1M5: Invisible Matrix Services

September 12, 2019
v2.0
https://github.com/1m5/1m5-docs

1M5

UNCENSORED COMMUNICATIONS

Whitepaper

Contents

0.1 Abstract

1M5 (Invisible Matrix Service—using leet) is the first decentralized services platform with intelligent routing between anonymity networks to bypass censorship. This is required as a base level for digital communications to ensure freedom of speech, expression, association, and assembly using electronics.

Censorship resistance is currently accomplished using Tor and I2P. In the future, it will include 1DN (a direct wireless ad-hoc network using radio and LiFi as well as other future anonymity networks. When a user's device gets blocked on one network, other networks are used to route around the block until another node can make the request.

In an effort to pre-empt 1M5 being shut down, the project is not being classified as an organization nor registered in any jurisdiction. Rather, it is a shared global mission between those who wish to support freedom of speech, expression, association, and assembly among all beings. Aligning with and following any laws of a particular jurisdiction would create a leverage over the mission ending its ability to sustain it. Operating the mission with common ethical principles such as the non-aggression principle [2] (NAP) and voluntaryism [3] (voluntary relationships) is key. Working with any entity known for aggression, especially of the systemic sort, compromises those ethics and is thus antithetical to the mission.

0.2 Collaborators

This paper represents the combined efforts of many individuals, whether directly or indirectly. Please address correspondence to info@1m5.io.

Brian Taylor: objectorange@1m5.io (PGP: DD08 8658 5380 C7DF 1B4E 04C2 1849 B798 CF36 E2AF)
Amin Rafiee: evok3d@protonmail.com (PGP: E3AA 4FDC0 AFC68 1CBBC 0266 BED5 BCCF CAEF F94DB)
Editor: Catherine Tansey (https://www.linkedin.com/in/catherinetansey)

1M5 would like to acknowledge the efforts, white papers, and communications of others in the privacy, open-source, blockchain, security, and decentralization space, whose work have contributed to the mission.

[1] Li-Fi. https://en.wikipedia.org/wiki/Li-Fi, 2019.
[2] Non-aggression principle. https://en.wikipedia.org/wiki/Non-aggression_principle, 2019.
[3] Voluntaryism. https://en.wikipedia.org/wiki/Voluntaryism, 2019.

1 Introduction

The fall of the Berlin Wall in November 1989 ushered in a new era, one with expectations of a more open and free global human society. Yet only several decades later we've experienced digital walls erected by governments and large corporations in the name of protection. These walls promote segregation and censorship of information while harming creativity, innovative technology, and freedom of speech.

> "Freedom of Speech is a principle that supports the freedom of an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship, or sanction. The term "freedom of expression" is sometimes used synonymously but includes any act of seeking, receiving, and imparting information or ideas, regardless of the medium used." [4]

Constraining the free flow of information between people is a direct threat to our freedom and censorship of communications online is growing worldwide [5].

Online communications are censored at the point of entrance by Internet service providers (ISPs), which act as the gateway and gatekeepers to the Internet. Their ability to restrict usage and track users' online activities via a leased IP address grant ISPs—corporations or often governments—control over freedom of speech and information. To make ISP tracking more challenging, a number of tools have been developed to mask the source and destinations of internet routes using onion-/garlic-routing [6]. In such cases, this identifying information isn't available without breaking encryption, a near-sisyphean task today considering the encryption algorithms used.

> "Censorship is the suppression of speech, public communication, or other information, on the basis that such material is considered objectionable, harmful, sensitive, politically incorrect or "inconvenient" as determined by government authorities or by community consensus." [7]

[4] Freedom of Speech. https://en.wikipedia.org/wiki/Freedom_of_speech, 2019, 2019.
[5] Documenting Online Censorship. https://internetfreedomwatch.org/timeline/, 2019.
[6] I2P. Garlic Routing. https://geti2p.net/en/docs/how/garlic-routing, 2019.
[7] Censorship. https://en.wikipedia.org/wiki/Censorship, 2019.

Many governments are using IP (Internet Protocol) geo-fencing (e.g. China's Great Firewall) to isolate people from global information and to facilitate mass surveillance (e.g. the US' NSA Prism and China's Social Credit System) and increase self-censorship. These systems are now being replicated by many other governments worldwide, working together to spy on the masses globally (e.g. Five/Fourteen Eyes).

In today's digital world, we're losing our privacy—the bedrock of freedom—at an alarming rate. Most large organizations (e.g. tech giants, the banking industry, governments) track and use our online behavior for their profit (e.g. captology [8]). Whistleblowers, the abused, minorities, and a myriad of other people could be emboldened by anonymity to speak out in a manner that would otherwise be unavailable if they were forced to identify themselves. Decentralized applications, like Bitcoin, are helping to wrestle some control from centralized organizations, although they struggle to maintain anonymity at the network layer. Smartphones, our primary means of global communication and collaboration, poorly maintain user anonymity and privacy, critical components to ensure individual freedom.

