# Zeronet (ZNET)

## Our Independence Is Under Attack!

Censorship!
Disrespect of privacy!
Drowning out minority views and hiding controversial topics!
The corporate oligarchy dominating the internet!

## Mission

Zeronet (ZNET) is a decentralized peer-to-peer internet for everyone who wants free speech with zero censorship.

## Improvements for Everyone

Page Rank is replaced with Trust Rank and your own approved ranking algorithms. A list of your personally trusted people decides content ranking. Content recommendations and trending topics are easily customized to one's own preferred methods and filters, without any unwanted pre-screening or censorship by others. The default recommendation algorithms will prioritize simplicity and transparency for all to see. So, people chose from a broadened selection of open-source and closed-source recommendation methods that avoid unwanted bias of others. Privacy is maximized so that asking for personal identity information such as a name, phone number, or email is avoided. All content is easy to save for when offline.

## Improvement for Content Creators

Uncensored content creators will get maximized share of donations and ad revenues with minimal interaction with middlemen. A network of dramatically improved incentive structures, donation prompts, and participation prompts minimize the desire for adblocking and maximize the desire for easy ongoing donations and other paid content.

## Improvements for Content Distributors

Copyrighted websites are replaced with public domain portals which when copied, most underlying data can also effectively be copied as well. So if Youtube was a portal, the distributor could copy & paste Youtube to their own portal of a different name and it would act just like Youtube does as if they copied and pasted the actual website with all data. Metastream portals are data feeds in replacement of social media websites.

## Mission Highlights

Zeronet (ZNET) makes it as easy as possible for participants to set up information services anonymously over the internet as both paid and sponsored services. Zeronet (ZNET) includes a total peer-to-peer network hosting platform. Peers develop a Web of Trust by connecting with friends and neighbors to help select a

trusted cybersecurity manager. The manager's job is to secure and manage their internet systems to make sure they are safe and useable by anonymous participants only for purposes permitted by the participant, such as content being ethical and moral. Netportal internet browser will be developed to help ensure content anywhere on the internet is discoverable on fair terms. Zeronet (ZNET) includes a collection many ideas which can be done alone without the rest of the network, or skipped as part of the network. If one part is disagreeable, the other parts may be implemented without it.

Adam Grant Generosity Study

A study by Adam Grant found that 19% of people are takers ("selfish" or "greedy"), 25% of people are givers ("generous"), and 56% of people are matchers (match taking with giving). This study may hint that IP (Intellectual Property) and other government systems may be replaced by more voluntary methods of cooperation which suppose humanity to have a capacity for both good and evil, and furthermore suppose that humanity can generally chose good as an option when given the opportunity. The path of Zeronet is to increase the opportunity for goodness by good-faith cooperation.

Call To Action

Please Consider: Take ownership of this road to the future. Participate by any and all actions of any kind they can such as by networking together. All statements in this writing are just as much questions, and you provide the answers. If you see a problem, fix a problem. Be the change you wish to experience. Don't wait unless there is good reason to wait, and question your reasoning to wait because it might not be good. Network with others to begin on this path immediately!

Donation Wallets:

BTC 1KgT45YnhWKfVbnQmsadm934xpYCN9QWV4
BTCH qrg3ugzv028p5zxsvkrxrts36g9z0xs2hutswar3wy
DASH XmfCdNkRMiREi36XHJiirmV7HB6J2U6ao4
MNRO
41nqYooePgJRSo9CtWfVm7V7b6gBEhS528BBeAJRxfVjfC5igqokWgD6zjWd
WsyJGaP2Jd9JxiSMACfdqKueUNVnSFmyjv6
ETH 0xfb84b64df9283257e20eb4e4dd5c583f7bf3952d
LTC Ld7XZ5xAFH8WohoqeosjuQUVoKs4sivQgK

Primary Incentive Reform

Participants pay directly for the cost of the bandwidth they use such as with tokens. Content creators are more directly rewarded both with a donation system and also an alternative advertising model for content creators which participants will be less incentivized to block ads. This change means content distributors will have less say in what sort of content will be produced as

creation influence shifts to creators and donating experiencers away from the people who claim to be distributing for "free" and more toward more transparent and courageous people. So, that legacy distribution model is not free because the distributor actually gets the valuable benefit of censoring and otherwise controlling what content is created, which is avoided with pre-paid bandwidth.

Zeronet (ZNET) Supporting Organizations
Zeronet (ZNET) is an expansive project that requires support from organizations that provide expertise and trustable records through a Zeronet participant web of trust. Essential services to run Zeronet (ZNET) could be better accomplished with the following recommended starting organizations.

Zeronet-Specific Service Organizations:
Rainbow Computer Management Cooperative (Racmac):
Mission  Peer-to-peer web hosting services for Zeronet connected devices.
Primary Offering  Zeronet service cog which securely and seamlessly, without interfering with ongoing processes or depleting batteries, helps participants sell their resources or otherwise donate unused computing resources via the Zeronet Open Exchange (OX).

Signisource:
Mission  Prevent resource leeching by distributing and validating mail tokens.
Goal  Mail tokens enable sponsored or gifted content on Zeronet to be distributed at no further cost to a participant.
Goal  Eliminate nuisances such as "are you a human?" tests while allowing afe traffic from otherwise suspicious IP addresses.

Trinium Traffic Reporting:
Mission  Accurate traffic reporting audits for content creators, content consumers, and advertisers, while keeping demographics data secure.
Goals
- Zeronet (ZNET) traffic and demographics summary reports to all members, while maintaining privacy of individuals and carefully protecting personal data, by Zeronet (ZNET) traffic reporting cog which may interacts with metastream, advertising, and other portals.
- Donation collections based on the smallest sponsorship base of the three mission groups, matched in equal amounts by the other two groups.
- High Trafficog reporting cog adoption rates for accurate traffic reporting statistics.
- High security demographics database, as it can match avatar names to demographics data.

Peernet Support Cooperative (Peersup):
Mission  Peer-to-peer computer technical support for Zeronet (ZNET) and other peer-to-peer networks.
Goals
  Maintain security of computing devices so Zeronet (ZNET) participants can securely and reliably use Zeronet (ZNET).
  Maintain guidance on establishing trustworthy Zeronet (ZNET) service providers.

