STEALTH PROJECT

Whitepaper v 1.0

Abstract

Today it is impossible to imagine life without Internet. While browsing the Web, everyone wants to remain anonymous in order to prevent the leakage of personal data, locations, bank account information, and so on. Denying unauthorized access to the information mentioned above for third parties without prior consent of the user is what essentially makes up anonymity.

The Internet is very instrumental in espionage and shadowing anyone in that space. Government agencies and secret services as well as business and banking entities are using the Web to collect information they need; advertisers and merchants build customer profiles on this info; single individuals are spying on each other. The Internet provides the

Not to surprise anyone, but you are always being snooped on when you are browsing the Web. You are being watched when you are entering the keywords in the search field. For example, as you hit the link in the Google search results, your search query as well as your personal data is sent to the site over the link. This site can keep the logs of who visited them and what they were looking for. Apart from that, by visiting promotional sites through ad banners, you disclose your privy information and your interests to them.

Using these pieces of information, your personal profile can be build. After that, intrusive advertising will follow you everywhere. But this is likely the least of evils.

Whether you like it or not, your personal information is being collected from any device you are using, not just your desktop computer. When you use a smartphone, the data collected by the device is available to the device manufacturer. At the dawn of the iOS and Android eras, Apple and Google got involved in numerous scandals linked to their positioning tools. The train of your private info follows you everywhere in the Internet.

To go online you use a network card which has a permanent MAC address programmed into it. You receive an IP address when you start surfing the Web. These things are following you, and they allow to identify you without fail. They are basically your network identity. The OS used may serve as an indirect indicator of your financial well-being (e.g. a top notch iPhone model, Mac OS, etc).

Any site can take advantage of this information. And this is what airfare search aggregators are already doing by offering Mac OS users flights at higher prices than users of the good old Windows XP.

You are voluntarily agreeing to these terms by filling a contract with your Internet provider or via registering with your name at any site. However, such binding doesn't always happen. All relevant info that you leave behind in the Internet is linked to your personal data. Let's take the License Agreement or Privacy policy of any software or online service as an example. Did anyone ever read them in full given that they are often not even translated? Obviously, no one did in practice.

For sure, everything is nice and neat there, legally speaking. You promise not to break the rules, while the producer promises the same and above all to keep everything undisclosed. And this is all for our well-being and convenience. Then we hit the Accept button and safely forget about that stuff. But these promises to keep everything secret are not worth a dime. Our personal info is saved, collected, processed, and then pulled out and brought to light at the right moment (maybe not so right for us, sorry).

Let's assume, on the other hand, that an individual doesn't want to reveal his true identity due to his professional activities. So he creates a disposable email using fake identity. But all his efforts fail instantly when his friend adds this email to his contacts using his real name, as he thinks it would be more convenient and then synchronizes his contacts with Google.

In 2013, Edward Snowden, a former Central Intelligence Agency employee, made himself famous by revealing to the public information about the PRISM surveillance program, which allows the US National Security Agency to get access to private electronic correspondence, voice and video messaging of the US citizens in the Internet.

The same Snowden handed over to mass media a copy of the court order dated April 25, 2013, according to which the court forced Verizon, one of the leading wireless carriers in the US, to report daily all calls of its subscribers to the National Security Agency. People who got interested in Snowden's story were later surprised to learn that surveillance programs like PRISM were operating all over the world, while some of these programs are massively transnational.

For example, the American ECHELON program is one of such systems, which aims at global electronic espionage. The key operating principle of the ECHELON program can be loosely described as follows: the communication channels are being monitored round the clock by powerful computers and if an incoming message includes a keyword or phrase, or matches a voice pattern present in the ECHELON "vocabulary", the message is then recorded. The ECHELON vocabulary comprises a huge number of keywords in many languages and is constantly updated.

It is tempting to say that staying anonymous, invisible and unidentified is impossible in the Internet nowadays. We are all under the Big Brother's informational watch, even though many people would love to keep network anonymity by default for various reasons. This is why blockchain-based cryptocurrencies have become so popular today. But **how anonymous** are they in practice?

For a long time Bitcoin had been considered an anonymous digital currency. But this is not quite true. Transactions made to Bitcoin addresses can be easily followed on the blockchain. Once a connection between such an address and a real person is established, all anonymity is instantly gone.

That's why today Bitcoin is considered a **pseudo-anonymous** currency rather than a truly anonymous one.

Analyzing the blockchain along with using KYC (Know Your Client) and AML (Anti Money Laundering) policies helped the police to track down users of the Dark Web. This approach allowed to catch Ross Ulbricht, a founder of the Silk Road, and track down the servers of Hansa, another darknet market platform.

More specifically, the police developed a specialized software tool which they used to analyze the blockchain in order to prove the link between a delivery address and a certain Bitcoin transaction address. This has already led to a tremendous amount of convictions during the last several years. Indeed, mostly criminals have been convicted, though **some innocent people**, which were accidentally involved in the transactions, got hurt too during the investigative process.

As soon as the drug dealers and anonymous hackers from the darknet learned that Bitcoin was not providing any impenetrable anonymity, many of them switched to Monero since this cryptocurrency had been specifically designed with anonymity in mind as its top priority in order to disrupt tracking down its users. Even so, one research group has recently discovered that while Monero is undoubtedly better than Bitcoin in this regard, it is not a panacea either.

Payments in the Monero (XMR) network are mixed with other such payments, thereby preventing tracking down a payment to a single user or linking it to a previous payment from the same source by analyzing the blockchain.

Nevertheless, a team of researchers from the world's leading universities including Princeton University, Carnegie Mellon University, Boston University, Massachusetts Institute of Technology, and University of Illinois at Urbana-Champaign have released a study where they discuss the shortcomings of the mixing algorithm through which it is **possible to trace** single transactions.

And the problem applies to all who ever used Monero in the past, not just the ones going to pay with it today as all payment details are **permanently carved into the blockchain** and easily available for analysis.

