



## **SYNAPTIC CELERITY**

AI Assistance for Humanity  
White Paper

### **1 Loss of Privacy and the Rise of AI**

The world is changing technologically at an ever increasing pace resulting in much change in how we live. Privacy, the bedrock of freedom, is being lost at an alarming rate and few know how to maintain it today. AI, perhaps after taking much of our jobs, might become a threat to our lives. How can we enjoy what new technologies have to offer yet maintain our privacy and use AI to assist humanity, not for it to become a threat?

- Most businesses (e.g. Facebook, Google, Microsoft, the banking industry) 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.
- Artificial Intelligence (AI) is dramatically enhancing our experiences resulting in profits windfalls to investors at the cost of many low skilled jobs (~80% of the job market).
- AI is considered by some to be a potential threat to humanity on the horizon.
- 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 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
- We should be able to use AI for assistance without being threatened by it

## 3 Objectives

What do we try to achieve?

- Provide the means to use mobile phones as an AI assistant where the end user can opt-in and opt-out of AI services without worrying about losing their privacy or being threatened.
- When information about a user is desired from a 3<sup>rd</sup> party (e.g. marketer, government consensus), that information can be sold to the 3<sup>rd</sup> party by the owner yet with/without personally identifiable information (PII) being transferred by choice.
- Provide a platform that monetizes itself internally.
- Support executing contracts with no need for 3rd parties while maintaining privacy.
- Supports sharing of information without being censored and without fear of being persecuted.
- Provides an identification system so that reputation can be established where necessary.
- Support mobile-to-mobile (M2M) communication without the need to depend on servers nor the internet - The People's Meshnet - cut the cord to ISPs for good.

## 4 Solution

Provide a mobile platform that is fully open-source that requires anyone modifying it to also keep the modifications open source, both software and hardware, and 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 supporting greater collective artificial intelligence as assistance to individuals.

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.

## **4.1 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.

## **4.2 Fundraising**

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

## **4.3 Token Distribution**

Tokens are offered in two forms: utility and foundation.

**Utility Tokens - Amino:** These are unlimited and based on end users' resources brought to the network. They will be provided by the internal application network. Amino 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.

**Foundation Tokens - Syn:** These are limited and issued to developers and anyone needed to support the application network. Percent ownership of Foundation tokens out of total outstanding Foundation tokens determines percent of the distributions from the transaction fees. A total of 1,000,000 (one million) Syn tokens will be issued with 18 decimal places. Transaction fees are paid in Amino and distributed in real-time using auto-contracts. Syn tokens can be sold during crowdsales.

## **4.4 Expenditures**

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

- 70%: Development / Maintenance Bounties
- 10%: Foundational Partners (I2P, Guardian Project, Cellular Privacy, etc)
- 10%: Operations (Admin / Monitor / PR)
- 10%: Syn Holders

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

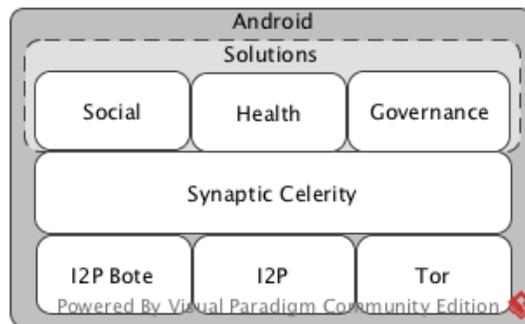
## 4.5 Accounts

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 foundational partnerships
- Operations: ETH account for paying out operational support
- Foundation: ETH account for distributing profits to Syn holders