Zeronet-Compatible Governing Service Organizations:
Caramel:
Mission: Evaluating impact, appreciation, and origins of intangible works to help reward original development.
Goal  Determine originality and influene of works over each other as a percentage number for donations to flow well.
Goal  Study donation patterns of donors for improved donation streams.
Goal  Give donors influence in how their donations encourage further original works.
Primary Offering: Analysis of intangible works providing subjective quantitative metrics of qualitative influence of intangible works over each other.
Secondary Offering: Award and reward structure for donors.

Caroline:
Mission  Help determine the general social quality standing of organizations or professionals.

Caracosa Trust:
Mission  Jointly and securely hold bonded funds for bonded assets with arbitration, escrow, and other dispute resolution organizations.

Caredro:
Caroasi Dispute Resolution Organization
Mission  Governing service for social contracts.

Carvahall:
Mission: Expert evaluation framework of contract performance qualities with quantified subjective metrics.
Goal: Framework for public domain peer reviews, open public reviews, and educational certifications.
Goal: Performance quality reporting including summary reports, honor attribution, standardized reporting, and protocols.
Goal: Data Discovery and Synchronization service cog and portal for creating and discovering experts, professional peer groups, and educational certification evaluation groups.

Zeronet Highlights
  Summary

## Zeronet Summary

Zeronet (ZNET) is a peer-to-peer decentralized internet with emphasis on the freedom of expression. Censorship on the network is essentially zero except as content is designed to be only removable by voluntary cooperation of broadcasting participants. Zeronet (ZNET) is a set of information systems that enables and sets examples for decentralization of services. Decentralized web hosting, decentralized banking, and decentralized civics are all aspects enabled by Zeronet (ZNET). This is primarily accomplished by a Web of Trust created by each participant, where participants delegate trust and control in ways that create a secure network generally by ranking who they trust from most to least and then delegating authorities based on the ranking. Trust is structured and established on an individual basis from peer to peer which then develops to a consensus using a Web of Trust system that increase reliability, comprehensibility, and general usefulness of the internet. The Web of Trust is used to form a peer-to-peer web hosting system. Privacy is strongly respected on Zeronet (ZNET) with anonymity enabled for everyone including distributors. The peer-to-peer hosting system will be kept anonymous for participants by implementing components such as Tor where needed. However, Tor is relatively slow and so it is not used when not necessary as adjustable with participant settings. Zeronet (ZNET) shifts focus from websites which have hidden backends to portals which have open-source distributed backends, and use the Web of Trust and other ways to filter content. Content is distributed through the Public Content Network (PCN), a distributed database system, and can be organized under the Information Graph (Iggy) database which tags or labels Public Content Network (PCN) content as a searchable distributed database of content, topics, lists, and other information. Participants chose Service Cogs (COG) to "latch" to as their trusted information service providers, who will provide Zeronet (ZNET) internet information services and applications. In place of social media feeds is expected to be a metastream service cog which generates a stream of recommended content for participants. Participant are encouraged to form new services as they see potential for improvement.

Agreements and group consensus can be well formed by using Democratic Communication (DCOM) protocols which are expected to be good ways to communicate. The Zeronet (ZNET) Open Exchange (OX) may be used to network with others to facilitate commercial exchange. This commercial exchange can be accomplished with low transaction costs and high transaction volumes using digital money and account ledgers, as support is expected for multiple currencies. Disputes, commercial or otherwise, may be settled with the Public Settlement Network (PSN) which offers methods of mediation, arbitration, and other governance to willing participants. Plain Text Protocol is a foundation protocol providing ease of understanding so that people can read and understand the inner workings of their internet service, making for easy audits of code. Then Group Records Exchange (GREX) is a unified way to share such easy-to-read database text records among organizations. Zeronet (ZNET) is founded on Rainbow Rock philosophy.

Zeronet (ZNET) Focused Virtues and Values

Truth  The truth may hurt. The truth sets you free. All virtue is grounded in truth.

Life  Live and let live. Live free or live not. Life is choices, and choices are opportunities for joy.

Love  We share enjoyment of life because we care. Sharing leads to unity. Unity leads to strength.

Peace  We tolerate and accept diverse values. We prefer patience, restraint, and forgiveness. We avoid attacking unless attacked.

Kaizen  We seek constant improvement. We invite constructive criticism with an attitude of humility.

Health  With value for life, we tune our bodies for satisfying potential.

Wealth  By encouraging creativity, joining in unity, and acting with courage, we build value that will span generations.

Balance  We shall be aware of many perspectives.  Our focus will be measured and adaptable.

Courage  We confront our fears, both external and internal.

These are from the Rainbow Rock Philosophy favored by Zeronet (ZNET) founders.

Zeronet (ZNET) is being created as a new internet to enhance ability to discover truth, enhance freedoms and life, promote equal opportunity and rights, resolve conflict, create prosperity, and facilitate contracts.

We encourage diversity of perspectives to be considered (in acknowledgment of our own bias), and create prosperity for content creators despite oppressive sanctions against sharing of certain viewpoints. Using Zeronet (ZNET), let’s help people achieve personal development despite a callous and demeaning attitude by powerful people, discover more positive aspects of our

challenging society, and bond with those who try courage against their fears in opposition to violence and monopolistic leverage.

Let's develop Zeronet (ZNET) to support the ongoing efforts to usher in an age of enlightenment, reason, and civilization while enjoying watching the oversized agents of evil behaviors disintegrate under their own weight. Organizations focusing on casting light to the shadows will have a truly solid foundation upon which they can launch their missions. We have great hopes for Zeronet (ZNET) to help achieve personal development, find balance, try our courage, and spread love. Let's inform the world of our path to victory and success for granting an opportunity for others to achieve the same joy.

Zeronet's initial developers generally agree with the Rainbow Rock philosophy. We seek to participate in decentralized governance platforms like those based on Rainbow Civics. We prefer decentralized digital money.

## Design Philosophy

Incentive Structuring  Zeronet (ZNET) is designed to ensure that participants are properly incentivized for cooperation. Participants have financial, social, and personal incentives to participate cooperatively. Participants are paid to operate Zeronet (ZNET), participants are honored to behave well on Zeronet (ZNET), and participants coach each other's personal development as part of Zeronet (ZNET).

