1M5

UNCENSORED COMMUNICATIONS

Invisible Matrix Services
White Paper

1 Loss of Privacy and the Rise of Censorship

When the Berlin wall was opened in November 1989, expectations of a more open human society sprang forward. Yet several decades later we are experiencing digital walls being raised by governments and large corporations in the name of protection. These walls promote segregation and censorship of information while having a negative effect on creativity, innovative technology, and freedom of speech, expression, association, and assembly.

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.

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.

Constraining the free flow of information between people is a direct threat to our freedom and censorship of communications on-line is growing world-wide.

- https://internetfreedomwatch.org/timeline/
- https://www.wired.com/2017/04/internet-censorship-is-advancing-under-trump/
- https://rsf.org/en/news/more-100-websites-blocked-growing-wave-online-censorship

On-line communications are censored at the point of entrance by Internet Service Providers (ISP).

They act as gateways to the internet providing governments control over speech by having the ability to restrict usage and track people's usage via their leased IP addresses. In order to make tracking usage much more difficult, tools have come out that provide techniques called onion-/garlic-routing where the source and destinations of internet routes can not be determined without breaking encryption, a very expensive feat, sometimes impossible today when considering the encryption algorithms used.

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

Privacy, the bedrock of freedom, is being lost at an alarming rate and few know how to maintain it today. Most large organizations (e.g. tech giants, the banking industry, governments) track, persist, and use our behavior for their profit not ours. Whistleblowers, the abused, visible 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 are difficult to maintain anonymity at the network layer. Smartphones, our primary means of global communication and collaboration, are weak in maintaining our anonymity and privacy - critical to ensuring individual freedom.

Two primary tools today that support this are Tor and I2P. Tor provides a browser that makes it easier to use while I2P is much less known. Both are complementary in that Tor was designed for browsing today's current web sites anonymously. 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 is one that completely circumvents ISPs by not using them. They're called direct wireless mesh networks and they can communicate directly phone-to-phone using technologies such as WiFi Direct. Firechat is an example used during the 2014 Hong Kong protests after the Chinese government threatened to shutdown the internet in that area. New mesh solutions are popping up including RightMesh that seek to improve on earlier designs. But the technology is still in its infancy and needs to be pulled into ever day applications more easily once they've matured.

Even getting these technologies in wide use doesn't solve the problem of online censorship. People in governments, corporations, and other thieves are constantly finding ways to circumvent these technologies to censor and steal information.

Tech-savvy people can always find a way to bypass censorship and maintain privacy, but the overwhelming majority can not thus preventing a critical mass to make positive change on a political level globally. What’s needed is to bring censorship resistance and data privacy to this overwhelming majority so that all people are not only able to become free, but that they can remain so.

2 Mission

1M5 is at its core a mission to ensure free speech, expression, association, and assembly. What's our core beliefs that drive us?

- EVERYONE, including criminals and unethical 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 - anonymity as a base
- Transparency in code/governance

- We own our data and should be the ones that profit from it
- Self-sovereign identity – people must establish and maintain their own identities, not by 3rd parties
- Self-sovereign money – people must be their own bank indebted to no one with the keys to their money

3 Objectives

What do we try to achieve?

- Supports sharing of information without being censored and without fear of being persecuted.
- Provides a self-sovereign identification system so that reputation can be established where necessary while the keys are owned and maintained by the individual.
- Support person-to-person/peer-to-peer (P2P) communication without the need to depend on servers nor the internet - The People’s Direct Meshnet - cut the cord to ISPs for good.
- When information about a user is desired from a 3rd party (e.g. marketer, government consensus),that information can be sold to the 3rd party by the owner yet with/without personally identifiable information (PII) being transferred by choice.
- Provide a platform that monetizes itself.

4 Solution

Provide a decentralized application platform that is fully open-source that requires anyone modifying it to also keep the modifications open source, both software and hardware, for decentralized applications that run without depending on servers sharing only what the owner specifically allows while also being created outside of manufacturers influenced by bad actors (e.g. open-source hardware / 3D printing) to ensure privacy while maintaining code and hardware transparency.