One of the study authors, Andrew Miller from the University of Illinois at Urbana-Champaign, says:

«People are eager to oversimply, and they expect Monero transactions to be guaranteed to remain private. In practice, though, there are still pieces of information ***which are not encrypted*** *by the network»*.

In this manner, Monero transactions remain **potentially traceable**, even though it is still a matter of probability rather than hard evidence. As the researchers warn, small chunks of information may build up and together with other sources create a strong evidence base over time. The early users of Monero should be most concerned now as they used the system when it was at its maximum vulnerability level, and all their actions **are imprinted on the blockchain** for many years to come.

And here we encounter a fundamental problem of privacy that cryptocurrencies face:

Any vulnerability discovered in the future can be applied to the past data, allowing an interested party to retrieve old skeletons from the cupboard. All changes are continuously written to the blockchain, and whenever a critical vulnerability is found, your past may catch up with you. Although we don't know what the future holds, the best way to predict it is to create it.

Here we present **STEALTH PROJECT** - a unique project with the new level of network anonymity.

It is a decentralized network ecosystem of a new generation based on the blockchain paradigm and employing state-of-the-art technologies in **cryptography and information security**. The project is expected to pass through several development stages:

1. Multi-cryptocurrency STEALTH WALLET is developed with strong emphasis on anonymity. It will offer a built-in mixer and users will be able to earn passive income while using it.
2. Self-sufficient anonymous and autonomous network infrastructure is built, similar to Tor.
3. Web content is created, available only from within the STEALTH PROJECT network.

[STAGE 1]

Multi-cryptocurrency anonymous STEALTH WALLET

How can a user become anonymous in the Bitcoin network? The market for cryptocurrencies is expanding rapidly with new and more anonymous coins springing up everywhere, but what should all those who discard such altcoins and want to be involved only with Bitcoin, Ethereum, and other pseudo-anonymous coins do? There is a solution to this question, so it is up to you to decide how private your transactions will be.

STEALTH WALLET is a software product developed for managing and storing cryptocurrencies. It aims to simplify the use of cryptocurrencies in everyday life as well as offer convenient and secure way of storing your assets in the new financial reality, where

STEALTH WALLET features

Supports the following cryptocurrencies:

Bitcoin · Bitcoin Cach · Etherium · Litecoin · Ripple · Monero · Dash · Zcash · Stelz coin

- Complete anonymity
- Highest known level of security
- Built-in coin mixer (for the currencies that are not initially supported)
- The possibility of passive, constant income simply by the ownership of cryptocurrency (Participation in a built-in mixer program is required)
- Private node system similar to TOR, network of private anonymous servers worldwide
- Instant payments within STEALTH WALLET system
- P2P exchange within STEALTH WALLET ecosystem (similar to ShapeShift)

Built-in VPN

Choice of online and cold wallets

Specifications

1. Wallet keys are stored:
   - on the user's device
   - in the cloud storage

   Keys and passwords to keys are generated and stored in the storage secured by the user. Keys are also saved in the shadow storage protected by a key phrase. The key phrase is stored in the main protected storage. Both main and shadow storage can be saved on a removable data storage device.

2. Blockchain is used on servers to prevent memory issues

3. Online transactions, for offline transactions an appropriate currency is used

4. Point-to-point as well as point-to-multipoint and multipoint-to-point transactions are possible

5. Using hop nodes (intermediaries) in transacting for the purpose of protecting both the sender and the recipient, combined with the option of activating this technology as well as setting the range of costs per currency

6. Cross-platform support (java, c/c#, python, ruby, go, rust)

7. Protection from external factors (DDoS, блокировки)

8. Features enabling integration with secure network services

9. Import/export of wallets for the convenience of end user

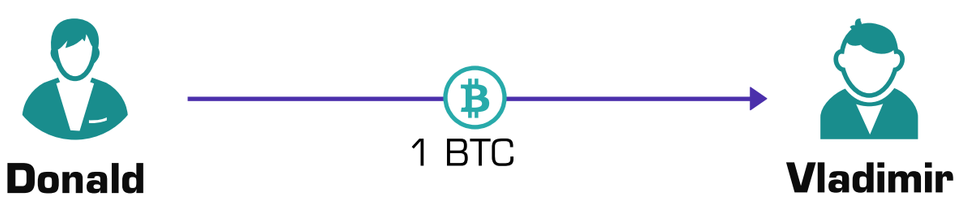
10. If the user agrees to participate in the mixing program, his funds are actively used for mixing, bringing him passive income