Understandable  Zeronet (ZNET) components are meant to prioritize understandability. The more easily you can comprehend, the more easily you can trust. We emphasize comprehensible system at every level from the philosophy to the smallest bits and bytes of construction.

Simple  Simple components are understandable. Zeronet (ZNET) components are constantly redeveloped to be satisfyingly simple and satisfyingly easy to redesign and work with, given the requirements of the network. Let's develop Zeronet as simple to use and also simple to understand, create, and redevelop. While every feature does require a certain amount of complexity to be added, efforts are taken to reduce that complexity.

Intuitive  Intuitive parts are understandable. All parts of Zeronet (ZNET) are designed as an estimation of the least amount of effort for someone who has never experienced technology to guess as to how it works without being told. Developers are encouraged to imagine what other people would agree is the most reasonable way to use Zeronet (ZNET) despite being expansively useful.

Marketing  Features and benefits of each component should be clearly presented. Functionality that is poorly explained will tend to be poorly used. Marketing is not just hype, but it is a means for people to understand what it is they have. Knowing what you have enables people to use what they have in full. Our

marketing isn’t so much for wealth as it is for learning.

## Call to Action

Please Consider: Help create this! If you can’t code, then any and all skills will be used to their full potential for this project.

Please Consider: Dedicate your spare computing resources to Zeronet (ZNET) using a trusted peer-to-peer network manager trustee. Or, you can begin your own peer-to-peer network under the Zeronet (ZNET) protocol such as by the Rainbow Computer Management Cooperative (Racmac) cog as an example. If you are passionate about technology engineering, you are encouraged to sell your own spare resources individually without any manager. If you are passionate about technology engineering, develop Zeronet (ZNET) with us.

## Peer-to-Peer Financial Incentive Structure

Good incentives are extremely important for not just Zeronet (ZNET) but to built a functioning society into a flourishing civilization. Participants are encouraged to sell their spare computing resources over the internet for the purpose of Zeronet (ZNET). They are furthermore encouraged to do this anonymously. They can do this them self for 100% of the revenues, or have a peer management service do it for them for a percentage of revenues. This peer management fee is hoped to be the primary driver empowering the network to grow quickly because we will have a revenue stream with which to accomplish that in comparison to other peer-to-peer networks like Bittorrent that while also successful have not been adopted by most internet users. We want it to be easy for anyone passionate about computing technology to participate in development in Zeronet (ZNET) by starting their own peer management service. Income from peer management services by participant is then encouraged to be directed in part to their favorite Zeronet (ZNET) content creators as donations, awards, and rewards. Content creators are then incentivized to invest in Zeronet (ZNET) peer management services.

## Security Focus

We want to be able to defend against the most well funded efforts to attack any participant, especially those being anonymous using the network to fail when they follow simple security steps while using the network. One security challenge for this network because of its encouragement of total anonymity will be avoiding use of the network for spamming and bot accounts that do fake reviews and other unethical behavior which must be well developed before deployment. A primary resolution to this may involve a bond-posting system where participants who lease another peers account post a bond to a mutually trusted participant in guarantee of avoiding such behaviors.

Example Experiences:

Zeronet (ZNET) Pull Experience Informal ’Use Case’ Explanation

A participant opens their Netportal internet browser. They have developed their Web of Trust with the help of their neighbor who gave them a memory card with the Zeronet (ZNET) software for their Android phone. Using this Web of Trust the participant’s computer establishes trusted internet connections for pulling (downloading) and pushing (uploading) content, and latching on to internet services recommended by a friend. The participant latched on Zeronet (ZNET) Service Cogs (COG) that provides them basic internet services including web search and metastream service. A metastream provider provides a list of internet content recommendations. Their Netportal application initially lists 24 items of all types of content recommended to them including video, text messages, news stories, music, and so on. Their preferences are to pull all content types which includes video similar to the "Youtube" website, pictures similar to the "Instagram.com" website, and messages from friends like the "Twitter.com" website. Their selected metastream provider shows exactly how recommendations are formed including all math involved, and subjects itself to regular code audits to prove their recommendations are not unfairly biased against "lesser people", even when they don’t have any followers. So for that reason and others, they trusted and selected that metastream provider. Their metastream provider includes most censored and banned content where at least one copy exists essentially anywhere on the internet. The participant has filtered out "Sexual Crime Evidence Video" against being recommended with their settings, which was the only default filter toggled on when they first connected, and the participant believes that is a good filter setting.

The participant then opens the Netportal internet browser which lists recommendations from the metastream provider. One of the items in the list is created by a creator named "Onion Report". The participant pulls (downloads) the item. The participant evaluates two of the recommended items, but only the item authored by "Onion Report" was found valuable. For that item he gave an award he custom-named "news of the day", the value of which is calculated to be $USD 4 cents according to an automated award formula that ensures award money won’t run out. The 4 cents was a below average award as this participant typically awards 26 different content items per day, but that leaves the participant more for good items like "news of the year" to have much higher awards, so there the participant gives $USD 1.00 for an award they call "news of the year". The participant did not edit the award amount setting (which automatically set the value of $USD 4 cents) so that was the default

value for the award. Onion Report is able to get enough such awards to create better content. This award system tells the metastream provider what kind of content it should recommend. Because Zeronet (ZNET) works partly on awards, an automated walk-through menu when the participant joined helped them decide how much they could afford to award on a regular basis to content creators to help ensure the highest quality content. The participant decided to cut cable service which costed USD$ 80 per month in the USA to instead give the USD$ 80 per month to help independent content creators, USD$ 70 of which goes to Zeronet (ZNET) content creators each month. Had the participant lived in Russia, the cable bill might have been closer to USD$ 5 per month and so the award would have been less at USD$ 0.0025. The participant then left a comment on the content asking the author to keep covering important stories. Finally, the participant clicked the share button to share the "news of the day" with a friend, and selected a friend who he knew would appreciate the news.

