White Paper

1 Censorship

Freedom of Speech - 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 - 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.

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 thatarea. 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.

In addition:

- Most organizations today (e.g. Tech, Banks, Governments, Hospitals) track, persist, and use our behavior for their profit not ours.
- Centralized organizations are major targets for theft.
- Closed source software can easily contain hidden back doors for thieves to access our information without our knowledge and many open source applications have closed source libraries embedded in them.
- 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.
- Blockchain based applications and cryptocurrencies like Bitcoin are helping to wrestle some control from centralized organizations although they are largely used on servers and distributed ledgers are still logically centralized and difficult to maintain anonymity at the network layer.
- Smartphone ownership around the world is greater than PC ownership.
- Smartphones, our primary means of global communication and collaboration, are weak in maintaining our anonymity and privacy - critical to ensuring individual freedom.

2 Solution

1M5 works to solve these issues by providing an intelligent router embedding Tor, I2P, Direct Wireless Mesh, and other networks, using them intelligently as one dynamic network, and providing easy to use APIs for developers to embed in their applications. In addition, it provides access to commonly desired decentralized services in an anonymous fashion including self-sovereign identities, IPFS, Ethereum, GitHub, and others in the future making integration a snap.

3 Mission

What's our core beliefs that drive us?

- All relationships should 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

4 Objectives

What do we try to achieve?

- Support sharing of information without being censored and without fear of being persecuted.
- Support mobile-to-mobile (M2M) communication without the need to depend on servers.
- When information about a user is desired from a 3rd party (e.g. marketer, government consensus, your doctor),that information can be given or sold to the 3rd party by the owner yet with/without personally identifiable information (PII) being transferred by choice.
- Provides an identification system so that reputation can be established where desired.
- Provide a platform that monetizes itself internally.
- Anonymity is baked in as a base layer for all communications; identity and reputation can be built on top voluntarily as desired by end users – just like off-line.
- Internet not required - The People's Meshnet - cut the cord to ISPs for good.

5 Solution

Provide a mobile platform that is fully open-source in the public domain, both software and hardware, supporting decentralized applications that run purely on mobile phones 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 mobiles. If a user loses their phone, their new phone will be able to restore itself with no loss of data.

Ensure the platform can monetize itself by monetizing mobile resources - network bandwidth, cpu cycles, and persistent storage - through the use of a utility token to represent them.

Support executing contracts written in natural languages with no need for 3rd parties while maintaining privacy.

A decentralized content distribution platform will be provided to support freedom of information.

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. Anonymity must be baked into the system from the beginning at the lowest of levels. Without the ability to provide anonymity, it can not be provided under any circumstance. When anonymity is supported, rules can be put in place to govern it.

5.1 Revenue

The mobile app network monetizes people's phone resources (network, cpu, storage) and users' personal information, all on a voluntary basis. Tokens 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 tokens to others who desire additional resources on-demand or scheduled in the future. They can also purchase tokens on the system to receive additional resources on-demand or scheduled in the future. All transactions incur a 0.5% transaction fee to fund development and maintenance of the system. It's desired to reduce this fee to the lowest possible in the future.

5.2 Fundraising

Crowdsale purchasers may buy Prana and Aten tokens at a discount to help fund system development if/when crowdsales have been approved by the organization.

5.3 Token Distribution

Utility tokens are offered to end users using the system and developers for developing and maintaining it.

End User Utility Tokens - Prana: These are unlimited and based on end users' resources brought to the network. They will be provided by the internal application network. Prana utility tokens are distributed in real-time. The price of each mobile's resources is set by the end user. Resources are automatically selected based on lowest cost unless configured differently (e.g. lowest latency or combined factors).

Developer Utility Tokens - Aten: These are unlimited and issued to developers and anyone needed to support the application network. Percent ownership of Aten tokens out of total outstanding Aten tokens determines percent of the distributions from the transaction fees. Transaction fees are paid in Prana and distributed in real-time using auto-contracts. Aten tokens can be sold during crowdsales.