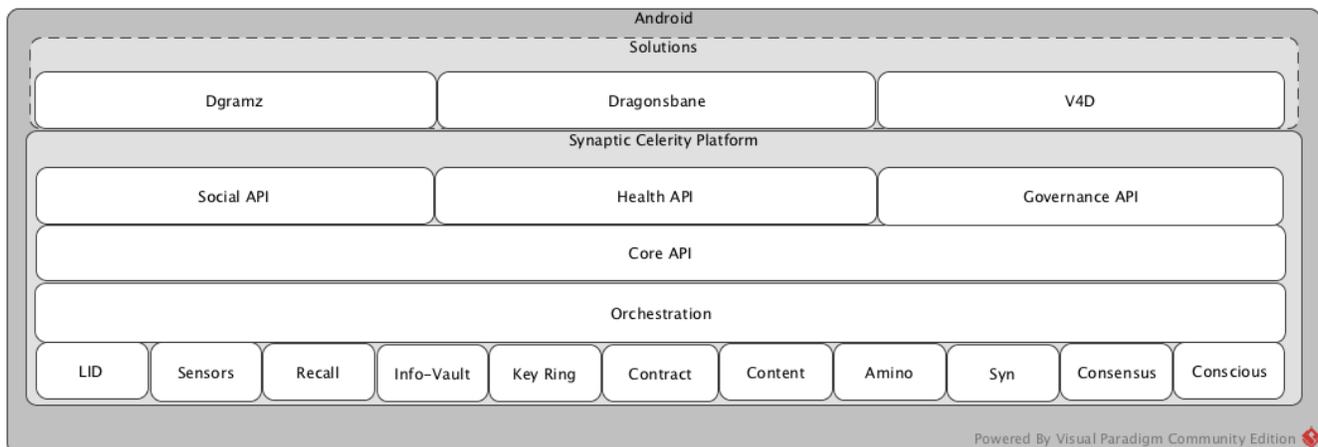
## 4.6 Context

Synaptic Celerity provides intelligence services for social, health, and governance android solutions while integrating with pluggable networks including I2P, I2P Bote, and Tor to ensure a base layer of anonymity with encrypted communication and persistence.



## 4.7 Platform

The platform consists of the components required to provide I/O, security, and consensus in support of its intelligence service (Conscious). This is performed through a set of APIs each focusing on a different business area, e.g. social, health, and governance.



## 4.7.1 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:

- **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:**
- **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:**
- **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 Kademia 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

## 4.7.2 Orchestration

This component provides application orchestration. Initially it will provide simple content-based routing (CBR) but is expected to take on full Enterprise Application Integration (EAI) pattern routing as the code base grows and especially when expected to be used as a platform.

## 4.7.3 Consensus

Using Amino 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 a POS algorithm that works for mobiles.

- Unpermissioned blockchain on Android.
- Requires a LID.
- Prevent double spend.

## 4.7.4 Key Ring

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

## 4.7.5 Amino - Utility Token

Limited 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 Amino balance going up.

- Amino Service can be stopped anytime by end user.
- Amino Service will provide scheduling.
- Amino Service can auto start/stop dependent on start charging/stop charging events.

#### **4.7.6 Syn - Foundation Tokens**

Limited tokens for determining transaction fee distribution for ongoing marketing, development and maintenance. One million tokens available. 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 Syn 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.

#### **4.7.7 Universal Basic Income**

Amino tokens rewarded for helping secure the system from double spend.

#### **4.7.8 LID - Life Identifier**

Self-Sovereign Identity, RepBAC (Reputation Based Access Control), and Circles of Influence. Anyone can get on by creating a LID, 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](https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm)
- Identity Recovery
  - Private key sharded & encrypted with random peer disbursement and replication
- Transaction Freezes
- Crime Recovery
  - Not sure about this
- Passing Down Tokens To Heirs

##### **Self-Sovereign Identity**

##### **Reputation Based Access Control (RepBAC)**

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

##### **Circles of Influence**

### **4.7.9 Content**

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

### **4.7.10 Conscious**

The nervous system of the platform and it's primary long-term service. Composed of Directed Acyclic Graphs (DAG) + Rete + Neuro-evolution - a form of machine learning that uses evolutionary algorithms to train artificial neural networks. It's expected to be driven long-term towards an AGI then ASI. The data shared is specific to an individual but it's shared across the collective membership in a privacy-maintaining method to derive a general intelligence to feed back into helping individuals specifically.

### **4.7.11 Recall**

Caching + graph + highly available/highly partition tolerant/tunable consistency persistence. Persisted data is automatically encrypted/decrypted using 256-bit AES encryption without needing the device to be rooted.

### **4.7.12 Info-Vault**

Keeps personal information confidential and available.

### **4.7.13 Contract**

Think Ethereum turing-complete platform on a mobile using OpenDocuments for the contract language and a Rete rules engine for execution. This supports using the Conscious service to truly make contracts 'smart'. 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.

## **4.8 Products**

### **4.8.1 Social**

Decentralized Social Media Android App.

### **4.8.2 Governance**

Voluntary Decentralized Delegative Direct Democracy Android App.

### **4.8.3 Gifting**

Giving Decentralized Android App.

### **4.8.4 Market**

Free and open marketplace - the Agora.

## 4.8.5 Content Distribution

P2P Mobile Web on Mesh - Internet 3.0.

## 4.8.6 Health

Maximum personalization of health and wellness for all individuals while ensuring privacy.

## 4.8.7 Escrow

When a 3rd party is desired.

# 5 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 platform and products will be rewarded from gifting accounts and/or in Syn. Syn 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 on a subject, each modifier should correspond to these 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 take on 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 Syn balances follow:

Software Developers [Mod:Syn Awarded]:

- Brian Taylor [P:15,680] [objectorange@protonmail.com](mailto:objectorange@protonmail.com) (2017 new codebase reset, had 58k+)
- Gerb Stralko [S:0] [gerb.stralko@gmail.com](mailto:gerb.stralko@gmail.com)
- Dirk Dorony [M:0] [dirk.dorony@gmail.com](mailto:dirk.dorony@gmail.com)
- Gerald Rama [J:8] [geraldrama@gmail.com](mailto:geraldrama@gmail.com)
- Theresa Augustin [J:8] [taaugustin@gmail.com](mailto:taaugustin@gmail.com)
- Srujitha Mullanpudi [M?:0] [srujitha.chowdry@gmail.com](mailto:srujitha.chowdry@gmail.com)
- Jeff Thomas [?:0] [aecend@gmail.com](mailto:aecend@gmail.com)
- Marilee Turscak [J:0] [marilee.turscak@gmail.com](mailto:marilee.turscak@gmail.com)