How it works

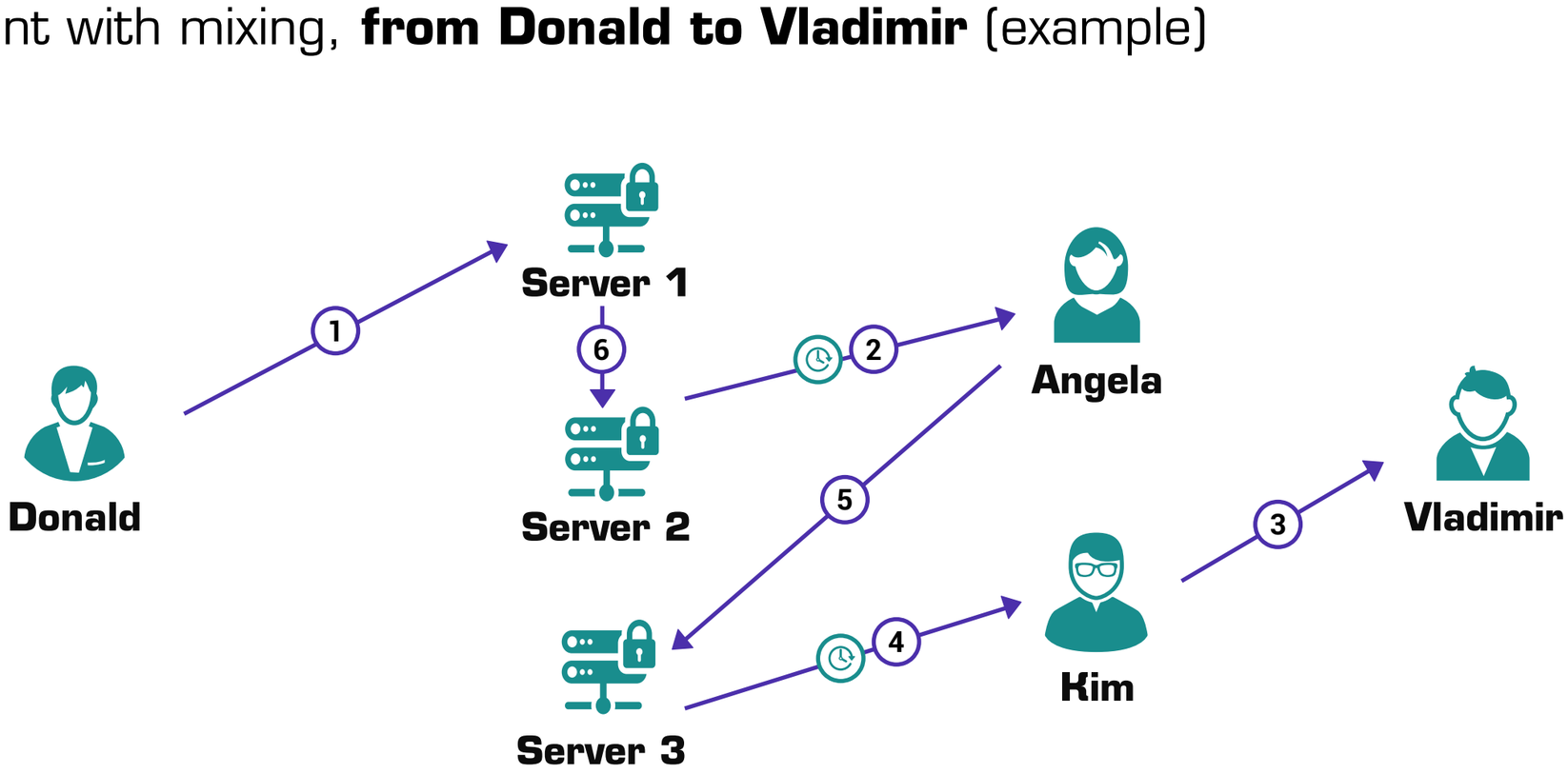
STEALTH WALLET is a unique payment system where everyone who agreed to participate in the anonymous transactions program and receive passive income through this program is mixing your coins. All transactions are instant for end users and processed automatically, with a delay for network nodes to provide better anonymity. Besides, it will be possible to make P2P exchanges inside the Stealth Wallet platform (for currencies available in the wallet). For the sake of security, we intentionally skip some possibilities here, though we demonstrate a few of them below.

So, some valid transactions available to users:

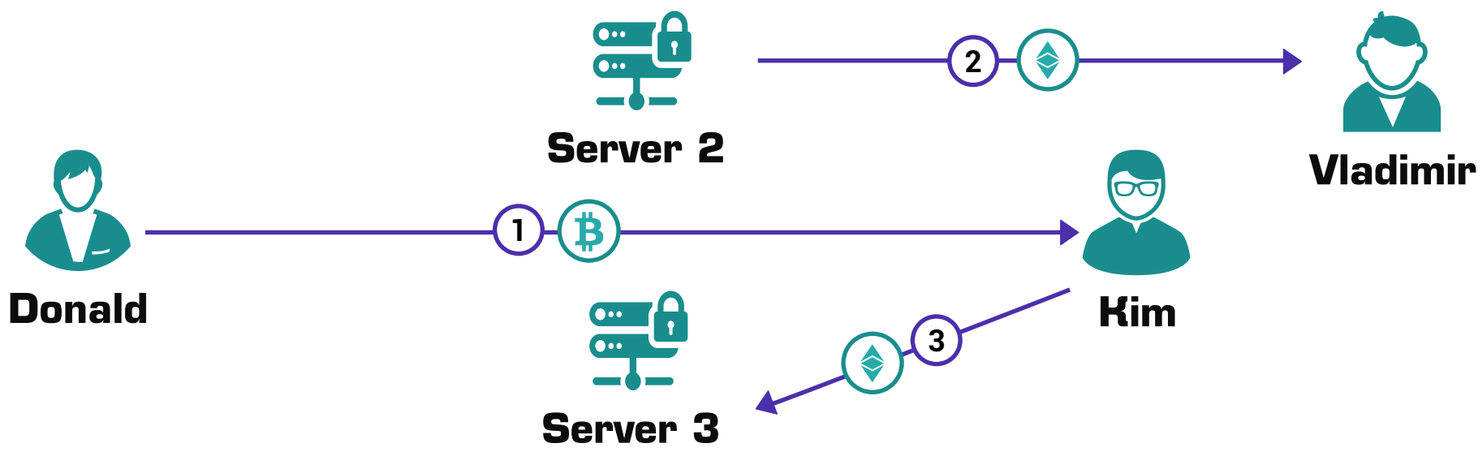
1. Simple cryptocurrency payment (Attention this transaction can be tracked!)