Two primary tools today that support anonymity are Tor and I2P [9], both internet overlays. Tor provides a browser making the tool more user friendly, while I2P is much less known. Both are complementary in that Tor was designed for browsing today's current web sites anonymously while I2P was designed for peer-to-peer communications within I2P. Neither have good APIs for developers to embed in their products, making uptake slow for many applications.

A third tool on the horizon circumvents ISPs completely by removing the need for them. Called direct wireless ad-hoc networks, these tools communicate directly between personal devices using technologies such as WiFi Direct. Firechat [10], the app used for communication during the 2014 Hong Kong protests when the Chinese government threatened to shut down the internet, is one example of this type of tool.

Meshing solutions provide access to multiple networks to benefit from each network's strengths but none provide an anonymous mesh. New mesh solutions are popping up that seek to improve on earlier designs. But the technology is still in its infancy and needs to be pulled into everyday applications more easily once they've matured.

[8] What is Captology. https://captology.stanford.edu/about/what-is-captology.html, 2019.
[9] I2P. https://geti2p.net/en/about/intro, 2019.
[10] Firechat. https://www.opengarden.com/firechat, 2019.

However, wider circulation of these technologies doesn't solve the problem of online censorship. Many people are constantly finding ways to circumvent these technologies to censor and steal information, and therefore a better solution is needed.

Tech-savvy people can normally find a way to bypass censorship and maintain privacy, but the overwhelming majority can not. This prevents the critical mass needed to make large-scale positive change on a political level, globally. Censorship resistance and data privacy must be available to and used by an overwhelming majority so that all people can become free and remain so.

Mission & Objectives

2.1 Mission

1M5's mission is to protect freedom of speech, expression, association, and assembly over electronic communications for all beings by ethical, sustainable means. The core beliefs driving the mission are:

- All people have a natural right to freedom of speech, expression, association, and assembly.
- All relationships must be voluntary.
- Privacy is the bedrock of freedom. We should be able to communicate as we please, privately and anonymously.
- Transparency in code/governance.
- Individuals own their data and should be the ones that profit from it.
- Self-sovereign identity. Individuals must establish and maintain their own identities, removing 3rd parties from the process.
- Self-sovereign money: Empower people to be their own bank, indebted to no one, with the keys to their own money.

2.2 Objectives

1M5 attempts to help achieve:

- Freedom of Information: Support sharing of and access to information free from censorship.
- Shielded Distribution: Support sharing of and access to information without fear of prosecution.
- Peer-to-Peer: Support P2P communication without the need to depend on servers nor the Internet (The People's Direct Network). Cut the cord to ISPs for good.
- Self-Sovereign Identity: Provide a self-sovereign identification system to establish reputation whereby the keys are owned and maintained by the individual.
- Self-Funded Protocol: Ensure sustainability by providing a platform that is self-funded.
- Privacy Control: Enable control over monetization of personal information. Users determine what is shared with and sold to 3rd parties.

3 Solution

The internet was not designed for anonymity. This feature must be implemented into a more open system from the beginning, at the most foundational levels, to ensure anonymity can be provided for all people under all circumstances.

To ensure privacy, while maintaining code and hardware transparency, hardware required for decentralized autonomous applications (dapps) [11] should be recommended based on openness (e.g. open-source hardware, 3D printing) or provided by 1M5.

Dapp platform supports a base level of services for running its framework and the minimal services for ensuring mission success. This includes a sensors service that provides intelligent routing across anonymity networks. It should be pluggable as new sensors come online. The platform should also support pluggable services for providing additional functionality as dapps require (e.g. a decentralized content distribution network).

The identification system will be self sovereign and reputation based to ensure privacy is maintained while allowing relaxation of privacy incrementally as desired as trust grows. Both machines and people can have identities. Both should be able to use identities anonymously, pseudo-anonymously, selectively, or fully open to everyone (public). Identities can be generated by the platform or brought to the platform as well as the ability to use those identities with other platforms—open standard identity technology will be well supported (e.g. OpenPGP).

1M5's solution will also support individuals voluntarily selling parts of their personal information while ensuring it remains secure on their flash drives. If a user loses their device, their new device will be able to restore itself with no loss of data.

Ensure the platform can be self-sustained by monetizing resources—network bandwidth, CPU cycles, and persistent storage—through the use of an internal token. Donations are fine for getting the core on its feet, but long-term sustainability requires self-monetization.

---

[11] Decentralized autonomous organization. https://en.wikipedia.org/wiki/Decentralized_autonomous_organization, 2019.

3.1 Context

1M5 works to provide private censorship-resistant communications as a base layer for dapps far and above anything in the marketplace.

3.2.1 Censorship Resistance Routing

The first layer in a secure highly network-based application must be a layer supporting anonymity. This is accomplished by 1M5's Sensor Service by using I2P [9] as the basis for routing over the internet, Invisible Direct Network (1DN) comprising radio & LiFi [1] when the internet is not accessible, and Tor for communicating with non-anonymous nodes in the clearnet like Bitcoin nodes. This routing is managed intelligently using a peer graph across all supported anonymous networks.