5.4 Expenditures

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

- 40-90%: Development / Maintenance Bounties
- 0-40%: Partners (I2P, Guardian Project, Cellular Privacy, RightMesh, etc)
- 0-10%: Operations (Admin / Monitor / PR)
- 10% (fixed): Aten Holders

As decision making is moved to a decentralized method implemented through auto-contracts, budgeting for Operations, Partners, and Dev/Maintenance Bounties will be performed through its process.

5.5 Accounts

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

- Bounty: ETH account for paying out development and maintenance bounties
- Partners: ETH account for supporting partnerships
- Operations: ETH account for paying out operational support
- Foundation: ETH account for distributing profits to Aten holders

5.6 Context

1M5 provides intelligent routing services for social, health, and governance android/java solutions while integrating with pluggable networks including I2P, I2P Bote, Tor, and Mesh networks to ensure a base layer of anonymity with encrypted communication and persistence. Additional pluggable services are expected to be supported such as consensus.

5.7 Core

The core consists of the components required to provide the functionality necessary to fulfill its mission.

5.7.1 Sensors

The first layer in a secure highly network-based application must be a layer supporting anonymity. For mobiles, this is a difficult proposition as people almost always have their mobile phones on or near them and register with cellular vendors losing any possible chance at anonymity. What's needed is a method to use these mobile phones without the need to register with 3rd parties in the long term, that is a mesh network, while in the short term using encrypted routing schemes to maintain IP privacy. This can be accomplished using I2P, Invisible Internet Project, as the basis for routing over the internet and mesh networks between I2P nodes and Tor Project for communicating with non-anonymous nodes in the clearnet like Amazon's AWS AI service. Additional sensors:

- **Aggression:**
- **Bluetooth**:
- **Bluetooth Low Energy:**
- **Cellular**:
- **Cleaners**:
- **Csploit**:
- **HAM**:
- **Honeypot**:
- **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).
- **IMSI**:
- **Mesh:**
- **Nearby:**
- **NFC**:
- **Redtooth**:
- **Rooting**:
- **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.
- **WiFiAware**:
- **WiFiDirect**:
- **WiFiHaLow:**

- **WiFiInternet**:

Further notes:

- Event I/O including all network plumbing and logic.
- Network Aware + DHT + UDP + Threat Mitigation.
- The system survives even if the internet goes down or is cut off falling back to peer-to-peer mesh networks to stay alive. As long as enough people still have their device, the network survives.
- An overlay network, it uses a modified Kademlia networking protocol (I2P)
- reputation system built in
- threat mitigation including IMSI-Catcher, Silent SMS, Silent/Spy Call detection and blocking.
- The system participates with the LID module automatically flagging misbehaving mobiles limiting them for bad behavior, logging all its actions to its recall memory.
- Continued bad behavior (reputation falls below a threshold) sees mobiles removed from the network.
- Decentralized DNS entries are replicated with DHT
- End-to-end encrypts/decrypts all network traffic
- Garlic/Onion routing for anonymity and traffic surveillance circumvention

5.7.2 Bus

The service bus is the asynchronous service router for 1M5 routing to/from sensors and services. It uses an asynchronous message channel backed by a blocking queue (persistent to come) and a configurable working thread pool to help throttle cpu usage. Services can be registered with the service bus supporting pluggable service providers.

5.7.3 Orchestration

This component provides intelligent service orchestration. Initially it will provide simple content-based routing (CBR) based on Envelope header information but is expected to take on full Enterprise Application Integration (EAI) pattern routing as the code base grows and APIs become more demanding.

5.7.4 Consensus

Using Prana Tokens across the network needs to be done in a method that prevents double spending of those tokens. Considering mobiles are not nearly as powerful as ASICs, POW algorithms can not be supported. Initially consensus will be performed by Ethereum. Long-term, consensus will be performed by an appropriate algorithm for mobiles.

- Unpermissioned blockchain on Android.
- Requires a DID.
- Prevent double spend.
- Randomly chosen validators.

5.7.5 Key Ring

Encryption and Signing keys kept safe in your mobile with transfers to/from cold storage.