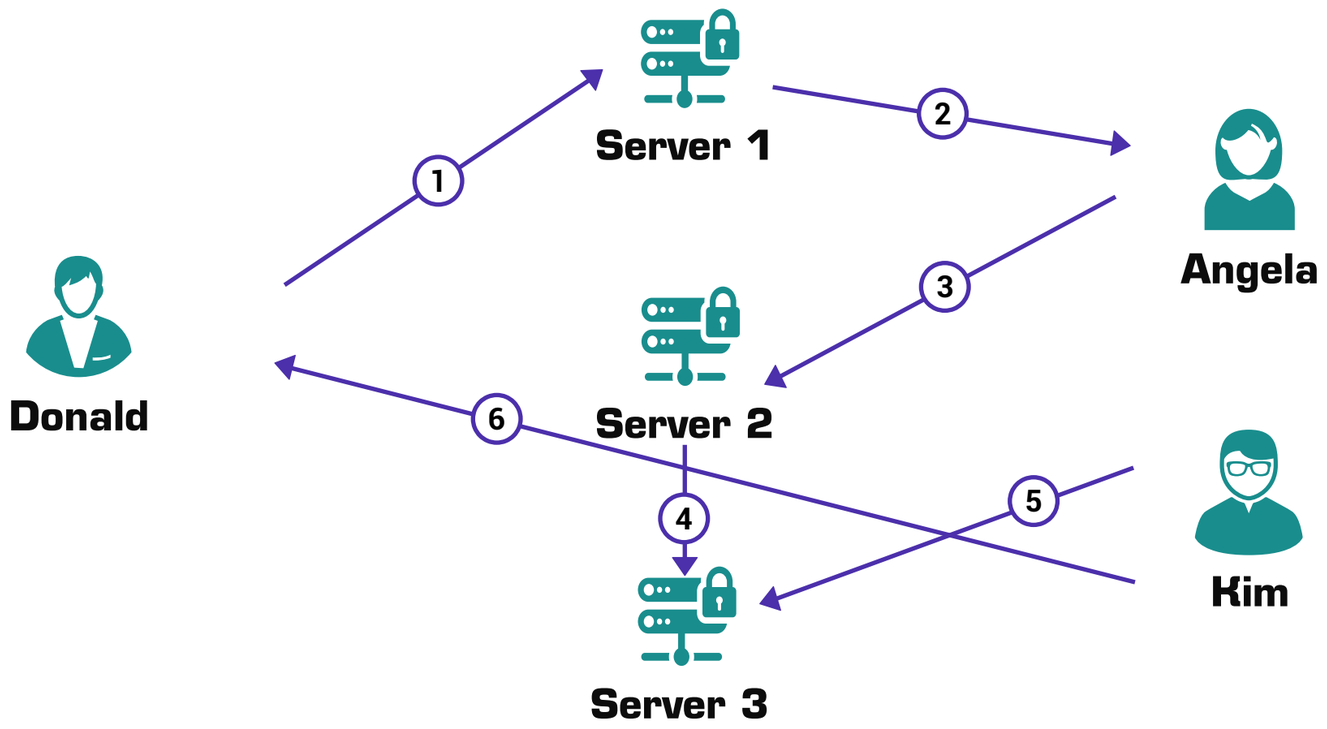
2. Payment with mixing, **from Donald to Vladimir** (example)



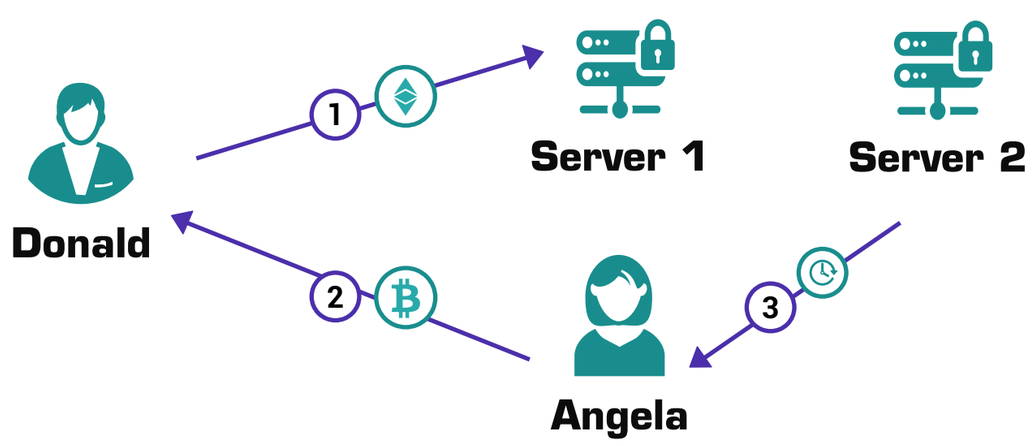
3. P2P-payment with exchange between **Donald and Vladimir**



4. Payment to yourself with mixing



4. Payment to yourself with exchange and mixing



There are many ways how STEALTH WALLET can send your coins with almost unlimited variations, which will be chosen by the system at random to provide better privacy.

Thanks to all this, complete anonymity becomes achievable, which excludes the possibility of giving away any personal data as it is impossible to track it down.

If you want to keep your private info safe and avoid falling victim to criminals or government agencies, you will simply have to use our wallet.

For making transactions we use a technology similar to Tor but with our own system of servers located across the world and which are not controlled by any official body of any country.

