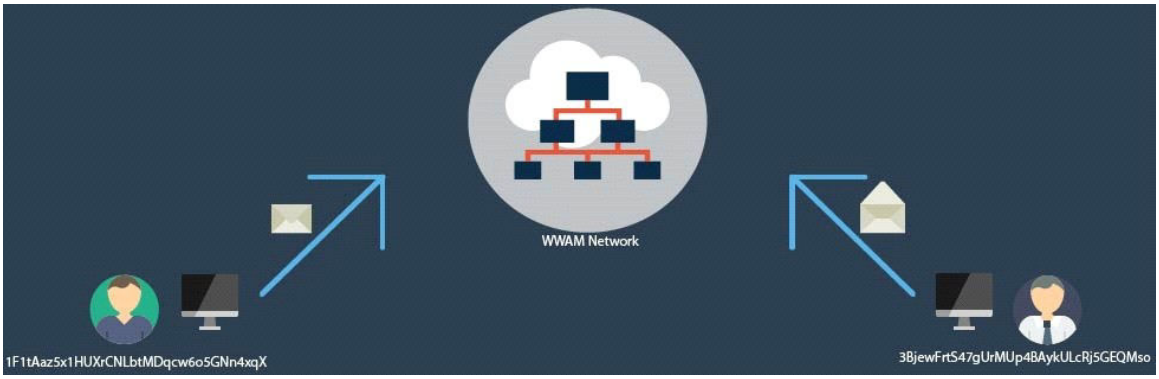
However, users still need to register on the jabber server. It means that the server can log their Internet Protocol address (IP) and store their contact lists, thus missing the whole point of decentralization.

1.3 – Aim of WWAM

WWAM seeks to make it impossible, for communication between users, to be compromised in any instance, when communicating over the internet. All messages between users on the WWAM network will be encrypted. Encryption will be mandatory, and un-encrypted messages rejected automatically by the network.

The nodes will have zero knowledge about the users on the platform, and they will not be able to read messages and content. Users will not be required to register to use WWAM, thereby rendering login and password combinations useless. There will be no central server to store private information, and all messages will stay in the blockchain. Contact lists and message history are non-existent unless the user opts to maintain one.

WWAM will use a large network of many nodes. Whenever a user sends a message, the network will process the message on different nodes. If a node on the network sees the user's Internet Protocol (IP) address, the rest of the network would be oblivious to that information. With a network of thousands of nodes, it is impossible for an attacker to control enough nodes to access the Internet Protocol (IP) address of a specific user. Should the improbable happen, and the attacker is able to see the users IP address, they will not be able to access the users messages.



In the diagram, Bob, identified on the WWAM network as 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX, sends a message to John, identified by WWAM as 3BjewFrtS47gUrMUp4BAykULcRj5GEQMso. Bob's message is encrypted, then broadcast by a random node on the network. The message is confirmed by multiple nodes and added to the blockchain. Whenever John queries the blockchain, he will be able to decrypt the message safely.

2 – TECHNICAL

2.1 – Rewarding scheme

WWAM will be broadcasting messages between users via the blockchain. There will be no generated coins or tokens. The supply will be fixed, and exchanged between users as transaction fees. Messages will be broadcast as transactions by the network, and nodes will be rewarded with fees for processing messages.

The process is peer-to-peer. The sender adds the appropriate fees, and the node that processes the transaction is rewarded with the fees. We believe the reward system is fair. If a user puts pressure on the network with large files or messages, they will pay extra fees, or process enough transactions on their own nodes to generate enough reward to pay.

The network will reward users that are part of the network, but are not active to limit spam and the use of bots. We will run thousands of nodes with very low fees at the coin's launch. It will keep transaction costs low and at an acceptable level, suitable for everyone. Nobody wants to pay $1 to send a simple message to another user. The node fee will be adjusted according to the index price of the coin, at a fixed rate of $1 for every 5000 messages.

2.2 – Anonymity Concerns

Steps will be taken to assure users of their anonymity on the WWAM network. The absence of registration, contact lists and save message history will ensure complete anonymity for the user. To communicate with other users, a user needs to generate a public and private key pair on the blockchain, then send their public key to the intended recipient.

Is it possible for spam or unwanted messages to be sent to a users publicized address. The short answer is no. Why? It is not possible because there is an authorization process involved.

The first transaction between two or more users will require authorization from the receiving address. If the recipient address declines authorization, any further attempts by the sending address to contact the receiving address will be rejected by the network. To keep the network less busy for the processing nodes, each authorization will be time stamped and valid for only 24 hours, after which it will expire. Please note that this could change in the future.

Everyone can view transactions and addresses on the blockchain. How will the WWAM network achieve anonymity?

