Dgramz

Open Private Communications for Humanity
White Paper

1 Loss of Privacy

The world is changing technologically at an ever increasing pace. Privacy, the bedrock of freedom, is being lost at an alarming rate and few know how to maintain it today. How can we enjoy communicating over long distances yet maintain our privacy?

- Most organizations (e.g. Facebook, Google, Apple, banks, governments) track, persist, and use our behavior for their gain.

- 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.

- Smart phones, our primary means of global communication and collaboration, are weak in maintaining our anonymity and privacy - critical to ensuring individual freedom.

- Many messaging applications exist but none have the means to ensure our privacy is maintained.

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

3 Objectives

What do we try to achieve?

- Supports 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),that information can be 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 necessary.

- Provide a platform that monetizes itself internally.

- Internet not required - The People's Meshnet - cut the cord to ISPs for good.

4 Solution

Provide a mobile messaging application that is fully open-source that requires anyone modifying it to also keep the modifications open source, both software and hardware, and without depending on servers sharing only what the owner specifically allows.

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.

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 monetizes people's phone resources (network, cpu, storage) on a voluntary basis. Tokens are used in this network to keep track of usage. Users can also purchase Amino tokens from Users with excess Amino tokens. Each User sets their price. All token exchanges 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 support up to 18 decimal places. They will be provided by the internal application network distributed in real-time. One token is received for each message relayed through the network (minus transaction fee) and one token per relayer is spent for each message sent through the network.

Foundation Tokens - Syn: These are limited and issued to early founders and anyone needed to bootstrap 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 and crowdsales 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.
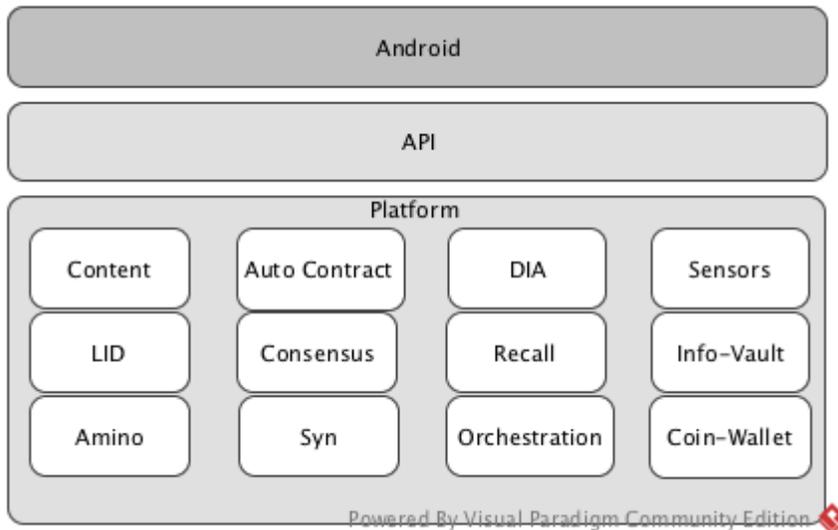
4.5 Accounts

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

- Bounty: ETH account for paying out development and maintenance bounties
- Foundation: ETH account for supporting foundational partnerships
- Operations: ETH account for paying out operational support
- Founders: ETH account for distributing profits to founders

4.6 Platform Components

The Synaptic Celerity platform provides application bootstrapping, environment awareness, configuration, and component integration. For Dgramz, the following components are used:

Diagram layers:
- Android
- API
- Platform
  - Content | Auto Contract | DIA | Sensors
  - LID | Consensus | Recall | Info-Vault
  - Amino | Syn | Orchestration | Coin-Wallet

Powered By Visual Paradigm Community Edition

4.6.1　　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.

- **Bluetooth**: 6.0
- **Bluetooth Low Energy:** 7.0
- **Cellular**: 1.0
- **HAM**: 5.0
- **I2P**: 1.0 – 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**: 3.0
- **Redtooth**: ?
- **Tor**: 2.0 – 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**: 4.0
- **WiFiDirect**: 4.0
- **WiFiInternet**: 1.0

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

4.6.2   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.