Zeronet (ZNET) Push Experience Informal ’Use Case’ Explanation

A content creator named "Onion Report" is a group of news media professionals who create news videos and news articles. One of the "Onion Report" professionals learns from a friend that they can publish to Zeronet (ZNET) in hopes of donations for the content in addition to advertising sales. The creator has a news report and an associated ’metafile’ with information about the news report type and credits for publication. The content creator participant developed their Zeronet (ZNET) Web of Trust with the help of the friend who provided a Zeronet (ZNET) memory card designed to share Zeronet (ZNET). With the help of a video creator tutorial included on the memory card, the creator latched several Zeronet (ZNET) Service Cogs (COG) to help them distribute their content. They latched Service Cogs (COG) for video file storage, an advertising service, content advertising service, and a citation and plagiarism detection service.

First, the creator pushes (uploads) a video to their latched File Storage Service Service Cog (COG) which is a service that specializes in video file distribution using the Zeronet (ZNET) peer-to-peer web hosting system. The file follows Open Collaboration Protocol to help the creator receive credit for their work when used as a basis for future content by other creators, and (by extension) credit others for credit due. The citation and plagiarism service is then automatically provided with a reference and pull token (a one-time upload password) to the video and associated metafile as part of their file storage service settings. The citation service pulls (downloads) the video for analysis. Their analysis is able to identify different sources for four audio clips and two video clips for a total of six

citations. That analysis is sent to the working professional's Zeronet (ZNET) private metastream by the citation and plagiarism service. The professional opens their Netportal browsers shows the private message at the top of their message stream. Although the message was not the most recent one, they set their Private Message Filtering Cog using Netportal (internet browser) to highly prioritize messages from the citation and plagiarism service causing one to appear at the top of their metastream content list. The participant loads the message which informs them that one of the video clips has not been properly credited, which references the associated Open Collaboration Protocol file. The Onion Report participant revises the metafile according to the Open Collaboration Protocol to credit that video author with the authorship. The video file is repushed (uploaded) but the push goes quickly, because only the changed part of the file (the metadata section) is replaced which credits all the collaborative content creators. The File Storage Service Cog has a feature to ensure that files with the same name are only repulled as needed. This time the file checks out well with the citation and plagiarism service.

The content is ready for publication. So next, the creator's Broadcast Cog is used to stake an Original Creativity Claim (Ocla) on the content through the Public Settlement Network (PSN) as will be better explained in those sections. The creator decided to include the expected original broadcast time in the content metafile, which is short enough to be distributed as a Public Settlement Network (PSN) message. Their trusted broadcaster replies with a confirmation and timestamp of their claim. The file is then added to the Public Content Network (PCN) by sending a link to the content to the creator's Data Discovery and Synchronization Cog (Disco). The participants Data Discovery and Synchronization Cog (Disco) is used to distribute links to the new video, which go to most metastream providers, and most Topic Search Cog providers for the widest distribution. These two provider types are the bulk of Zeronet (ZNET) content distribution systems for this type of content. Metastream providers have an easy time distributing the content reference immediately because the "Onion Report" is widely subscribed. 1,096,153 subscribers are online combined with all metastream providers, who all receive notice of the pending publication within one minute of its announcement. The File Storage Cog uses a Service Distribution Cog to ensure that the file is widely available for pulling (downloading) in 2,588 Zeronet peer locations upon release for the first thirty minutes of release when high demand is anticipated. A summary of the content appears in 3,739,305 participants metastreams in the first day of publication. All metastream providers send up-to-date statistics on all

of this including revenue information as requested. When the "Onion Report" professional checks their Netportal metastream distribution portal, they notice that the content is appreciated when they see about 125,000 participants on that day who gave an average of 4 cents to the content, so "Onion Report" receives a total of about USD$ 5,000 for the day, for the newly released content.

Zeronet Component Summary:

Public Content Network (PCN)

is a method for distribution of information providing freedom of speech in that content may only be removed with voluntary cooperation of all participants having copies of the content. This is a distributed internet content database. All participants have the opportunity to share any content they wish. Participants can better distribute both 'free' as sponsored and paid content according to their goals. The Public Content Network (PCN) enables a high percentage of revenues (perhaps 95%) for content creators who accept money awards, while all participants may also be well compensated for their content distribution. So, there are many different methods content creators are rewarded for their creations. The network supports an expansive range of information services including video, text articles, topic search, database, consulting, and interactive forms. These services are generally organized on a cooperatively formed 'Topic Map' system for searching, querying, and browsing by topic. Participants select from a range of recommendation engines with transparent recommendation systems. The Open Collaboration systems (ref Democratic Communication:Collaborative Development) allows participants to cooperatively develop content without a specific hierarchy but with controls to prevent malicious edits. Content is interactive with feedback and development encouraged in many ways. While participants have expansive control over the content they broadcast, encryption makes discerning what is being broadcast difficult to impossible without specific reports from content recipients including a decryption key if the content is encrypted. This network is expected to be filtered using the Web of Trust to help eliminate malicious content and increase information accuracy.

Web of Trust

is a trust ranking system where each participant carefully establishes who they trust most and least. This is used to offer a perspective and filter of the internet. Trust rank is used to determine permissions for modifying Zeronet (ZNET) devices including creating and modifying Zeronet (ZNET) records, files, processes, and applications. This provides security, having information with prioritized accuracy, satisfying privacy, and expansive connectivity by cooperating with

trusted people. The Web of Trust is the key component to develop consensus and certification with peers for improved security and data integrity of Zeronet (ZNET). Personal information is encouraged to be kept locally on the participants device without being shared to anyone, except as considered needed for specific purposes. Participants delegate trust to groups through their network of trusted peers, and such groups are used to form consensus as further described in this writing. Public reviews of public pledges including contract performance information is expected to be shared as public trust rank information, which is cooperatively reviewed and summarized by peer review participants. Sufficiently trusted peers are delegated to certify or otherwise help determine information by analysis and testing. Peer reviews are then re-filtered through the web structure using trust rankings controlled individually by each participant. This process helps participants determine what information they might find most valuable and display the the confidence they can expect to have in that information given the source or source chain. When personal or sensitive information is shared using the Web of Trust, there is expected to be an explanation of all details of information sharing (who, what, when, where, why, how). Participants have control over this sharing process to share as little or as much of their information as gracefully as possible. When information is shared, redistribution is encouraged to be carefully controlled with a Data Negotiation Service. A web of trust is a useful element for many Zeronet (ZNET) components, including the Public Settlement Network (PSN), Open Exchange (OX), Public Content Network (PCN), and Open Collaboration Protocol. After participants form consensus on guarantees of behavior to each other, participants are encouraged to build trust with others in their network by Posting Bond to guarantee behavior according to those assurances on Zeronet(ZNET). Further trust is encouraged by formally rate each other's reliability with their contract performance.