- **I2P:** an overlay network over the internet using garlic routing to provide anonymity and end-to-end encryption for privacy using a volunteer network of approximately 65k nodes. Garlic routing [6] encrypts multiple messages together using multiple levels of encryption so that each node that performs routing is only aware of the previous node and the next node but no other nodes especially the originating node. Endpoints are cryptographic identifiers (public keys).

- **1DN:** a wireless ad-hoc network as a sensor to provide private communications outside of the internet using WiFi Direct, the full radio spectrum (Software Defined Radio – SDR), and LiFi [1]. As of 2019, LiFi is an emerging technology.

- **Tor:** directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis using onion routing. Primary focus is on private browsing of clearnet sites and providing hidden service sites.

3.2.2 Orchestration

This component provides application orchestration through simple content-based routing (CBR) with support for Enterprise Application Integration (EAI) pattern routing and decentralized algorithms as the code base grows. Current routing uses by default

[1] Li-Fi. https://en.wikipedia.org/wiki/Li-Fi, 2019.[9] I2P. https://geti2p.net/en/about/intro, 2019.
[6] I2P. Garlic Routing. https://geti2p.net/en/docs/how/garlic-routing, 2019.
[9] I2P. https://geti2p.net/en/about/intro, 2019.

a Dynamic Routing Slip [12, 13] implemented as a stack. It's dynamic in that each service can push additional routes onto the stack at any point in the current routing of the message. For example, an end-user may wish to access Service A but when it gets to that service, Service A requires authentication, so Service A adds a call to the Authentication Service and a call back to Service A with the results. Once the results return to Service A, it will perform the service as desired. Other likely examples include data service requests whereby a service needs additional data to satisfy the service request.

3.2.3 Key Ring

Encryption and Signing keys kept safe on specialized flash drives that when added they can not be read nor changed. Encryption and signing happen on-drive only, using the OpenPGP standard.

3.2.4 Decentralized IDentifier (DID)

Self-Sovereign Identity [14], Reputation Based Access Control, and Circles of Influence. The DID service works with the Key Ring service to provide identity services. Anyone can get on by providing a DID, but can be restricted in what they can do based on reputation. As of mid-2019, only Self-Sovereign Identity is implemented with OpenPGP and only minimally.

Requirements

- Identity through Correlation [15].
- Reputation Based Access Control.
- Identity Recovery.

Self-Sovereign Identity

Provide means for importing, generating, using, and exporting cryptographic identities supporting well known and used standards.

Reputation-Based Access Control (RepBAC)

Not to be confused with Role-Based Access Control (RBAC), RepBAC supports users in placing restrictions on access based on reputation parameters.

[12] Dynamic Router. https://www.enterpriseintegrationpatterns.com/patterns/messaging/DynamicRouter.html, 2019.

[13] Routing Table. https://www.enterpriseintegrationpatterns.com/patterns/messaging/RoutingTable.html, 2019.

[13] P2P Foundation. https://wiki.p2pfoundation.net/Self-Sovereign_Identity, 2019.

[15] Joe Andrieu, Kevin Gannon, Igor Kruiper, Ajit Tripathi, Gary Zimmerman. Identity Crisis: Clearer Identity through Correlation. https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/final-documents/identity-crisis.pdf, 2016.

Circles of Influence

Build groups of identities automatically based on a set of defined reputation parameters. Aids in quickly building groups on known reputation parameters.

3.2.5 Info-Vault

Keeps personal information confidential and available on personal flash drives.

3.2.6 Monetization (Aten & Prana)

Currently, 1M5 is funded by donations; no monetization is in progress. If/when monetization is decided on, it will be to monetize people's hardware resources (network, CPU, storage) and users' personal information, all on a voluntary basis. Tokens will be used in this network to keep track of usage, just like a utility provider. End users could offer their resources for tokens to others who desire additional resources on demand or scheduled in the future. They could also exchange tokens with others in the applications to receive additional resources on demand or scheduled in the future. All transactions would incur a transaction fee to fund development and maintenance of the network based on current approved budget requirements (should be less than 1%, if not much lower). Further details are to be expected through future design. Monetization subject to change at any time as the design below is in a very rough draft. Exchanges will be supported using a Decentralized Exchange (DEX) [16].

- **Aten – Development Tokens:** These are limited to developer (mission and system) hours and/or funds used in building, maintaining, and supporting the network. Percent ownership of Aten tokens out of total outstanding Aten tokens determines the percent of the distributions from the transaction fees. Transaction fees are paid in Prana.

- **Prana – User Tokens:** These are limited to the end-users' resources brought to the network. They can be used within the 1M5 network of Dapps for services if the Dapp supports it.

- **Tor:** Komodo [17] (KMD) tokens are collected when User and/or Development tokens are exchanged with KMD tokens.