4.6.3   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/POS algorithms are not likely to be supported. Additional methods will need to be researched to determine the best technology including graphs.

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

4.6.4   Token Wallet

Token safe keeping in your mobile with transfers to/from cold storage.

4.6.5   Amino - 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 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.

4.6.6   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.

4.6.7   LID - Life IDentifier

Requirements
- Key Management
  - Double Ratcheting: https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm
- Identity Recovery
  - Private key sharded & encrypted with random peer disbursement and replication

Self-Sovereign Identity

4.6.8   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.

4.6.9 Info-Vault

Keeps personal information confidential and available.

4.6.10 Auto-Contract

Ethereum for now.

5 Development

Those who contribute to the platform and products will be rewarded from ETH accounts and/or in Syn with bounties. Current contributors and their Syn balances follow:

Software Developers [Mod:Syn Awarded]:

- Brian Taylor [P:10,310] objectorange@protonmail.com (2017 new codebase reset, had 58k+)
- Gerb Stralko [S:0] gerb.stralko@gmail.com
- Dirk Dorony [M:0] dirk.dorony@gmail.com
- Srujitha Mullapudi [M?:0] srujitha.chowdry@gmail.com
- Jeff Thomas [?:0] aecend@gmail.com
- Marilee Turscak [J:0] marilee.turscak@gmail.com

Advisors / Inspirers:

- Daniel Jeffries [1,000] danj737-linkedin@yahoo.com
- Carsten Munk [200] carsten.munk@gmail.com
- Howard Wetsman [0] howard@tocdr.com

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

6 Context

Synaptic Celerity, the platform for Dgramz, 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. Dgramz is the first such product.

7 Product Roadmap

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. Long-term functionality expected to evolve into full social media application for AI assistance.

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

7.1 Market Comparisons

Why build Dgramz? Aren't there plenty of mobile messaging applications on the market?

- Messaging
  - **Signal**
    - Pros
      - Double Ratchet Key Management
      - End-to-End Encryption
      - AGPLv3 Clients
      - GPLv3 Servers
      - On GitHub
      - Android Mobile App
      - Voice & Video Calls
    - Cons
      - Unable to find all source on GitHub
      - Clients have proprietary dependencies
      - Uses Servers
      - Not running on Anonymous Network
      - No Mesh Support
      - Uses cellular numbers for identification
    - Dgramz Differences
      - All source on GitHub
      - No proprietary dependencies
      - NO Servers used, only P2P
      - Anonymous Network (I2P)
      - Uses public keys with Alias for identification
      - Voice Messages → 2.0
      - Voice Calls → 3.0
      - Video Calls → 4.0
      - Mesh Support → 5.0
  - **Telegram**
    - Pros
      - Claimed Fastest on Market
      - End-to-End Encryption
      - Photo Editing
      - Clients are GPLv3
      - Supports Bots
      - Voice Messaging
      - Voice and Video Calls
    - Cons
      - Clients contain binary blobs
      - Uses Servers and those have proprietary license
      - Custom unproven security protocol
      - End-to-End Encryption not default
      - Messages stored on servers
      - Has Russian ties including devs in Russia
    - Dgramz Differences
      - Fully AGPLv3
      - NO Servers

- - - Full source on GitHub
    - End-to-End Encryption Always On
    - No Government ties
    - Proven security protocols
  - **I2P Messenger**
    - Pros
    - Cons
    - Transmit Differences
  - **FB Messenger**
    - Pros
      - Everyone and their mother is using it
    - Cons
      - FB owns your data
      - Little privacy
    - Dgramz Differences
      - You and only you own your data
      - Full Privacy
- VoiceMail
  - ?
- Email
  - ?