Yes, WWAM will be completely anonymous. Every message on the blockchain will be protected with double

encryption, using Pretty Good Privacy (PGP) and Elliptic Curve Cryptography (ECC). The network will also use temporary "dummy" addresses to obfuscate transactions between users.

During the first authorization process, a pair of new addresses will be generated, one for each user in the communication. An authorization message will be sent from the senders address to the recipients address, and all subsequent messages between the authorized addresses will be between the newly generated "dummy" addresses.

Owing to the fact that the blockchain is publicly view-able, it will show that address Y authorized address X to send messages to it. However, only the users communicating will know the dummy addresses. The public will see the exchanges between the dummy addresses but they wouldn't know which authorized addresses are associated with them.

2.3 – WWAM Protocol

The WWAM network's goal is to be a protocol rather than a single application. We want developers to develop and implement their own chat clients. They will be free to create their platform from web, mobile, desktop or integrated chat clients.

We will provide a simple desktop client, and Representational State Transfer (REST) API to use with the blockchain protocol. A few servers will be up and running at launch, to give interested developers a sandbox to experiment with before developing their own. A full breakdown of the technical protocol and the API, will be released as we approach the launch date.

3 – DEVELOPMENT

3.1 – Our client

A Windows instant messaging desktop client using the WWAM protocol, will be available at launch. It will be fully functional, but will come with its basic functions. Users will have the option of using Representational State Transfer (REST) or run the blockchain locally. We will also provide users with Windows and Linux software for running nodes at launch. Everything will be open source and made be publicly available using GNU general public license.

3.2 – Our API

To develop a fast and reliable application suitable for the WWAM protocol, you need to use an API that runs on a remote server to query the blockchain. Downloading the blockchain is up to the user. We will provide the source code of our implementation of the API, using the GNU general public license. We will also make a few servers available to the public, as a Representational State Transfer (REST) API.

4 – ROAD MAP

WWAM is a long-term project. We are still at the very early stages of development, thus making it hard to foresee an accurate road map. This section is subject to change and will be updated on a regular basis to provide up-to-date information.

We can already provide a few dates and approximations for the project:

-August 9, 2017 - 20h UTC -> Crowdsale Stage 1 begins

-August 16, 2017 - 20h UTC -> Crowdsale Stage 2 begins

-August 23, 2017 - 20h UTC -> Crowdsale Final Stage begins

-September 6, 2017 - 20h UTC -> Crowdsale Ends

-Q1 2018 -> Protocol and API breakdown

-Q2 2018 – Q3 2018 -> Protocol and node software release

-Q3 2018 -> REST API release

-Q3 2018 -> Windows/Linux Client release

5 – TOKEN CROWDSALE (ICO)

5.1 – WHY

WWAM is a token based system. All tokens will be created during the crowdsale and distributed among investors. A maximum supply of 500,000 ETH worth of tokens will be made available. Development, maintenance and marketing of this project comes at a cost. You are invited to be a part of this project, and as a reward you will receive a share of the limited tokens. We believe that this project has huge potential and scope for growth and profit.

We have set a minimal goal of 500 ETH for the crowdsale. A project of that scope needs funds, and we believe that it would be unreasonable to dive into such a project without enough funds. Therefore, if the minimal goal is not reached, the Ethereum contract implements a method to refund every investor and cancel the project. This is also the guarantee for you to invest in a project that will live and have enough token supply to reach a comfortable market cap.

5.2 – HOW DOES IT WORK

The ICO will be offered in three stages and you can find the relevant dates for all three stages in the Road-map section. Early investors will be rewarded with more tokens, as it takes foresight, courage and determination to invest early in this kind of project. We respect their faith in our project and development team, and will rightly reward them for making a bold decision.

- First stage investors (Early investors) will receive a 15% bonus on their investment.

- Second stage investors will receive a 10% bonus on their investment.

- Third stage investors (Final stage) will not be rewarded with any bonus.

The ICO tokens will be issued via smart contract on the Ethereum blockchain, you can read more details on how to participate on our website: www.wwam.io/ico

5.3 – FUNDS BREAKDOWN

Every token generated during the crowdsale will be shared among investors. Up to 1% of the maximum

tokens supply will be allocated to the bounty campaign, and an amount equal to 1% of the total token supply generated during the crowdsale will be allocated for the team as a reward for our hard work and dedication to the project.

All ICO funds will be view-able to the public on the Ethereum blockchain and we will perform a methodical examination and review of all our expenditure and accounts every month. In the aftermath of the ICO, if successful, funds will be quickly allocated to renting thousands of servers to run nodes.

We will hire powerful servers to provide the REST API as quickly as possible. Some funds will be used for advertising and marketing between the end of the ICO and the release of the coin. Surplus funds will be used to keep the nodes and API servers up for as long as possible, and some for maintenance.