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 monetize itself by monetizing resources - network bandwidth, cpu cycles, and persistent storage - through the use of an internal coin to represent them. Donations are fine for getting the core on its feet, but long-term sustainability requires self-monetization.

The identification system will be reputation based to ensure privacy is maintained while allowing relaxation of privacy incrementally as desired as trust grows.

The internet was not designed for anonymity, it must be baked into the system from the beginning at the lowest of levels to ensure it can be provided under all circumstances.

4.1 Revenue

The core network monetizes people's hardware resources (network, cpu, storage) and users’ personal information, all on a voluntary basis. Coins are used in this network to keep track of usage, just like a utility provider does today except its ours. End users can offer their resources for coins to others who desire additional resources on-demand or scheduled in the future. They can also purchase coins in the applications to receive additional resources on-demand or scheduled in the future. All transactions incur a transaction fee to fund development and maintenance of the system and reward investment. It’s desired to reduce this fee to the lowest possible in the future. Initially it will be 0.5%.

4.2 Revenue Distribution

Distributions are offered in two forms: user and development.

User Coins - Prana: These are unlimited but based on end users' resources brought to the network. They will be provided by the internal application network. Prana utility coins are distributed in real-time. Prana coins may be sold during crowdsales.

Development Coins - Aten: These are also unlimited but issued to developers and anyone needed to support the application network. Percent ownership of Aten coins out of total outstanding Aten coins determines percent of the distributions from the transaction fees. Transaction fees are paid in Prana and distributed in real-time. Aten coins may be sold during crowdsales.

Note: Coins will never be just added to the system arbitrarily producing intentional inflation.

4.3 Expenditures

Funds from revenues (0.5% of revenue) are expended to build and maintain the system including its core partners and reward Aten coin holders.

- **10%** (0.05% of revenue): Auto distribution to Aten holders.
- **20%** (0.10% of revenue): Auto distribution to Basic Income: Admin / Monitor / PR / Maintenance. Initially each member is granted $2500 USD worth of Bitcoin monthly or another suitable stable currency as measurement. Left over funds are allocated based on consensus by admin staff. Admin staff selected by foundational partners but eventually through consensus by Aten holders. Changes to Basic Income as a percentage of expenditures requires unanimous vote by foundational partners but eventually through consensus by Aten holders.
- **70%** (0.35% of revenue): Distribution determined by consensus among Aten holders; if no consensus made within a rolling 30 day schedule, accumulated distributions are sent on each 1st to development account for new development.

4.4 Accounts

Funds are managed through smart contracts on Komodo with the following hard-coded accounts:

- Aten Holders: direct to KMD Aten Holder accounts
- Basic Income: to KMD account then to KMD Basic Income accounts
- Development: KMD account for paying out development and maintenance bounties

4.5 Context

1M5 works to provide private uncensorable communications as a base layer for decentralized applications far and above anything in the marketplace.

4.6 Platform

The platform consists of the components required to provide I/O, security, and consensus in support of its censorship resistance routing service. This is performed by a core bus combined with a core set of services each focusing on a different responsibility.

4.6.1 Censorship Resistance Routing

The first layer in a secure highly network-based application must be a layer supporting anonymity. This is accomplished by 1M5 by using I2P, Invisible Internet Project, as the basis for routing over the internet, direct mesh networks like 1DM 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. Garlic routing 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).
- **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.
- **1DM**: a direct mesh network as a sensor managing WiFi-Direct and Bluetooth sensors to provide private communications outside of the internet.
- **Peer Graph**: the Neo4J Sensor Manager manages these sensors along with their known peers in a graph to battle censorship re-routing messages as needed across the 1M5 network by all its means.