[16] Komodo. Atomicdex. https://atomicdex.io, 2019.
[17] Komodo. Antara Framework. https://komodoplatform.com/antara-framework, 2019.

3.3 MANCON

1M5 dynamically bypasses attempts to censor communications within application in which 1M5 is implemented. It does so by maneuvering against blocks and attacks on the internet as well as direct mesh networks. This maneuvering experiences varying levels of situational conditions called MANCON.

MANCON is an alert state signalling the maneuvering required to achieve the mission. It can change at any time in response to new conditions arising. The base MANCON recommended for a claimed jurisdiction is largely based on the World Press Freedom Index [18].

End-users can at any time select the MANCON they feel they need to protect their privacy.

MANCON 5 – Low

No expected censorship or privacy intrusion attempts.

- **Web:** Will use HTTPS. Failures will assume the site is down.
  - Tor for .onion addresses.
  - I2P for .i2p addresses.
  - No additional latencies.
- **P2P:** I2P is used for peer-to-peer services such as messaging.

MANCON 4 – Medium

Typical censorship attempts by states on reading news (public web sites getting blocked, government shutdown of cloud cdn content). No fear of circumventing censorship expected.

- **Web:** When an HTTPS clearnet site appears down, other nodes will be used to attempt access. If these fail, the site will be assumed to be down.
- All other routing remains unchanged (See MANCON 5).
- **Latency:** 500 milliseconds to 2 seconds.

MANCON 3 – High

Strong censorship attempts are being made with freedom of speech getting little support. Borderline police state is emerging. Potential retaliation for circumvention of censorship attempts. This is the default setting for 1M5.

- **Web:** Will use Tor as default access to clearnet sites. When Tor gets blocked, will use I2P/1DN to route around blocks.
- All other routing remains unchanged (See MANCON 5).
- **Latency:** 1-10 seconds.

MANCON 2 – Very High

Police state emerging. Prison likely for censorship circumvention attempts.

- **Web:** Will use an I2P peer with random delays that has access to Tor to make the request.
- **P2P:** Direct comms with I2P but with random delays up to 90 seconds per I2P relay node.
- **Latency:** 4 seconds to 3 minutes.

MANCON 1 – Extreme

Police state / dictatorship. Local cellular service towers shutdown.

- **Web:** A 1DN peer will be used to access Tor and/or I2P.
- **P2P:** A 1DN peer will be used to access Tor and/or I2P.
- Intentional random delays 90 seconds to 5 minutes per 1M5 relay node (up to 90 seconds per I2P relay node) will be used to help protect end-users.
- **Latency:** 4-30 minutes when in large cities with many 1M5 nodes.

4 Implementations

4.1 Proxy (In Active Development as of 2019)

1M5 Proxy Service acts as a proxy for your favorite browser routing all clearnet and .onion requests through Tor and all .i2p requests through I2P. When Tor gets blocked, it uses I2P/1DN to find a peer with Tor unblocked to complete the request.

4.2 Browser (Researching)

Pre-configured bundling of Tor Browser with 1M5 Proxy for ease of use.

4.3 Phone (Planning)

Minimalist phone on open hardware and software with no closed or proprietary systems.

- Only 1M5 core with sensors, proxy, browser, and messenger will be installed.
- Only additional 1M5-based services and applications will be supported.
- Hardware will be based on Raspberry Pi Zero W.
- Operating system will be a minimal Linux From Scratch (LFS) build.
- To include camera and microphone.
- Will use 1DN (the outernet: full spectrum Radio + LiFi) and internet (Tor + I2P) when necessary.
- Perfect for places with no infrastructure and people being targeted.

4.4 Decentralization of Things (DoT) (Planning)

- Minimalist DoT headless devices on open hardware and software with no closed or proprietary systems.
- Only 1M5 core with sensors will be installed while only additional 1M5-based services will be supported.
- Hardware will be based on Raspberry Pi Zero W.

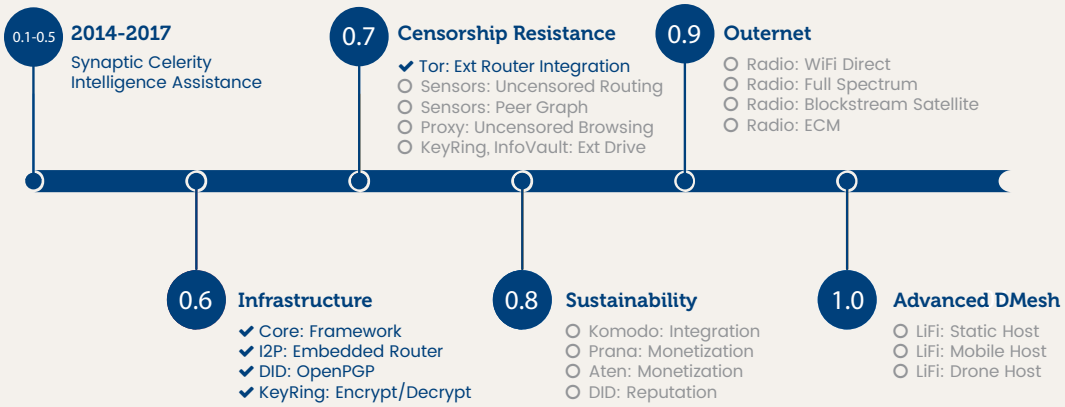
- Operating system will be a minimal Linux From Scratch (LFS) build.
- Will use IDN (the outernet: full spectrum Radio + LiFi) and internet (Tor + I2P) when necessary.
- Perfect for places with no infrastructure.