Organizational Developers:

- Daniel Jeffries [1,000] [danj737-linkedin@yahoo.com](mailto:danj737-linkedin@yahoo.com)
- Howard Wetsman [400] [howard@tocdr.com](mailto:howard@tocdr.com)

- Carsten Munk [200] [carsten.munk@gmail.com](mailto:carsten.munk@gmail.com)

Products desired and ordered by preference are: Social, Health, Gifting, Governance, Market, Content, Escrow.

## **5.1 Schedule & General Funding**

- **Social 1.0:** 2017-2018 – Dgramz 1.0 1k ETH
- **Health 1.0:** 2018-2019 – Dragonsbane Neurocog 1k ETH
- **Gifting 1.0:** ? – Giv4.me 1k ETH
- **Governance 1.0:** ? – V4D.io 5k ETH
- **Market 1.0:** ? 5k ETH
- **Content Distribution 1.0:** ? 1k ETH
- **Escrow 1.0:** 2018 – 2019 – Onessus 1k ETH
- **AGI 1.0:** 2017 – 2027 50k ETH

## **5.2 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 network.

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

### **5.2.1 Platform**

- **Whitepaper**
- **Architecture Documentation**
- **App**
- **Data**
- **Recall**
- **Sensors**
  - I2P
  - Cellular
  - WifiInternet
- **Life IDentifier (LID)**
  - Crypto Authentication
- **Amino**

- SYN
- Token Wallet

### 5.3 Health

Partnering with Dragonsbane who, as of 4th Qtr 2017, is writing their whitepaper. Monitoring their whitepaper. Interests are human fertility assistance (start 4th qtr 2017?), health monitoring & recommendations (start 4th qtr 2018?), and a cure for addiction (start 2nd qtr 2019?).

#### 5.3.1 Platform

- Health UI
  - ?
- Conscious
  - Impairment Testing
  - DAG? + Rete? + Min Neuro-Evolution?
  - ~ 1000 Principal hours
  - ~ 10k Syn Bounty Total

#### 5.3.2 Features

### 5.4 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.

#### 5.4.1 Platform

- Sensors
  - Mesh
  - ~ 1000 Senior Hours
  - ~ 6k Syn Bounty Total
- Recall
  - NoSQL Columnar Database as a layer over P2P Network
  - ~ 2000 Senior Hours
  - ~ 12k Syn Bounty Total
- Consensus
  - Permissioned by the end users' LID, decentralized, and sharded using NoSQL DB
  - ~ 2000 Senior Hours
  - ~ 12k Syn Bounty Total

## 5.4.2 Features

## 5.5 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.

### 5.5.1 Platform

- **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 Syn Bounty Total

### 5.5.2 Features

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

## 5.6 Market

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

### 5.6.1 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

### 5.6.2 Features

## 5.7 Content Distribution

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

## 5.7.1 Platform

- **Content**

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

## 5.7.2 Features

### 5.8 Escrow

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.

## 5.8.1 Platform

## 5.8.2 Features

## 6 FAQ

## 7 Community

The team behind Synaptic Celerity 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 Syn and/or a preferred cryptocurrency through gifting.

### 7.1 Foundation



#### Founder – Brian Taylor

---

INTJ/INTP/INFJ/INFP with 20 years developing software, 17 as a Software Architect, from bootstrapped startups to Fortune 100 enterprises, specializing in distributed computing, scalability, and real-time analytics, focusing on decentralizing and copyleft open sourcing all aspects of computing promoting voluntary and transparent relationships while maintaining personal privacy moving towards a publicly owned global personal ASI assistance.

### 7.2 Partners

#### 7.2.1 Dragonsbane

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

## **7.2.2 I2P**

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

## **7.2.3 Tor**

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

## **7.2.4 Guardian Project**

Orbot embedded for using Tor.

## **7.2.5 Cellular Privacy**

IMSI-Catcher, Silent SMS guarding...

## **7.2.6 Cybernetic Development Center**

Android cleaner service, wireless mesh service, nearby service.

<https://www.linkedin.com/in/murdoch-pizgatti-51886150/>

## **7.2.7 Onessus**

Decentralized escrow.

# **8 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.

# **9 Legal**

The following general information applies to this document.

## **9.1 General**

This organization is structured as a decentralized autonomous organization and as such is not confined to any jurisdiction.

## **9.2 Knowledge Required**

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

## **9.3 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.

#### ***9.4 Representation and Warranties***

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

#### ***9.5 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 as a whole through voting.