5.7.6 Prana – End User Utility Token

Unlimited utility tokens for platform to monetize network bandwidth, cpu cycles, and storage. They are minted on-the-fly to be used to track resources provided.

Sensitivity: Mobile P2P challenge will be bandwidth, memory, hard drive, and battery. Hard to convince people to run on phone if it impacts those items to the point it noticeably degrades user experience.

- Phones will be able to support 1TB SSD External Storage soon.
- They have dual quad CPUs with hyperthreading now.
- Ram is moving up to 6GB now. They're as powerful as some laptops.
- Take 10B+ mobile phones as a collective. How much CPU and memory is that?
- Bandwidth definitely a serious factor but workable especially as networks improve and mesh becomes more of a reality.
- Definitely need to favorably weight phones within a high-bandwidth network.
- Battery life can be maximized by preferring processing loads when the phone is charging.
- Definitely place throttles on everything to ensure a good end-user experience.
- Phone resource usage will be voluntary and controlled by end user.
- Excess phone resource usage will be compensated with a utility token while usage of the network beyond an end user's phone capacity will result in utility token decrements (funding) kind of like having solar power on your house while plugged into the electric grid.
- Will provide a Foreground Service with Notification Bar while phone being used as processing service showing Prana balance going up.
- Prana Service will provide scheduling.
- Prana Service can be stopped any time manually.
- Prana Service can auto start/stop dependent on start charging/stop charging events.

5.7.7 Aten – Development Utility Tokens

Unlimited tokens for determining transaction fee distribution for ongoing marketing, development and maintenance. By default, 90% of profit 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 profit goes to Aten token holders for distribution. Eventually it is expected that this ratio will be voted on as there may be times where more resources may be needed for marketing, development, and other activities and other times less.

5.7.8 Universal Basic Income

Prana tokens rewarded for helping secure the system from double spend through random selection.

5.7.9 DEX – Decentralized Exchange

Ability to exchange tokens directly mobile-to-mobile or mobile-to/from-external blockchain.

5.7.10 DID - Decentralized IDentifier

Self-Sovereign Identity, RepBAC (Reputation Based Access Control), and Circles of Influence. Anyone can get on by creating a DID, but are severely restricted in what they can do until their reputation improves. As it does, their access will too. If it falls, so does their access.

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 & encrypted with random peer disbursement and replication
- Transaction Freezes
- Passing Down Tokens To Heirs – Will Contracts?

Self-Sovereign Identity

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

Circles of Influence

5.7.11 Repository

Access and manage code repositories such as Github to support software development bounties by contract.

5.7.12 Content

Full-stack synched decentralized javascript web applications on android for decentralized content distribution.

5.7.13 Info-Vault

Keeps personal information confidential and available.

5.7.14 Contract

Think Ethereum turing-complete platform on a mobile using OpenDocuments for the contract

language and a Rete rules engine for execution. Self-executing self-enforcing software implemented contracts intended to facilitate, verify, or enforce the negotiation or performance of contracts providing security that is superior to traditional contract law while greatly reducing transaction costs.

5.8 APIs

5.8.1 Social

Decentralized Social Media Android Apps – Dgramz.io

5.8.2 Governance

Decentralized governance – V4D.io

5.8.3 Gifting

Giving Decentralized Android Apps – Give4.me

5.8.4 Market

Free and open marketplace – 460R4.io

5.8.5 Content Distribution

P2P Mobile Web on Mesh

5.8.6 Health

Decentralized health – Dragonsbane.io

5.8.7 Escrow

When a 3rd party is desired.

6 Product Roadmap

This is a large long-term endeavor to ensure people are empowered in the evolving online community. In order to accomplish this, many components are required to form a platform to enable that mission with some components depending on others to work first. Considering this is such a large and long-term endeavor, we can't build everything in a big-bang and boil-the-ocean approach. We will think more Kaizen starting with smaller and easier products to flush out the minimal infrastructure then work out the infrastructure by continuing to build additional products.