Democratic Communication (DCOM)

This Zeronet (ZNET) component defines how public and private communications among participants happen. Protocols(languages and their syntax) and naming conventions used by participants are shared and accessible in a transparent cooperative way. A set of network protocols defines how communications occur on Zeronet (ZNET) at all levels of the network. Methods for establishing identity as a participant and also methods of private encrypted communications among participants are adapted by each participant for cooperation with other network participants. Importantly for reduced conflicts, this system shared sets of word definitions for social and commercial contracts. Methods for creating and distributing public and private messages

are established for that. Transparency is required for trustworthiness and improved participation, and this is achieved with Plain Text Protocol (PTEX), which allows an expansive range of people to be able to be able to see and change the inner workings of Zeronet (ZNET) with comprehensibility.

Information Graph (Iggy)

is a search database used to organize shared information on Zeronet (ZNET) including information on the Public Content Network (PCN). The Information Graph (Iggy) is designed as a database of words or phrases (typically forming searchable topics) connected to specific meaning and content, in order to easily share lists and sets of information that are referenced frequently. All other Zeronet (ZNET) components that use any sets of information may use the Information Graph (Iggy) as their database and list source. It is expected to contain simple word or phrase lists used by other Zeronet (ZNET) components as well as networking connectivity information. The Information Graph (Iggy) is an associative network of connected node's (like a spider web having lines or "edges" that connect at certain points) that enables grouping, classification, and sets by other components. For example, a person may assign certain individuals to a group name and then rank them equally in the Web of Trust. So, a man named "Nicola Tesla" could be listed in a "scientist" set and classified equally with other scientists in their Web of Trust. That list could be created by other components based on participant data entries to Zeronet (ZNET). Importantly, it acts as a search engine database component for Zeronet (ZNET) for components that have lists of links. This component is only designed to be used by other components where sets are relevant. The same graph structure and data can be used by multiple components. Like the Democratic Communication (DCOM) component, this may be used independently.

Service Cog (COG)

Zeronet components may depend on each other for functions. Such data interactions are expected to be done in the form of an automated Service Cog. For example, the Netportal component is a browser that is expected to retrieve a search result set for a given internet search query, and that function could be made accessible by other applications. Organizations may be formed to offer any and all data queries, data processing as a service, and any information service they wish to other participants. Zeronet (ZNET) participants may offer content creators improved broadcasting effectiveness by division of labor to Zeronet Service Cogs (COG), outsourcing information processing using this component. Content providers may offer content receivers improved query effectiveness by connecting them to content they find valuable with paid or sponsored search services. One important Service Cog

(COG) is expected to be a Topic Search Cog which is an internet search query service where you provide a search query and the results are returned by the Service Cog (COG). Also, all individual components can be considered a Zeronet Service Cog (COG) component when these components exist on a remote shared computer as a service. That allows more ways of using Zeronet such as accessing it through a traditional internet browser. Depending on privacy considerations and available resources, these cogs may be done on a participants device, outsourced to a peer, or a combination of both.

Public Settlement Network (PSN)

This standardized public announcement format has the primary purpose of secure commercial exchange. The Public Settlement Network (PSN) is a network focused on the broadcast of public statements of fact and guarantees that facilitate transactions, evaluate public pledges, and help resolve conflicts. This settlement network also helps participants determine public consensus on any number of issues of interest, including blockchain validation. This network relies on both the Web of Trust and Democratic Communication (DCOM).

Open Exchange Network (OX)

A public forum protocol for online stores, trade offers, social contracts, and any other public exchange offerings. This exchange is based on the Web of Trust, Public Settlement Network (PSN), and Public Content Network (PCN). Open Exchange (OX) includes a system named the Private Information Technology Resource Exchange (PITREX) for leasing computing resources for remote usage expected to be easy to use by Zeronet (ZNET) participants for peer-to-peer web hosting and other purposes. The system prioritizes and satisfies the privacy capabilities of exchange participants, although some of the contract information is intended to be publicized for efficient market exchange.

Netportal

Netportal is a display system for Zeronet (ZNET) content. Netportal is an internet browser software application for viewing, filtering, and searching the Zeronet (ZNET) content in discovery of high value content. Viewing trusted information from a limited number of sources can limit one’s range of information available. Netportal includes a Competing Perspective Consideration feature which allows people to view a full range of competing perspectives to encourage more people to think for them self. Furthermore, the monitoring option helps allow one to keep an eye on opponents in addition to allies to avoid group think bubbles.

Netportal is expected to have a flexible navigation system. Websites are expected to be replaced with portals, which are designed to be more adaptable so that a portal can be easily copied and repurposed for similar services.

Zeronet (ZNET) Detailed Highlights:
- Design Philosophy
- Example Experiences
- Zeronet Component Summary
- Public Content Network (PCN)
  - Key Features
  - Topics
  - Metastreams and Content Propagation
  - Content Development
  - Content Distribution
  - Content Analytics
  - Value Exchange
  - Focus Points
- Web of Trust
  - Web of Trust Basics
  - Foundations for Trust
  - Public Trust Reporting
  - Perspective Development
    - Web of Trust Garden
  - Honor Assessments
  - Trust Information Sharing
  - Trust Analysis
  - Zeronet Permissions and Control Assignment
  - Privacy-Transparency Balance
  - Open Collaboration Trust
  - Web of Trust Consensus
  - Contracts
  - Pledges
  - Reviews
  - Assurances
  - Data Negotiation Service
- Democratic Communication (DCOM)
  - General Concepts
  - Overview
  - Encryption Terms
  - Identity Information
  - Contact Security Considerations
  - Protocol Establishment
  - Cooperative Development
    - Contract Agreement Communications
    - Open Collaboration Incentives
    - Open Collaboration Protocol
    - Open Collaboration Structure
  - Conflict Resolution
  - Protocol Resolution
    - Sigil X Protocol
  - Zeronet Protocol (Zerp)
    - Protocol Development
    - Topic Search Protocol
    - Network Connectivity
    - Data Traffic Strategies
  - Security Suggestions
  - Secrets Protocol (SPROC)
    - Secrecy
    - Privacy by Encryption

Zeronet Additional Goals:
Component Adaptability Principle

Zeronet (ZNET) components are open ’pluggable’ systems broadly designed to be replaceable by competing components. Each component is designed to be usable by (both indirectly related or unrelated) information systems with simple data interfaces. Components are designed to have a generic human-readable text interface with each other. Content posted to the network is likewise formatted in such a way as to be easily edited.