4.6.2 Orchestration

This component provides application orchestration through simple content-based routing (CBR) with support for Enterprise Application Integration (EAI) pattern routing as the code base grows. Current routing uses by default a Dynamic Routing Slip implemented as a stack.

4.6.3 Consensus

Nothing has been proven more secure than Bitcoin’s POW consensus. But it doesn’t support creating new coins that can be used in applications for utility. Komodo works with Bitcoin to build onto it providing this gap. 1M5 interfaces with both Komodo and Bitcoin to monetize end users’ resources.

4.6.4 Key Ring

Encryption and Signing keys kept safe on specialized flash drives where once added they can not be read nor changed. Encryption and signing happens on-drive only. OpenPGP used for standards support.

4.6.5 Prana – User Coins

Unlimited coins for platform to monetize network bandwidth, cpu cycles, and storage. They are minted on-the-fly to be used to manage resources provided. To receive Prana, applications make known what resources they are offering to the network as providers. When those resources are used by a peer application as a consumer, Prana coins are transferred from the consumer to the provider.

4.6.6 Aten – Distribution Coins

Unlimited coins for determining transaction fee distribution for ongoing marketing, development and maintenance. By default, 90% of revenue goes back into the application either to marketing, development, and maintenance or as gifts to those in need or for reducing transaction prices and 10% of revenue goes to Aten coin holders for distribution.

4.6.7 Basic Income

Prana coins given to administrative staff to secure a base level of income.

4.6.8 Decentralized Exchange

When Prana and Aten coins are desired to be exchanged for Bitcoin or other cryptocurrencies, the Komodo DEX can be used.

4.6.9 DID - Decentralized IDentifier

Self-Sovereign Identity, RepBAC (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.

Requirements

- Identity through Correlation
  - https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/final-documents/identity-crisis.pdf
- Reputation Based Access Control (RepBAC)
- Key Management
  - Double Ratcheting: https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm
- Identity Recovery
  - Private key sharded, duplicated, & encrypted with random peer disbursement; 12 words used to rebuild key

Self-Sovereign Identity

Reputation Based Access Control (RepBAC)
Not to be confused with Role-Based Access Control (RBAC)...

Circles of Influence

4.6.10 Info-Vault

Keeps personal information confidential and available.

5 Community

This is a community led mission driven by privacy and censorship-resistance needs of the community. Community members are either donating or prospecting. Donating members provide enough Bitcoin donations to support at least one individual. Prospecting members are supportive of the mission and recognize the need to be part of the community but have yet been able to provide donations. Donating members' needs are prioritized over prospecting members. Every new member starts as a Prospecting member until foundation members unanimously approve their membership to donating. We do this in an attempt to maintain a strong long-term stable community with shared support for the mission.

5.1 Donating

- Inkrypt (https://inkrypt.io): The Private and Censorship-Resistant Decentralized Content Distribution Network

5.2 Prospecting

- Purism (https://puri.sm): Open source hardware running open source software you can trust.

- Cloudivus (https://www.youtube.com/watch?v=Nvg2S2ngsXE): decentralizing the data center by offering hardware ownership and resultant revenue directly to individual hardware owners.

6 FAQ

7 Legal

The following general information applies to this document.

7.1 General

This effort is structured as a decentralized autonomous mission and as such is 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. Therefore, no one individual can represent 1M5 just as no one person represents that natural right.

7.2 Knowledge Required

To be an active member of this mission requires understanding of how it operates.

7.3 Risks

Decentralized autonomous missions are new efforts having no state supporting them and therefore none of the protections that come along with registering with a state. Each jurisdiction may come up with laws on dealing with these missions or similar efforts in the future. It is the responsibility of each member to handle these relationships as they see best to protect themselves and their families.

7.4 Representation and Warranties

No warranties are offered and no one person can represent this mission.

7.5 Governing Law and Arbitration

All internal disputes shall be resolved within the mission through arbitration agreed to by all parties involved. External issues are to be dealt with by the mission as a whole through consensus.