Those who contribute to the core and apis will be rewarded in Aten tokens and/or Ether. Aten bounties are derived by difficulty modifiers multiplied by hours expected and are provided as estimates. The modifiers are as follows:

0-Intern, 1-Junior, 3-Mid, 6-Senior, 10-Principal, 20-Legion

Assuming 2000 hours/year working in software development, each modifier should correspond to these yearly ranges:

Intern [0-1], Junior [1-5], Mid [3-12], Senior [10-25], Principal [18-40], Legion [30-60]

They should be applied based on strength in general but also at the task at hand. Legions are extremely rare developers who can design and build the most complex of software designs having a massive toolbox of experience and tooling to come up with extremely innovative software. They tend to be extremely productive in both design and coding.

Current contributors and their Aten balances follow:

Software Developers [Mod:Aten Awarded]:

- Brian Taylor [P:18,480] objectorange@protonmail.com (2017 new codebase reset, had 58k+)
- Gerald Rama [J:12] geraldrama@gmail.com
- Theresa Augustin [J:10] taaugustin@gmail.com

Organizational Developers:

- Daniel Jeffries [1,000] danj737-linkedin@yahoo.com
- Howard Wetsman [400] howard@tocdr.com
- Carsten Munk [200] carsten.munk@gmail.com

Products desired and ordered by preference are: Social, Health, Gifting, Governance, Market, Content, Escrow. These are general applications to drive the 1M5 design and implementation to ensure it is meeting marketplace needs.

6.1 Schedule & General Funding

- **Social 1.0**: 2017-2018 – Dgramz 1.0 1k ETH, WAM Social 1k ETH
- **Health 1.0**: 2018-2019 – Dragonsbane Neurocog 1k ETH, WAM Dr 1k ETH
- **Gifting 1.0**: ? – Giv4.me 1k ETH
- **Governance 1.0**: ? – V4D.io 5k ETH, Cultu.re 5k ETH
- **Market 1.0**: ? – 460R4.io 5k ETH
- **Content Distribution 1.0**: ? 1k ETH
- **Escrow 1.0**: ? – Onessus 1k ETH
- **AGI 1.0**: 2018 – 2028 50k ETH

6.2 Social

Social Media 3.0 - Decentralized with end-to-end double-ratchet encrypted messaging. Like Signal yet no servers required, totally open sourced on GitHub, and ran over anonymous I2P/Tor/Mesh networks.

Minimal functionality to prove out 1.0 platform idea. Estimated ~2k person hours, 15.6k Aten dev bounties.

6.2.1 1M5

- **Whitepaper**
- **Architecture Documentation**
- **App**
- **Data**
- **Sensors**
    - I2P
    - Cellular
    - WifiInternet
- **Decentralied IDentifier (DID)**
    - Crypto Authentication
- **Prana**
- **Aten**
- **Key Ring**

6.3 Health

Partnering with Dragonsbane. Interests are a cure for addiction.

6.3.1 1M5

- **Health UI**
    - ?
- **Synaptic Celerity**
    - Impairment Testing
    - DAG? + Rete? + Min Neuro-Evolution?
    - ~ 1000 Principal hours
    - ~ 10k Aten Bounty Total

6.3.2 Features

6.4 Gifting

A marketplace of love where people can put out there what their needs are, people within their circles of influence can rate how much they need it, supporting people giving freely by need.

6.4.1 1M5

- **Sensors**

    - Mesh
    - ~ 1000 Senior Hours
    - ~ 6k Aten Bounty Total
- **Synaptic Celerity – Recall**
    - NoSQL Columnar Database as a layer over P2P Network
    - ~ 2000 Senior Hours
    - ~ 12k Aten Bounty Total
- **Consensus**
    - Permissioned by the end users' DID, decentralized, and sharded using NoSQL DB
    - ~ 2000 Senior Hours
    - ~ 12k Aten Bounty Total

6.4.2 Features

6.5 Governance - V4d

Provide the means to support a voluntary, decentralized, delegatable, direct, democracy allowing any and all individuals to initiate Bills and build consensus around them from grassroots outwards.