Component Independence Principle

Most components are generally designed to be installable as the one and only purpose of Zeronet (ZNET) installation on any given device. So, participants can run one part of Zeronet (ZNET) without using any other component when that can be done well.

Internet Signup and Login Elimination

Currently people must establish an identity for each website they visit on the internet by a sign-up or registration system. Internet websites are hoped to be replaced with Zeronet (ZNET) portals. A Zeronet (ZNET) portal does not need this because users self-identify by their public encryption key for communications. If you have an encryption key then you have a universal login to any Zeronet Protocol portal or website. People often leak their data to untrusted globalist voyeur networks such as Amazon in order to sign into a website. By the year 2030, the traditional signup and login process might be eliminated in favor of minimalist self-identity. For a login to any Zeronet (ZNET) portal, simply create a common encryption key. The fact you have a common encryption key is expected to work on all Zeronet (ZNET) portals as an effective log-in although some services may need additional information to provide services you want.

Performance Targets

One webpage display of text and some image data should load in less than twice ping time. So, if ping time to a peer is 200ms the load time should be under 400ms. Non-random data is expected to be compressed to some degree before being encrypted.

Encryption should take no more than three times the unencrypted loading time for any given file.

Offline Capability

We may also establish a paper version of Zeronet (ZNET) in case the internet goes offline or for those who don’t have internet access.

PUBLIC CONTENT NETWORK (PCN):

Key Features:

Metastream

Participants are expected to use a Metastream service to discover Zeronet (ZNET) content. A Metastream is a frequently or continuously updating list of content recommendations. Most content is expected to be

delivered by a Metastream provider whose job it is to help participant's to prioritize content to be pulled (downloaded) and loaded (displayed, played, reviewed, etc). So, a Metastream is like Youtube, Reddit, Twitter, and all other social media websites recommendation pages combined into one. However, the stream can be limited or compartmentalized to be virtually identical to any of those websites by displaying specific types of recommendations. Unlike other social media, metastreams may recommend private messages, content recommendations, or both at once depending on participant preferences such as set by their Netportal browser. The Metastream list contains the title to each prospect content and a reference that the participant selects to receive the content such as by pulling (downloading) from a specific broadcaster or internet location. Participants may choose which topic interests are shared with each of their metastream Service Cogs (COG) by sending them profile information to improve recommendations. Participants may set an ongoing stream of award and reward revenues to be distributed to positively valued content upon review which is the primary way a metastream provider determines which types of content the participant likes.

Content Discovery

The most commmon ways expected to discover Public Content Network (PCN) content are Metastreams and topic searches. The content is expected to be displayed through a Netportal internet browser. Topic searches deliver any specific query for information and are basically "web searches". Portals (ref Netportal:Portals to Replace Websites) are the primary interface for both sending and receiving Zeronet (ZNET) information and are much like websites but some portals have capability to change system settings. Those portals which do have capability of changing a participant's local device processes are expected clearly marked as such for improved security. Metastream service is "latched" by linking to a metastream service cog. See Service Cog:Public Content Network Cogs:Metastream Cog for details.

Content Types

For expected Zeronet (ZNET) Content Type categories, see Democratic Communication:General Concepts:Content Types (Metaclass).

Public Content Network Cogs

The Public Content Network (PCN) uses multiple information services that each automatically perform a specific task. These information services are "service cogs". A listing of starting Zeronet (ZNET) Service Cogs (COG) can be found in that neighboring section. Each service provider may have one or more "service cogs" which are similar to browser plug-ins.

Topics:

Topic

Topics are like the current hashtag (#) usage on Twitter and other social media platforms marking important subjects of content. Each topic has a meaning, and each element of meaning is associated with a corresponding topic node on the Information Graph (Iggy) Topic Map (as detailed in that neighboring section). Content submitted to the Public Content Network (PCN) is expected to be classified into one or more topics using an index file listing each topic and the associated content reference pointing to which part of the content best matches with the topic. While topic(s) are expected to be assigned by the content creator, additional topics may be assigned by anyone for any content. When content has multiple topics, the content may be marked with reference points or ranges corresponding to specific parts of the content that are associated with each different topic. This may be done automatically to some extent by a Topic Cloud Cluster Cogs (ref Service Cog:Public Content Network Cogs:Topic Cloud Cluster Cog). Topics may be referred to as "tags" or "tagging" but Zeronet (ZNET) tagging also refers to attaching certain types of commentary and review information to existing content either on Zeronet (ZNET) or other information networks (ref Netportal:Content Tagging). Each Public Content Network (PCN) topic is a word or phrase that classifies content to a category listed on the Information Graph (Iggy) Topic Map (explained in a section nearby).

Network Map

A network nodal graph. A database of network nodes, node. connections (or edges), and values or weight of each connection. Each node represents a semantic entity.

Topic Map

List of available topics and the connection from each topic to each other topic as a topic "network map" (see nearby section). The more similar one topic is to another, the more they are considered connected to each other and so connect on the topic map.

Long Topic

A topic that is actually a number of topics put together as a "topic map path" (see "topic map" nearby). This would be like a multi-word hashtag on Twitter. So, "hill" is a topic, and "hiking" is a topic, therefore "hill hiking" could also be a topic. Order is important, so the encouraged order of words is most to least common grammar so that "hill hiking" would be the expected topic rather than "hiking hill".