STELZ token

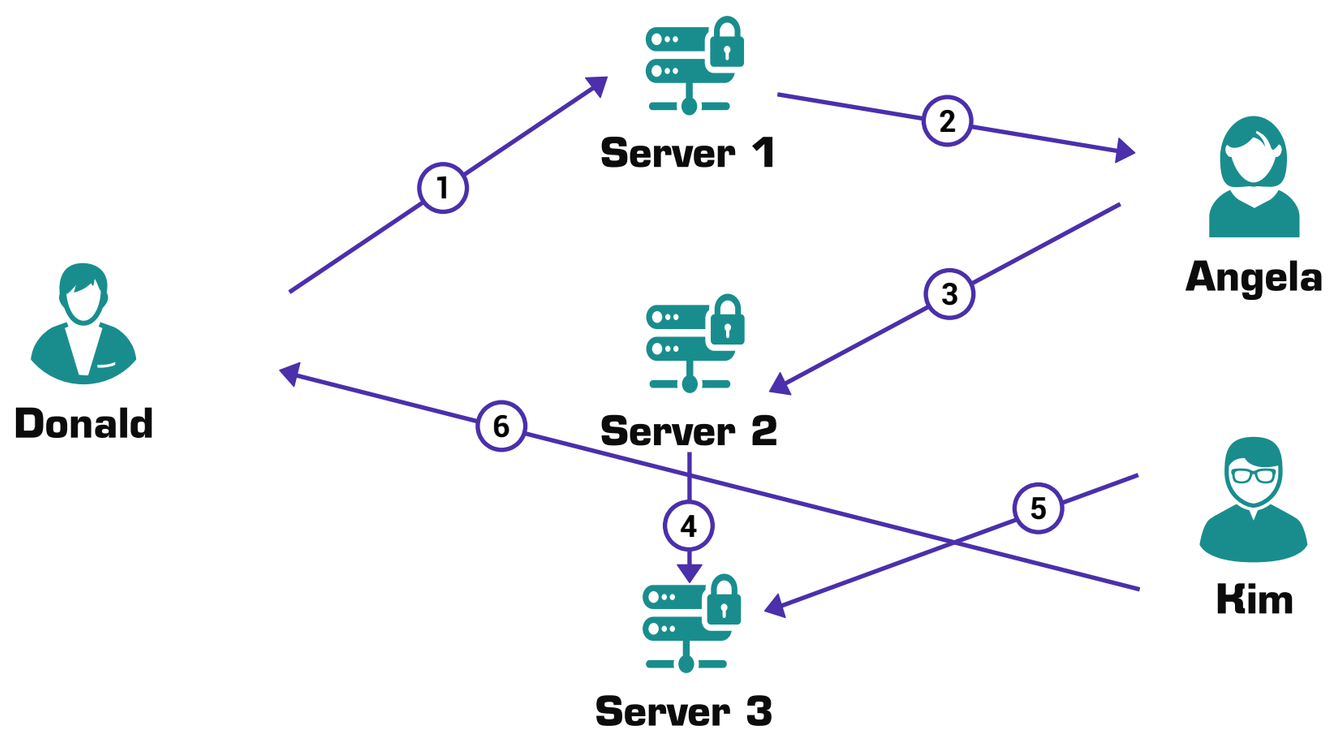
Use case for the STELZ token

- STELZ will be used as an internal currency and a means of payment for certain transactions in STEALTH WALLET
- STELZ will be used as payment to those who agree to participate in the anonymous transactions program

How it works

For example, let's take a simple transaction "to yourself with mixing"

Donald sends 1 bitcoin to himself with coin mixing.



- Here, to make the transaction, Donald has to pay 1 STELZ* as a *transaction fee**
- Accordingly, the system represented by the Servers 1, 2, 3 receives 20%, or 0.2 STELZ
- On the other hand, the individuals which agreed to offer coins in their wallets for mixing, Kim and Angela, receive 40% of the fee amount, or 0.4 STELZ each.

Stelz will be made available right after ICO for external wallets supporting ERC20 tokens (such as MyEtherWallet , MetaMask, Mist, ImToken, Parity) as well as at some *cryptocurrency exchanges.* * *

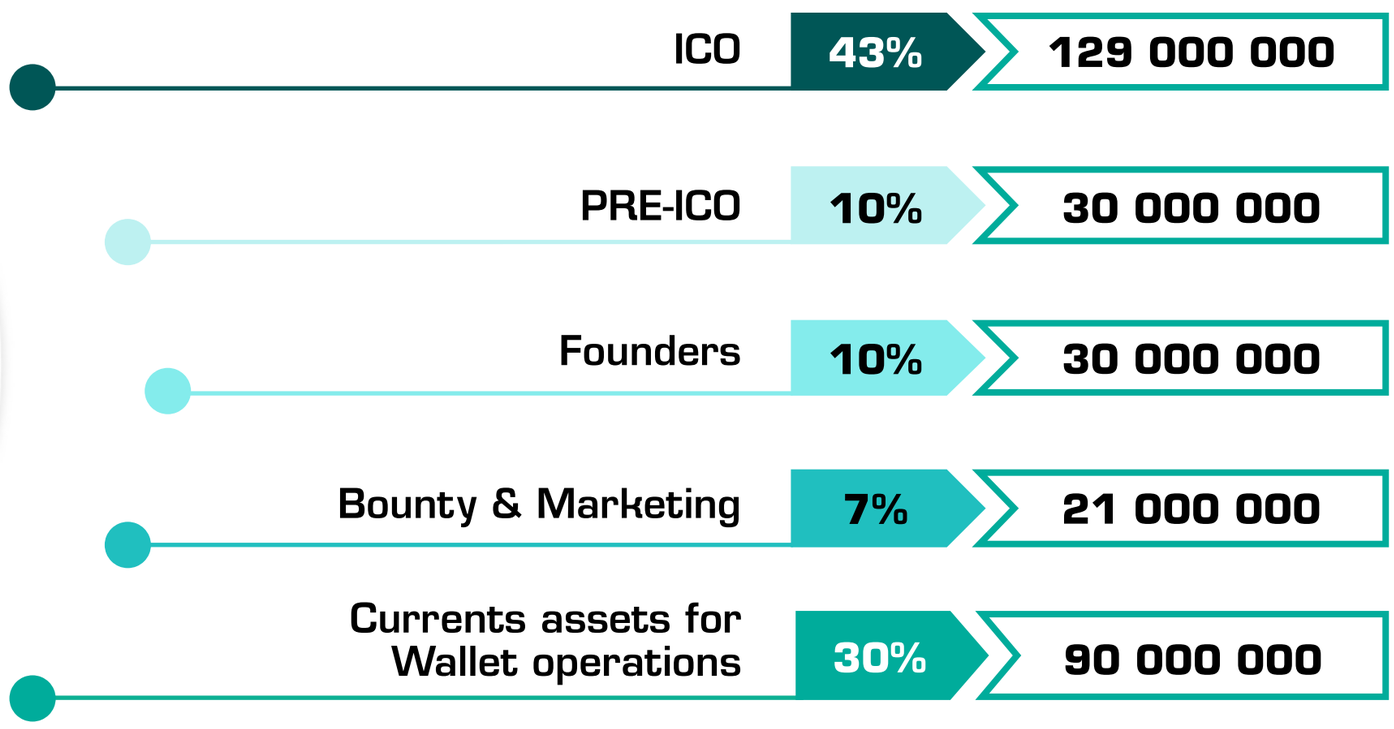
---

* As an example. The fee amount will depend on the type of the transaction and amount transacted, but it will never exceed 3% of the transaction total