4.5 DoT Drone (Planning)

- Places the DoT device within a mobile platform.
- Multiple drones will be available for specific use cases.

5 Development Roadmap

IM5's development is solely dependent on the support received via donations and contributions. These plans may change due the nature of technological development and advancements. The goal will remain to support the best technologies available.

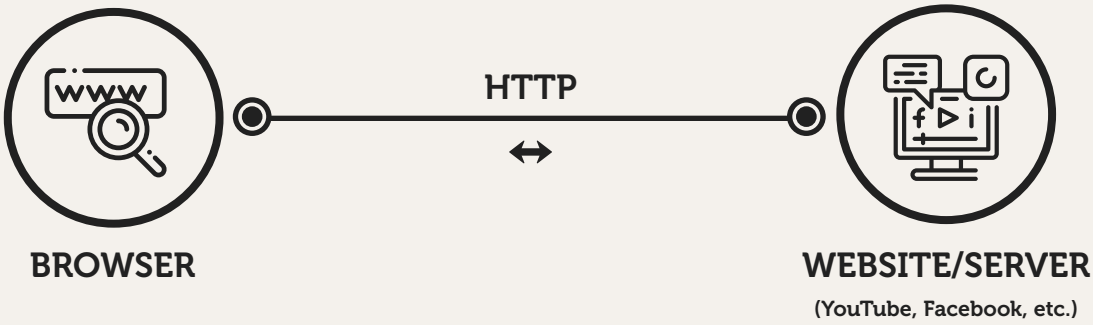


6 How 1M5 Works

6.1 Scenario 1: Viewing a Clearnet Website

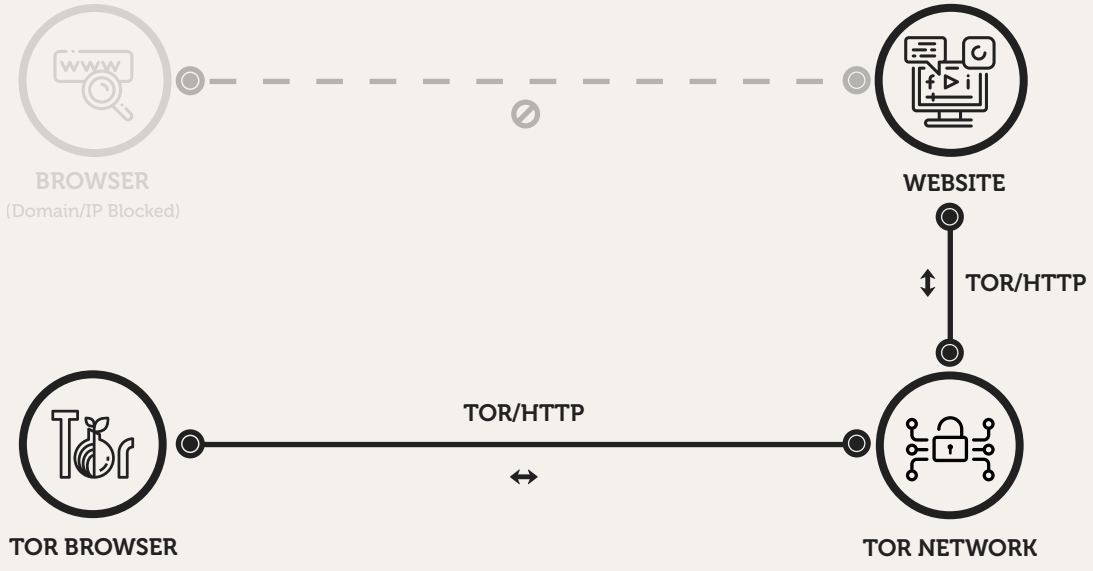
6.1.1 Situation 1: Standard Access

A browser is used to connect to a web site. If this path is blocked by the Internet Service Providers (ISP) or the government, users look for a way around the block.