Topic Map Nodes (#)

Part of the Information Graph (Iggy) is the Topic Map. Each point on the Information Graph (Iggy) associates with specific content and also is considered a potential Public Content Network (PCN) Topic Map node (#) to which information may be appended by any person for any reason using any one of many other Zeronet (ZNET) components. So, all Information Graph (Iggy) nodes may be considered

as Topic Map nodes (#) because any content or content part may be individually considered and casted as a topic. Important Information Graph (Iggy) casted as topics include Democratic Communication (DCOM) avatars, Public Content Network (PCN) content, Public Content Network (PCN) broadcast channels, Open Exchange (OX) records, Open Collaboration Protocol content, and any other node on the Information Graph (Iggy). All of these nodes are considered topics which can be searched for in the Public Content Network (PCN) using a topic Service Cog (COG) or search Service Cog (COG). One usage for such topic node connections is to easily add public comments to any internet content as comparable to Gab's Dissenter service. As another example, a Service Cog (COG) could import each new product posted to a UPC goods barcode database for example as an Open Exchange (OX) record. Participants could then add a Group Records Exchange (GREX) (ref attachment) record as public content with the topic being UPC Bar Codes and the content set being each UPC barcode record.

Topic Cluster

Topics are expected to be classified into topic clusters according to activity level such that each group has a closer to equal amount of activity, relatively higher activity groups become more average, or relatively lower activity groups then become more average. So, strongly linked topics are summarized as one topic cluster. A topic may be divided to two strongly linked topics to result in lower per-topic activity so that the topic is closer to an average traffic level. Topics may belong to more than one topic cluster. Topics may be arranged in a hierarchy depending on the interpretation of the Topic Map Service Cog (COG) or participant client Netportal application. (ref Service Cog:Public Content Network Cogs:Topic Map Service Cog) Avoid confusing Topic Clustering with Content Cloud Clustering (C3) which merges sufficiently similar content so that slightly different data is treated identically as one content so that practically identical content is not effectively double listed in content lists. Clustering is also expected to be used to reduce the required processing of a topic map by Service Cogs (COG) as participants are expected to have a large number of topic interest records.

Formal vs. Informal Topics

Any meaningful semantic can be considered a topic. However, if the topic isn't listed on the topic map it is translated to an existing existing formal topic or created as a new topic.

Main Topic

For a given content, the main topic is expected to be determined by several factors. The primary factor is expected to be the topic in which the content is found most valuable. So, when subscribers to that topic honor the content more than when that content is hosted in an

alternative topic, the content is likely a better fit as the main topic. This may lead to people most passionately interested in a given content be the ones to determine the topic of the content. Other factors include the topics as specifically delegated by the creator and the topics as specifically delegated by a Topic Service Cog (COG). The Topic Service Cog (COG) selected by each participant may use participant preferences and their Web of Trust to determine which content to allocate to a specific topic for that participant. Because of exponential complexity in such a process, its likely there will be a small number of Topic Maps (ref that section nearby) that apply to different participants who differently consider topics differently due to language differences.

Topic Hint

The topic assigned by a Topic Hint Cog (COG) expected to be the most valued topic of the content as broadcasted. Multiple topics may be ordered by most to least likely. This is a service that matches Public Content Network (PCN) content to specific topics so content creators can see what topics their created content may belong in.

Topic Map Network Links

For search and discovery purposes, topics are generally linked to each other on the Topic Map (ref that section nearby) by any content that refers to multiple topics in close proximity. Generally "topic proximity" refers to the rated value content has in that particular topic. All participants involved including content creators and metastream providers negotiate topic proximity in a content index file for each piece of content on the Public Content Network (PCN). This is expected to be done in many ways such automatically by a content creators summary software, by a specialized Service Cog (COG) (ref Zeronet:Service Cog section), or by individually custom manual review. Each connection on the Topic Map has direction, relative strength, and crossover. Crossover is the likelihood that a person who values one topic will also value the topic of comparison topic as measured by average shared value on the network. Each node on the topic map has a certain popularity. Popularity defines the direction of each connection. Less popular topics point to the direction of any more popular topic of highest crossover rate. This allows the formation of a tree-like hierarchy perspective of the topic map without having to "manually" define such a structure, because for example "music" is expected to be more popular than any one specific type of music. This directionality also enables a way in which the network nodes may be fully sorted in a list for faster searching.

Omni Point Topic Node

The most popular topic node on the Information Graph (Iggy) Topic Map is considered the ’ommni point’ node, which is simply a node for a topic representing all

topics. This organizational node ensures that all topics will connect to each other by at least one path on the Information Graph (Iggy) Topic Map. This allows the Topic Map (ref that section nearby) to be organized according to a hierarchal data tree structure. All content may be considered a member of that topic and may be indexed as an "omni point" topic.

Topic Search Cog

(ref Information Graph Cogs:Database and Search Cogs:Topic Search Cog)

Subscription (Sub)

A direct subscription occurs when a participant wants to receive content meeting specific conditions (typically content created by a specific creator or being listed under a specific topic) on an ongoing basis. Subscriptions are delivered by a Metastream Service Cog (COG) when they insert the subscribed content into the metastream. The timing of delivery is expected to be set by the participant, whose avatar profile (ref associated section) is expected to include default instructions for delivery of new subscriptions. Any changes made to that delivery timing should be relayed automatically to all metastream Service Cogs (COG) selected by the participant. Each metastream provider is expected to have a unique offering of subscription services, so some may be better at filling requests than others. An indirect subscription occurs when a participant tends to signal value for content meeting one specific condition involving one specific factor without specifically requesting it. Common subscription types are expected to include topic subscriptions, creator subscriptions, and broadcaster channel subscriptions.

Topic Streams and Topic Subscriptions

A Topic Stream is a metastream of a specific Zeronet (ZNET) topic. If a participant wants to know about one specific topic, then they can directly request or view the topic stream as a single channel which only displays content about that topic. A Topic Subscription is when a Zeronet (ZNET) participant implies or expresses interest in content, their indirect recommendations with the associated topic are expected to increase. A participant may adjust subscription levels indirectly by interacting with content, or directly by requesting a higher receipt level for the content topic or content participant. So, the participant’s chosen metastream Service Cogs (COG) are expected to list and rank content according to both direct request and indirect implications. This is comparable to current Youtube recommendations but without as many "mistakes" where creators unfriendly to the ruling class are "accidentally unsubscribed". As with all Service Cogs (COG) each participant selects a metastreamer who suits their budget and trust level. Metastream Service Cogs (COG) track newly added content to a topic and may relay the metastream of that content to participants upon subscription. So, each topic on the

topic map may have a subscription level. Such subscriptions may also lead to content from related topics being added to the participants metastream that are heavily associated with the channel when they predict the participant is likely to want that. So, the direct subscription may trigger indirect subscriptions on related topics as the metastream service decides.