** The list of the exchanges will be published after ICO

Stelz Coins Emission and Distribution

300 000 000 coins will be issued on ERC20 protocol

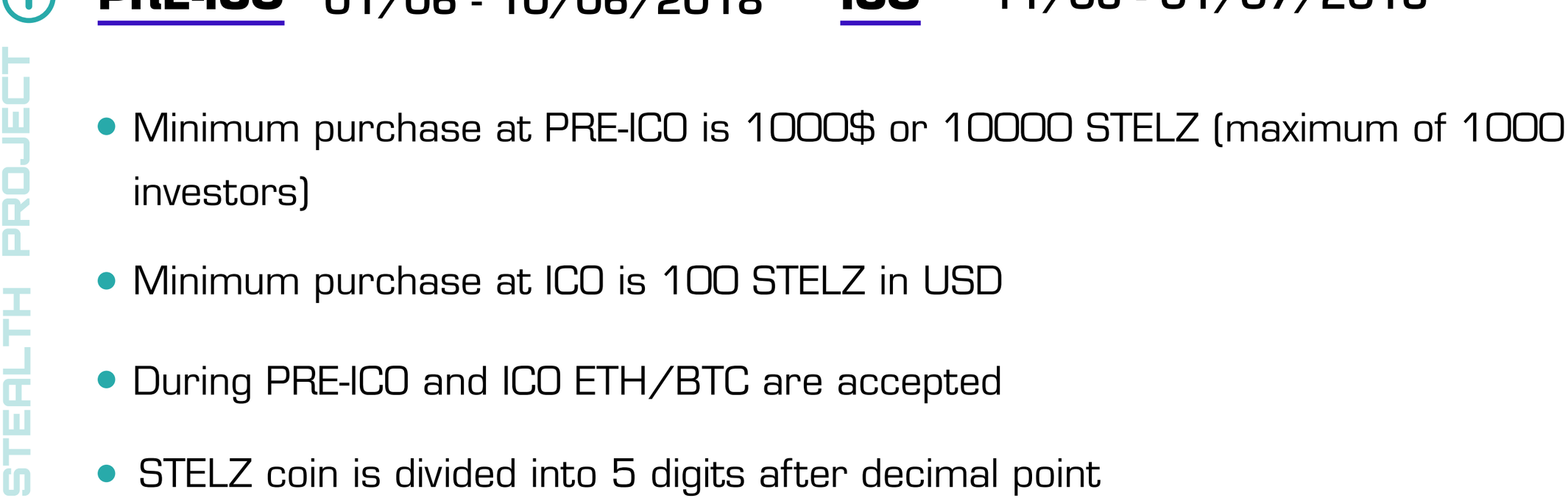


10% = 3 000 0000 - PRE-ICO
43 % = 129 000 000 - ICO
30% = 90 000 000 - Currents assets for Wallet operations
7% = 21 000 000 - Bounty & Marketing
10% = 30 000 000 - Founders

PRE-ICO 01/06 - 10/06/2018 **ICO** 11/06 - 01/07/2018

- Minimum purchase at PRE-ICO is 1000$ or 10000 STELZ (maximum of 1000 investors)
- Minimum purchase at ICO is 100 STELZ in USD
- During PRE-ICO and ICO ETH/BTC are accepted
- STELZ coin is divided into 5 digits after decimal point

Token price



Return on investment

STELZ is set to be a success without doubt since over 90000 people signed up to use the wallet at the early private sign-up phase in the Deep Web.

According to our estimates, there will be around 1M STEALTH WALLET users by the time of the release, with about 700000 transactions daily on average.

The STELZ token is required to support operation of the wallet, so it is a matter of time till its release in December when the token price should rise a few times.

Apart from that, we guarantee to buy back 1 000 000 STELZ at $0.5 after the beta-release of STEALTH WALLET on 01/11/2018. *

---

* Tokens will be bought only from the participants of the pre-ICO phase if they choose so

Raised funds distribution

As the project doesn't have a soft cap, the release of STEALTH WALLET will occur under any circumstances.

A hard cap is equal to approximately $30 000 000

- $4 000 000 will be spent on developing STEALTH WALLET on a turn-key basis
- $10 000 000 will be spent on buying anonymous physical and virtual servers worldwide and building the network similar to Tor (stage of the STEALTH PROJECT)
- $10 000 000 will be used for the project support for first 2 years (complete financial independence)
- $6 000 000 is a required liquidity level (operating capital) for the mixer

Roadmap

1 **09/2017**
Project founders first meeteing. Creation of STEALTH PROJECT

2 **10/2017 - 02/2018**
Lively discussion of a project on Deep Web

3 **03/2018**
Preparation of terms of reference

4 **04/2018**
Evaluation of project's financial credibility. Final decision to go public to start ICO.

5 **05/2018**
ICO-project preparation

6 **01/06 - 10/06/2018**
Pre-ICO

7 **11/06 - 01/07/2018**
ICO

8 **01/07 - 20/12/2018**
STEALTH WALLET software development :

- User Interface Design (UI) for Windows, Android, Mac, Web, Linux platforms (standard display resolutions)
- User Interface Design for client and server applications
- Server application development
- Windows client application development
- Web client application development
- Android client application development
- iOS client application development
- Linux client application development
- Self-testing of software

9 **09/2018**
Listing STELZ on cryptoexchanges

10 **15/10/2018**
STEALTH WALLET beta-version release

11 **01/11/2018 - 01/12/2018**
Purchase of 1 000 000 STELZ; 0,5$/token

12 **11/2018 - 12/2018**
Software acceptance testing

13 **20/12/2018**
STEALTH WALLET release

14 **01/2019 - 07/2019**
STEALTH PROJECT ecosystem development

15 **07/07/2019**
STEALTH PROJECT release

Our team

We understand that by hiding our faces and actual data we risk the release of our ICO.