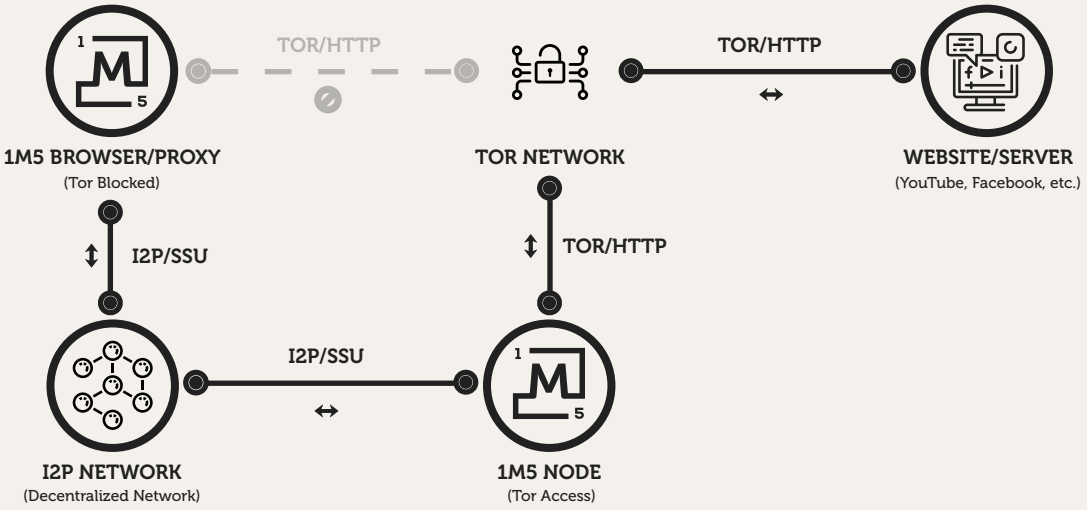
6.1.2 Situation 2: Domain/IP Blocked

The Tor browser is successful in bypassing blocks as long as the exit nodes are not blocked. But more astute governments (e.g. China, Iran) find the entrance nodes running Tor and blacklist the IP addresses, preventing access to the Tor network.



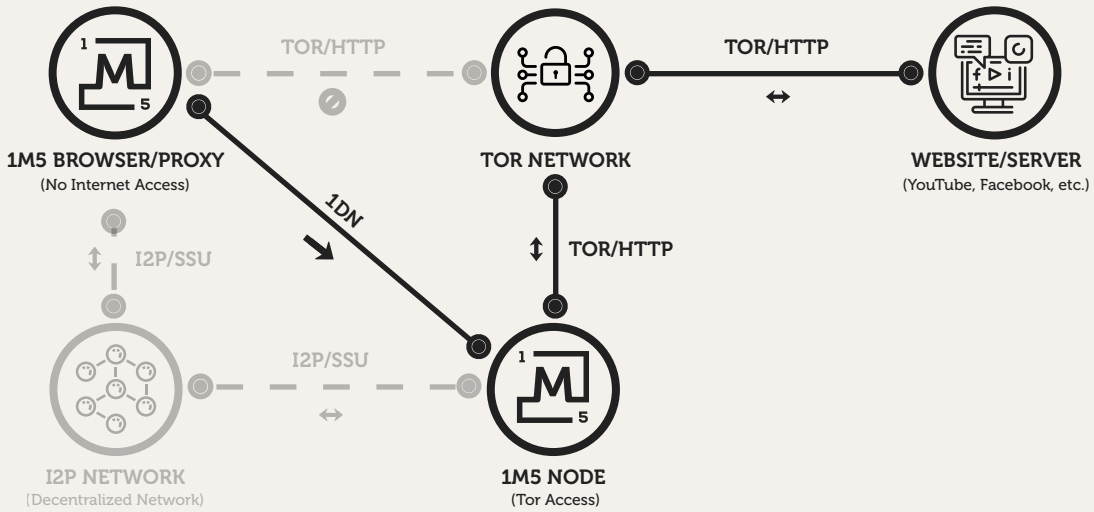
6.1.3 Situation 3: TOR Blocked

Unable to access the Tor network, the request is sent to another 1M5 node that has access to Tor (using I2P). The secondary DApp node's 1M5 instance connects to the site desired, collects the response, and forwards it to the original requester.



6.1.4 Situation 4: No Internet Access

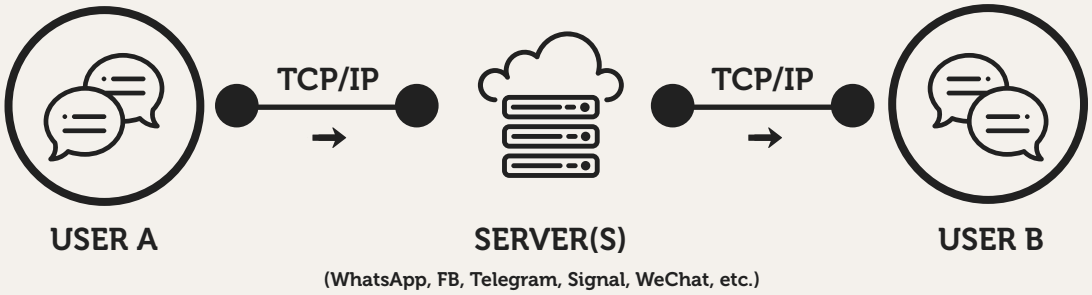
1M5 uses the 1DN ad-hoc network (e.g. WiFi radios in your phone) to route out until it successfully locates a 1M5 node with Tor access.