7.2 Features

- **Messaging**
  - List all open Conversations - 1.0
  - Start New Conversation - 1.0
  - Open Conversation - 1.0
    - Call Contact
    - Send Message to Conversation - 1.0
    - Add Picture to Conversation
    - Send Voice Recording to Conversation
    - Receive Message in Conversation - 1.0
    - Double tap Pic: View Pic larger
    - Long tap message shows menu: - 1.0
      - View Message/pic Details
      - Delete Message in Conversation - 1.0
      - Copy message/pic to clipboard - 1.0
      - Save Message/pic to storage
      - Forward Message to Contact
    - Menu – 1.0
      - Add Attachment to Conversation
      - View All Media with Contact
      - Conversation Settings
        - Mute Conversation
        - Notification Sound
        - Vibrate - Settings Default, Enabled, Disabled

- - - ○ Color for this Contact
    - ○ Block
  - ● Invite - 1.0
    - ● Mute Notifications - 1hr, 2hrs, 1 day, 7 days, 1 year
  - ○ Long tap Conversation shows Menu: - 1.0
    - ■ Archive Conversation
      - ● Undo
    - ■ Delete Conversation - 1.0
    - ■ Batch Select All Conversations
      - ● Archive
      - ● Delete
  - ○ Search Conversations by Contact
  - ○ Clear All Message History
  - ○ Invite Contacts - 1.0
  - ○ Import System SMS Database - 1.0
  - ○ Import Plaintext Backup - 1.0
  - ○ Export Plaintext Backup - 1.0
  - ○ View Settings - 1.0
    - ■ SMS and MMS
      - ● SMS Enabled
      - ● SMS Delivery Reports
      - ● 'WiFi Calling' compatibility mode
    - ■ Notifications - 1.0
      - ● Messages - 1.0
        - ○ Notifications - Off/*On* - 1.0
        - ○ Default ringtone
        - ○ Vibrate - Off/*On*
        - ○ LED Color
        - ○ LED Blink Pattern
          - ■ Fast, *Normal*, Slow
          - ■ Custom - On For, Off For
        - ○ In-Chat Sounds
        - ○ Repeat Alerts
          - ■ Never, One Time, Two Times, Three Times, Five Times, Ten Times
        - ○ Show
          - ■ Name and Message
          - ■ Name Only
          - ■ No Name or Message
        - ○ Priority
          - ■ Default, High, Max
      - ● Events
        - ○ Contact joined SC Messenger
    - ■ Privacy - 1.0
      - ● App Access - 1.0
        - ○ Enable Passphrase - 1.0
          - ■ Enter & Re-Enter Passphrase - 1.0
        - ○ Change Passphrase - 1.0
          - ■ Enter Current, New, and Re-Enter New Passphrase - 1.0

- - - ○ Screen Security
  - ● Communication
    - ○ Blocked Contacts
  - ■ Appearance – 1.0
    - ● Theme – 1.0
      - ○ Light, *Dark* - 1.0
    - ● Language
      - ○ *Default* - 1.0, *English* - 1.0, Arabic, Bulgarian, Catalon, Chinese Cantonese, Chinese Mandarin, Deutsch, Spanish, French, Greek, Hebrew, Indonesia, Italian, Japanese, Korean, Portugese, Russian, Serbian, Slovenian, Turkish, Vietnamese
  - ■ Chats & Media
    - ● Media Auto-Download
      - ○ When using Mobile Data
        - ■ *Images*, *Audio*, Video, Documents
      - ○ When using WiFi
        - ■ *Images*, *Audio*, *Video*, *Documents*
      - ○ When roaming
        - ■ Images, Audio, Video, Documents
      - ○ When using I2P
        - ■ Images, Audio, Video, Documents
      - ○ When on Mesh
        - ■ Images, Audio, Video, Documents
    - ● Chats
      - ○ Message Font Size
        - ■ Small, *Normal*, Large, Extra Large
      - ○ Show Invitation Prompts - *On*/Off
      - ○ Use system emoji - On/*Off*
      - ○ Enter key sends - On/*Off*
    - ● Message Trimming
      - ○ Delete Old Messages - On/*Off*
      - ○ Conversation Length Limit
      - ○ Trim all conversations now
  - ■ Linked Devices
    - ● List Linked Devices
    - ● Link Device
  - ■ Advanced
    - ● Submit debug log (View & Edit)
      - ○ Submit Log
- ○ Bots API
- ○ ~ x Mid Hours
  - ~ y Syn Bounty