However, taking into consideration the nature of the project as well as the fact that some of us are currently employed by well-known companies, we prefer to stay incognito.

We understand that we oppose a well-established system.

We acknowledge that most governments do not accept anonymity.

Our **main** principle is that that everyone has the right to privacy.

There is a strong possibility that one day we will reveal our real identities, although the dates are still to be determined.

STEALTH PROJECT founders

- Current employee of one among the largest crypto wallets
- Former manager of one among the largest search engines
- Hacker specializing in cryptolockers and cryptowallets
- Developer of The Onion Router (TOR)
- Former special services officer (USA)

Разработчики

Lead Developer

UI/UX Designers Team

Cybersecurity Specialist

Windows Developer	4	System Analyst	4
Linux Developer	4	Quality Assurance Engineer	4
Android Developer	4	Test Automation Engineer	2
iOS Developer	4	System Recources Manager	2
Web Developer	4		

All STEALTH PROJECT staff are allowed to disclose their participation in the project

Conclusion

STEALTH WALLET is set to become a modern, safe and anonymous cryptowallet with a built-in coin mixer and an option for earning passive income.

STEALTH WALLET - MIX and EARN ©

[STAGE 2]

Anonymous STEALTH PROJECT ecosystem (similar to Tor)

In practice, STEALTH WALLET is designed to be an integral part of the closed STEALTH PROJECT ecosystem with its own network of servers and a browser. Many will think that we are really going to copycat the Tor network which is already there. However, this is not quite so. Let's take a wider look.

Right now, the Tor Browser is the only widespread and popular alternative for surfing the Web.

Tor is a web browser which makes a free and open Internet space possible. It uses its own grid of proxy servers allowing several networks to interconnect anonymously at the same time with protection from snooping. The Tor system is basically a virtual network with anonymous tunnels for passing encrypted information.

When using Tor, Internet users can keep their anonymity while surfing the Web, blogging, messaging, as well as using various Web applications.

In the spring of 2011, the Tor browser developers received an award from the Free Software Foundation, and in the fall of the next year Tor received the EFF Pioneer Award, which is as significant as the Oscar award in the film industry.

Now let's look into the history of the Tor browser and its features, as well as examine its weak and strong sides.

About TOR Browser

The Tor browser was developed in 2001 by the employees of the US Naval Research Laboratory at the Supercomputing Resource Center in collaboration with the Free Haven Project. In the next year the project was declassified and its sources were handed over to information technology experts, which developed client/server software and released it into the public so that all Internet users could try it out.

According to statistics, by the end of 2014 the number of the Tor network nodes exceeded 6500, while the number of its users 2.5 million.

Use

Individuals make up the majority of Tor users, and it is particularly popular among those who are looking to safeguard their privacy and personal information as well as restrict access to blocked data. By using hidden services, Tor users are able to create sites and other online resources, while their location is thoroughly disguised.

The Tor browser is very often used by reporters to receive info from whistle-blowers. Edward Snowden is one famous user of this browser, who uses Tor to communicate various pieces of information to news outlets and websites.

Staff members of non-governmental organizations are using Tor to visit special sites in their overseas assignments when they want to disguise their professional activities from the local authorities.

In addition, civil activists from the Electronic Frontier Foundation welcome Tor as they consider it a tool capable of protecting basic civil rights and freedoms in the Internet.

Many corporations are using Tor to stealthily examine the operations of their competitors. Various special services are also making use of the browser to maintain secrecy of their sting and undercover initiatives.

Design and Function

1. Anonymous outgoing connections

Tor users run on their computers separate Onion proxy servers which connect to the main Tor servers, thereby organizing Tor web chains, which are using multilevel encryption.

All data packets entering the system pass through 3 split-level proxy servers, which are chosen at random.

Before sending a packet, it is successively encrypted with three keys. When the first server receives the data packet, it decodes the top layer of the message (like peeling the onion) getting to know where to send the packet along the chain.

The other two servers do essentially the same in their turn.

In the inner Tor networks packets are redirected between routers, and in the end they finally arrive at the output final point, where already encrypted packets reach first server. After that packets from recipient go in the opposite direction to the final Tor network points.

2. Anonymous hidden services

In 2004 Tor started to make servers anonymous as well, hiding their location in the Internet by setting special options used in the anonymity network. So you can gain access to these hidden services only if you are using a Tor client.

You gain access to hidden services by using a special top level pseudo-domain called ".onion". Such services are anonymously identified by the Tor nodes which send data packets to them. The packets are processed by regular software set up for listening on closed interfaces. Addresses in the ".onion" domain are generated with an open server key; they consist of 16 digits as well as Latin letters.

3. Limitations

Tor aims to hide a client's connection to the server, though complete obfuscation can't be achieved even in theory as encryption used here serves only the purpose of gaining anonymity in the Internet. To achieve a higher level of privacy, it is required to have additional protection for the communication hardware used. Also, it is preferable to employ steganography methods when encrypting data.

Main advantages of Tor

Tor has the following advantages:

- Free and unrestricted access to any web site from any quarter of the world, irrespective of who is your Internet provider
- Client's IP address is changed which guarantees proper anonymity
- Tor is easy to install and set up, while its use is absolutely free for everyone

- Mirror networks can be used as well
- Protection from data sniffing which may compromise privacy
- Features that may compromise security are automatically blocked
- Privacy-protection package need not to be installed. It can be run from any device, including portables

Main disadvantages of Tor

- Slow loading of web content
- Some videos can't be played
- Subpar overall security level

The most probable train of events is that Tor will remain a "good but not perfect" anonymity network available for common use.

STEALTH-browser

We allowed for all weak sides and shortcomings of Tor in the new STEALTH browser which will employ more advanced security concepts. And we are going to use the Tor network in our operation but only as far as maximum anonymity requires it.