6.2 Scenario 2: P2P Applications

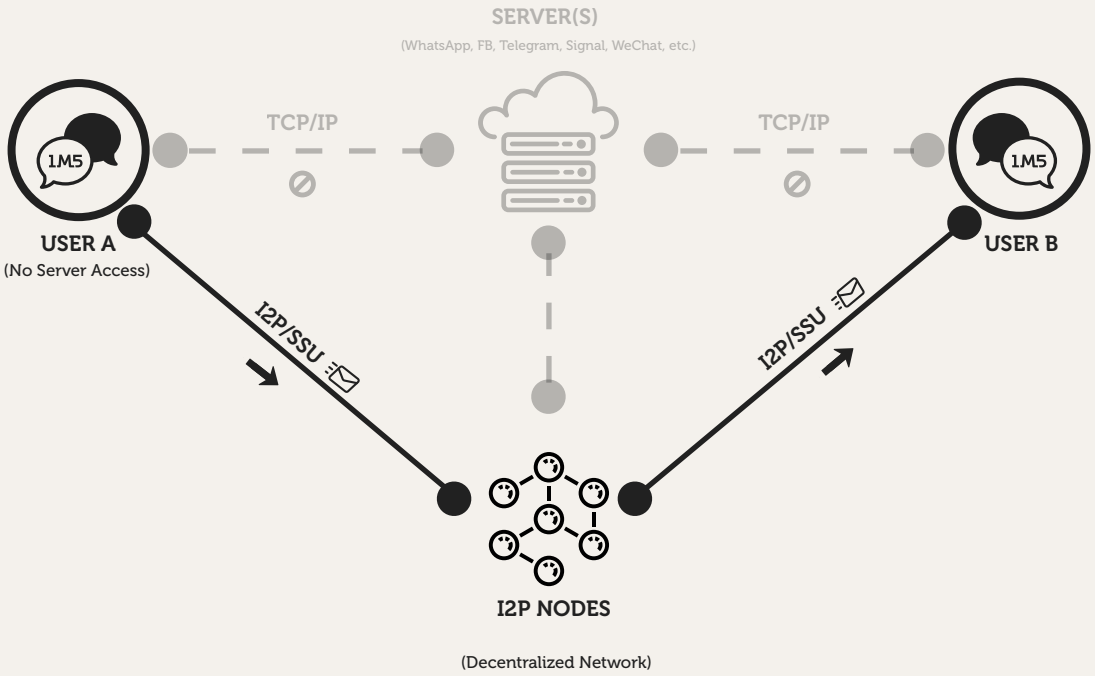
6.2.1 Situation 1: Centralized Access (The Norm)

A typical messenger using TCP/IP (the Internet) to communicate with a centralized server.The message is then forwarded to the end-user by the server.



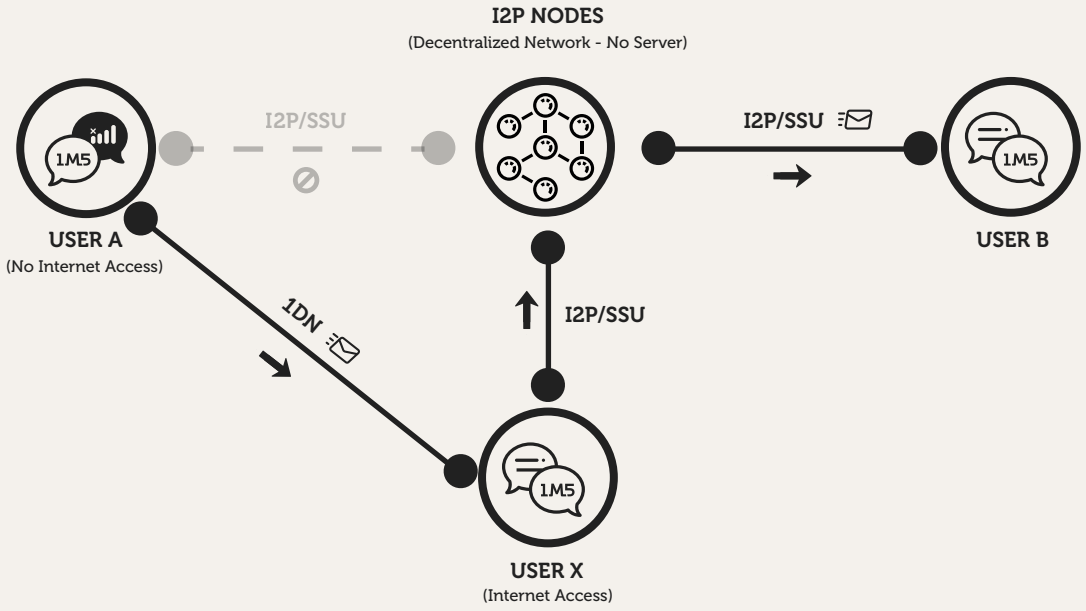
6.2.2 Situation 2: Servers Are Blocked

A messenger (1M5 embedded) is used for messaging over I2P (SSU) preventing censorship by shutting down or blocking a server (no servers are used).