7.3 Components

- **Whitepaper**

- ○ ~ 200 Principal Hours
- ○ ~ 2k Syn Bounty Total
- ○ **In Progress - Brian Taylor**
- **Architecture Documentation**
  - ○ ~ 200 Principal Hours
  - ○ ~ 2k Syn Bounty Total
  - ○ **In Progress - Brian Taylor**
- **App**
  - ○ Bootstrapping
  - ○ Environment Driven Configuration
  - ○ ~ 500 Mid Hours
  - ○ ~ 1.5k Syn Bounty Total
  - ○ **In Progress - Brian Taylor**
- **Data**
  - ○ Entities
  - ○ ~ 100 Junior Hours
  - ○ ~ 100 Syn Bounty Total
  - ○ **In Progress - Brian Taylor**
- **Recall**
  - ○ Working Memory - Contained within Event
  - ○ Short Term Memory - Contained within RAM
  - ○ Medium Term Memory - Internal Storage
  - ○ Long Term Memory - SQLite and weighted based on time
  - ○ Features
    - ■ Decentralized
    - ■ Fault Tolerant
    - ■ Durable
    - ■ Tunable Consistency
  - ○ ~ 100 Mid Hours
  - ○ ~ 300 Syn Bounty Total
  - ○ **In Progress - Brian Taylor**
- **Sensors**
  - ○ I2P
    - ■ ~ 1000 Senior Hours

- ■ ~ 6k Syn Bounty Total
- ■ **In Progress - Brian Taylor**
  - ○ Tor
    - ■ ~ 500 Senior Hours
    - ■ ~ 3k Syn Bounty Total
  - ○ OpenVPN
    - ■ ~ 250 Mid Hours
    - ■ ~ 750 Syn Bounty Total
- ● **Life IDentifier (LID)**
  - ○ Crypto Authentication
  - ○ ~ 100 Senior Hours
  - ○ ~ 600 Syn Bounty Total
- ● **Amino**
  - ○ Network Bandwidth, Storage, CPU Cycles
  - ○ ~ 500 Mid Hours
  - ○ ~ 1.5k Syn Bounty Total
  - ○ **In Progress - Brian Taylor**
- ● **SYN**
  - ○ Foundation distribution
  - ○ ~ 500 Mid Hours
  - ○ ~ 1.5k Syn Bounty Total
  - ○ **In Progress - Brian Taylor**
- ● **Token Wallet**
  - ○ Save to Vault
  - ○ Load from Vault
  - ○ Save Token
  - ○ Use Token
  - ○ ~ 200 Mid Hours
    - ~ 600 Syn Bounty Total

8 FAQ

9 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.

9.1 Foundation

9.1.1　　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.

9.1.2　　Development Team

9.2 Partners

9.2.1　　I2P

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

9.2.2　　Tor

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

9.2.3　　Guardian Project

Orbot embedded for using Tor.

9.2.4　　Cellular Privacy

IMSI-Catcher, Silent SMS guarding...

9.2.5　　Cybernetic Development Center

Android cleaner service.

10　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 be prepared that will include information regarding how contributed money towards the development of the organization and its technologies at the end of each fiscal year.

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

11 Legal

The following general information applies to this document.

11.1 General

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

11.2 Knowledge Required

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

11.3 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.

11.4 Representation and Warranties

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

11.5 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.