Major deanonymization approaches used in the Internet

1. **Deanonymization through administrative means** - assumes sending official requests to a hosting provider to make available connection logs. If a few connection links are used, for example, via several VPNs, requests are made to each hosting provider, starting from the last one in the chain. As a result, it is possible to go to the first link which an individual connects to with his real IP address.

2. **Deanonymization using malware** - assumes running a malware program on a victim's computer which then reports the info about it. The reported data includes the real IP address of the victim as well. A malware program can be disguised as a regular application, image, document, or an arbitrary file. Both law enforcement agencies and special services from various countries are eagerly buying this kind of software.

It is also widely used by criminals to collect information about their victims.

3. **Timing attacks -** come in all shapes and colors. To better understand the concept behind them, imagine a bunch of tangled pipes spewing out water and a valve. How can you find out which pipe is attached to the valve? You just turn the valve off for a moment and take notice of the pipe from which water stops running.

4. **Deanonymization via vulnerability -** assumes finding a vulnerability somewhere in the chain of connections. A vulnerability in one element of a chain link may threaten the privacy of the user and instantly lead to his complete deanonymization, while other links may be resistant to this attack vector.

5. **Deanonymization via web browser vulnerabilities -** assumes the user follows a hyperlink. In that case the owner of the destination site will learn the real IP address of the victim. It is possible due to browser vulnerabilities being discovered and closed every day. We described this approach as the last in the list, though it is the most widespread one nowadays. It is popular because of its high success rate and simplicity of application as it is easier to make the user follow a hyperlink than open a file.

Respectively, our browser will be fitted with:

Cookie Autodelete

Cookies are text files with some settings stored by an application (often by a browser) for various tasks, for example, authentication.

If we want to achieve privacy, all cookies should be deleted after the browser is closed.

Convenient built-in utility similar to CCleaner will help wipe out all traces of Internet activity saved in the most remote corners of the data storage device.

Java, Flash, Adobe Reader...

All these plugins are separate applications which are run under the user account. They can ignore browser proxy settings, save their own long-lasting cookies (Flash — Local Shared Objects), etc. All plugins will be disabled or deleted. It is possible to live without Java and Adobe Reader but sometimes you need Flash since otherwise you may not be able to see the web content.

We will update Flash regularly and prevent it from saving Local Shared Objects (LSO) as well as storing cookies. Flash will be enabled only on demand in the Stealth Browser. In this manner, you will run Flash only when you really need it.

Browser Fingerprint

A browser sends dozens of values of different types, which also include so-called user agent. All such parameters may create a dangerously unique digital fingerprint of the browser making it possible to distinguish the browser from many others even within the anonymous session. Our browser will boast a built-in automatic user-agent spoofer.

Javascript

Client-side JavaScript scripts can collect and send to a server certain types of identifying data. Moreover, if a popular site is vulnerable to cross-site scripting (XSS), a hacker may be able to deliver a successful attack with all ensuing consequences. We will enable automatic recognition of this attack vector and prevent such scripts from running.

Built-in alternative to Request Policy

RequestPolicy is required for cross-site requests and protection from CSRF. Cross-site requests are made when you visit one site and it requests some resource, for example, an image from another site and then shows it to you. Such requests are often used for promotional purposes. Under certain conditions, malicious sites can do pretty bad things, for example, conduct unauthorized actions at another site with your saved cookies. Now imagine what it can lead to.

Web Bugs

The Web Bugs are invisible elements on a web page used to collect stats about the site's visitors. They can send various info about the client to the server. To block the web bugs there are two major addons such as Ghostery and DoNotTrackMe.

HTTP-referer

The HTTP-referer is an http header which can be used to determine the source of traffic. If you clicked a hyperlink on a webpage that sends an HTTP-referer, the destination webpage can find out the webpage where the request originated. Our browser will have a special feature which will control sending the referer.

HTTPS Everywhere

This addon is required if you want to use only https with sites that support this protocol.

How STEALTH PROJECT works

Our browser will be integrated into STEALTH WALLET with the network designed to operate in the following way:

User → VPN → Remote Desktop → STEALTH → Internet

Deanonymization through administrative means	**High-level protection**
Deanonymization using malware	**High-level protection**
Deanonymization via timing attacks	**High-level protection**
Deanonymization via vulnerable connection-chain elements	**High-level protection**
Deanonymization via web browser vulnerabilities	**High-level protection**

This is the most reliable part resistant to both active approaches to deanonymization and deanonymization through administrative means. Low speed due to Tor limitations is its main disadvantage. However, we are going to solve this problem by using our own nodes.

In the end, any solution will include a proxy for changing IP address periodically.

No logs are saved, either known or hidden.

A master password is used for encrypting all passwords, so that it is impossible to have a sneaky peek at them in plain text. Other features are to be discussed with the community during the process of browser development

[STAGE 3]

Building a grid of private sites within the anonymity network STEALTH PROJECT similar to .onion network

onion — is a special pseudo-domain of the top level (similar in application to .bitnet and .uucp domains used before) for accessing anonymous or pseudo-anonymous addresses in the Tor network (abbreviated from The Onion Router). These addresses are not valid DNS entries, and they are not stored by the root servers in the DNS hierarchy. When using special software to access resources in the Tor network (for example, Orbot for Android or Torbutton plugin for Firefox), applications can access resources in the .onion domain by sending requests via the network of Tor servers.

You will be able not only to host sites within our network but also to take advantage of our easy-to-use site builder integrated with the STELZ payment system, which would allow as well free exchange of cryptocurrencies supported by STEALTH WALLET.

All in all, what we go for is:

1. Secure decentralized network with privacy protection as well as integrated service infrastructure
2. Anonymous publication of information via Web technologies
3. Protected transactions between members of the network

Implementation Requirements

1. Compulsory encryption of traffic (TLS/SSL) with session keys (P2P)
2. Partitioning of traffic between network members
3. Hiding IP addresses of nodes providing network resources
4. Network infrastructure integrity