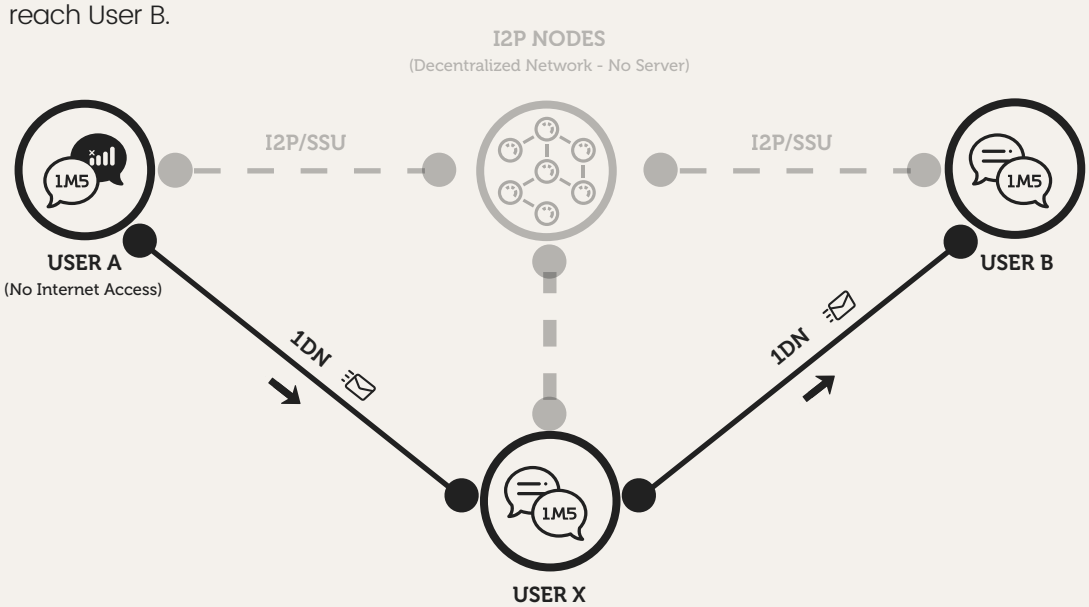
6.2.3 Situation 3: No National Internet Access

User A has no Internet access to reach User B. The protocol uses the 1DN sensors (radio and/or LiFi) depending on latency and/or security requirements to get the message to a 1M5 peer who has Internet access (User X). The message can then continue through I2P's decentralized network until it reaches User B.



6.2.4 Situation 4: Global Internet shutdown

User A has no internet access and protocol is unable to find any users with an active internet connection. The protocol uses the 1DN sensors (radio and/or LiFi) for all communications. The message will relay through the 1M5 network of peers until it can reach User B.



7 Integration

The following outlines various ways that 1M5 can be integrated.

Chat

1M5 would use I2P to route messages between messaging apps switching to 1DN (radio & LiFi) when internet access is blocked.

Browsing

1M5 would work to ensure end-users can browse any publicly available web site globally regardless of block attempts. All .onion and .i2p sites would automatically work without configuration. Tor entry node blocks (e.g. China) would get routed around using I2P/1DN.

Email

1M5 would initially use I2P's email system using public keys as destinations with optional aliases. Future 1M5 work would result in the 1M5 network having a decentralized email system to ensure email would work regardless of internet access, which is required by I2P.

Social

IM5 would enhance messaging functionality to include a reputation system.

Office Suite

1M5 would provide google-docs like office sharing workspace with censorship-resistant access and decentralized content distribution (e.g. Inkrypt [18]).

OS

1M5 would be integrated directly in the operating system. All communications can take advantage of the decentralized censorship-resistant communications. Would likely require rewriting 1M5 in C++/Rust/etc away from Java.

[18] Inkrypt. https://www.inkrypt.io, 2019.

8 Legal

The following general information applies to this document.

8.1 General

This effort is a mission not confined to any jurisdiction as it would risk alienating individuals and providing a vector for attack. This doesn't mean that others will not attempt to exercise control over it, that is to be expected as free speech is given more lip service world-wide than actual support. No one person speaks for the natural right to free speech, expression, association, and assembly and this mission seeks to uphold that natural right.

8.2 Risks

Decentralized autonomous missions like 1M5 are new efforts not associated with any one state and therefore have none of the protections or support of state-registered organizations. Jurisdictions world-wide may establish laws in an attempt to govern efforts like 1M5 or others in the future.

8.3 Representation and Warranties

Security is never a guarantee. It is a constant effort for us all to prevent theft by others. Therefore, no warranties can be offered. Know the limitations of the system and use at your own risk.

8.4 Governing Law and Arbitration

1M5 is a global mission not an effort specific to any jurisdiction. There will be no internal disputes as this is not an organization of any kind.