6.5.1 1M5

- **Auto Contract**
    - OpenDocuments https://www.openoffice.org/
    - OpenDocument DSL XML-to-PMML XSLT https://en.wikipedia.org/wiki/XSLT
    - Drools Rules Engine Integration https://www.drools.org/
    - ~ 1000 Senior hours
    - ~ 6k Aten Bounty Total

6.5.2 Features

- **V4d – Voluntary Decentralized Delegative Direct Democracy**
    - Smart Contracts + Mobile App
    - ~ 2000 Mid hours
    - ~ 6k Aten Bounty Total

6.6 Market

Provide a free and open marketplace, an Agora, secured by LID based reputations.

6.6.1 Platform

- **Recall**
    - Graph Database as a layer over NoSQL Columnar Database
    - ~ 2000 Senior Hours
    - ~ 12k Syn Bounty Total
- **Info Vault**
    - Personal Information Management
    - ~ 500 Senior Hours
    - ~ 12k Syn Bounty Total

6.6.2 Features

6.7 Content Distribution

Move web servers onto mobile phones and distribute and decentralize all web content.

6.7.1 Platform

- **Content**
    - Web 3.0
    - ~ 1000 Senior Hours
    - ~ 6k Syn Bounty Total

6.7.2 Features

6.8 Escrow

Considering partnering with Onessus who, as of 4th Qtr 2017, is fundraising. Will contact in 1st Qtr 2018 to see if funding was achieved. Expect to support them in their 2.0 or 3.0 version. Their 1.0 will use Ethereum.

6.8.1 1M5

6.8.2 Features

7 FAQ

8 Community

The team behind 1M5 is growing starting from its founder. We will work to keep it as small as possible to ensure minimal overhead in building the platform. To do that, the community will be compensated in Aten and/or a preferred cryptocurrency.

8.1 Development

Founder – Brian Taylor

INTJ/INTP/INFJ/INFP with over 20 years developing software, most as a Software Architect, from bootstrapped startups to Fortune 100 enterprises, specializing in distributed computing, scalability, and real-time analytics, focusing on decentralizing and open sourcing all aspects of computing promoting voluntary and transparent relationships while maintaining personal privacy moving towards a publicly owned global personal ASI assistance.

8.2 Partners

8.2.1 Dragonsbane

Healthcare AI for everyone. Starting with Neurocog, a workplace impairment testing app to replace ineffective and privacy intrusive workplace drug testing.

8.2.2 I2P

Bote – P2P store-and-forward messaging using garlic routing with end-to-end quantum resistant encryption by default.

8.2.3 Tor

Onion routing with end-to-end encryption by default used when interacting with non-anonymous sites such as Amazon Web Services (AWS).

8.2.4 Guardian Project

Orbot embedded for using Tor.

8.2.5 Cellular Privacy

IMSI-Catcher, Silent SMS guarding...

8.2.6 Cybernetic Development Center

Android cleaner service, wireless mesh service, nearby service.
https://www.linkedin.com/in/murdoch-pizgatti-51886150/

8.2.7 Onessus

Decentralized escrow.

8.2.8 RightMatrix

Mesh networking. Investigative for now until open-sourced.

9 Accountability

The organization must always be transparent with all members. So, it will make sure that all parties are informed on revenue received, profit distributed, funds raised, and expenses.

Therefore, an Organization Report will always be available that will include information regarding how contributed money towards the development of the organization and its technologies.

The information will be delivered to its members through its Android app.

10 Legal

The following general information applies to this document.

10.1 General

This organization is structured as a decentralized autonomous organization and as such is not registered in any jurisdiction.

10.2 Knowledge Required

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

10.3 Risks

Decentralized autonomous organizations are a new organizational structure 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 DAOs in the future. It is the responsibility of each member to handle these relationships in their jurisdiction. The organization will work to help each member in doing so as it grows.

10.4 Representation and Warranties

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

10.5 Governing Law and Arbitration

All internal disputes and controversy shall be resolved within the organization through arbitration agreed to by all parties involved. External issues are to be dealt with by the organization through unanimous membership approval.