Monitoring Subscription

When a Zeronet (ZNET) participant is interested in a topic but does not currently wish to support the associated content creators or developers the participant may subscribe as "monitoring". This would offer a perspective of opposing viewpoints without supporting such viewpoints, and contributions are expected be offered to dissenting perspectives or other content. (Related: Netportal:Competing Perspective Consideration )

Topic Map Avatar Profile

An ordered list of preferred topics and their level of subscription. Formatted as a network map.

Metastreams and Content Propagation:

Metastream

See Key Features:Metastream in neighboring section.

Metastream Service Provider

Participants are expected to select a service provider Service Cog (COG) who provides the best content recommendations for their given budget and expressed interests. A public Metastream Cog (ref Service Cog:Public Content Network Cogs:Metastream Cog) delivers the metastream by the metastream provider. Added to this list is expected to be content as recommended by trusted peer(s). Any participant may become a Metastream Cog (COG) provider and so it is up to each participant to use their Web of Trust and personal judgment to select the best fitting Metastream Cog. As with all Service Cogs (COG) the Metastream Cog may use other Service Cog (COG) participants for all other service functions or may do all functions their self on their device locally if enough resources are available.

Metastream by Avatar

Zeronet (ZNET) participants select a Metastream Service Cog (COG) for a given avatar to display a list of prospective valuable content. So, different metastreams may display based on the Avatar selected, likely by using the Netportal browser to switch avatars. This allows multiple participants to use the same browser by switching to different avatars and allows more privacy by compartmentalizing public interactions to different avatars. Also, this allows people to look at the internet in different perspectives by switching avatars. Participants may want to use different avatars for different types of activities such as an avatar to represent them as part of an organization.

Metastream Collation

The participants computer (such as using Netportal) may collate multiple metastreams by either different Metastream Data Service Provider(s) or multiple metastreams of one Service Cog (COG) into one metastream. Avatar data may be stored on remote systems in such a way that computers can be almost instantly reconfigured to change the set of avatars receiving data. This is most relevant in circumstances of censorship where metastreams may be under monitoring by hostile parties. It may also be done to reduce security breach damage. Advanced Metastream Data Service Provider services could include cross-network collation such as providing Facebook or other social media content or content links and notifications (including HTTPS push notification and custom proprietary notification types) collated to one metastream.

Content Payment Instructions

Content creators are encouraged to be the participants to supply content payment method information, not the metastream provider, as to properly incentivize higher value content.

Content Propagation

Content listed on the Information Graph (Iggy) Topic Map begins under a specific topic then spreads to other associated topic channels at a speed according to the expected value of a content given its potential placement in the neighboring topic channel. For example, if content featuring a bear toy does well under "teddy bears" it may then be placed in "stuffed animals" and subscribers to the "stuffed animal" topic then receive that content reference in their metastream. If it does poorly in that topic, it could then be removed by those metastream providers. If it does well, it might then be added to "toys" topic by a metastream provider. Furthermore, the number of new topics tested simultaneously for highly valued content would be expected to increase exponentially until reaching an expected peak topic count. As the content ages, the topic placement count is expected to decrease over time until reaching zero topic placement upon its deletion by all content hosts, although archive services may cause deletion to take a long time. Each topic may have an associated ’archive’ subtopic where content remains indefinitely. Each metastream provider may independently decide which content belongs in which topics, though first notices any topic hints listed by content creators in that decision.

Topic Network Pulse Propagation

The Information Graph (Iggy) is a set of nodes, many of which are cast as topic nodes. See nearby Topics:Topic Map section for details. Content generally begins at a single topic node. Periodically the network measures the viewing traffic to all content with public cooperation of all participants encouraged though not required to publish traffic data to the public domain in a way that

can be audited for data trustworthiness. Content having relatively high current views or donations propagates to the most related topic channels which have not yet adopted the content to their channel.

Topic Popularity

is determined by multiple factors using participant negotiated statistics. There is expected to be paid traffic reports involving a mostly automated negotiation process among various Web of Trust participants to determine topic popularity.

Traffic Reporting Accuracy Incentives

Traffic reporting is a system with complex dynamics because many different Zeronet (ZNET) participant roles have many different incentives for traffic reporting accuracy (or inaccuracy). Content pullers (downloaders) have mixed incentives. Incentives for content pullers are generally neutral. Some will prefer to under-report for content considered hostile that they monitor. Others will prefer to over-report for content they have a positive bias to, in an effort to get others to notice the content by claiming popularity. Advertisers will want traffic to be under-reported. Content developers and distributors are generally to over-report to make their content appear popular or collect more adverting revenues. Incentives to under-report may also exist for controversial or banned content, which may be done in an honest way as it is considered acceptable to keep such information private. The most difficult to fake reporting is expected to be based on donations done by public ledger currency. Anti-adblocker content may have incentive for under-reporting by hostile ad-removed version providers. The expected preference for Zeronet (ZNET) content is for expansive control to be on the demand pull side in reduction of unwanted advertising. Multiple reporting sources are encouraged to be used by all participants so that the services reports can be compared. The important incentive structure though is for Metastream Providers (ref associated section) because the incentive varies for different providers. Donation-only and ’donation rejected content’ providers are expected to be a neutral party whose primary interest for traffic is accurate reports to best decide what content would be most valuable to each participant. So, these services are expected to be the primary middleman for accurate information. But even in these cases, they may wish to report traffic to others falsely to have a competitive advantage or other unknown reasons. This is why multiple sources must be checked against each other. To properly tune incentives, a traffic negotiations process is expected to be done by a Data Negotiation Service (ref Web of Trust:Data Negotiation Service) specifically set up where revenues are equal between pull and push side. So, both traffic push sources (distributors, content creators, etc) and traffic pull sources (generally Netportal participants)

are both expected to directly pay a Data Negotiation Service Cog for receipt of accurate traffic statistics. Each service provider is expected to use a spillover accounting system that refunds any mismatch in statistics revenues using a system of public accounting ledgers. Furthermore, it is expected to be a relatively easy task for any participant to start a service cog of their own. One issue is that it is difficult to know whether an unknown participant is actually a push or pull source. So, claims filtered through the Web of Trust are important for traffic report analysis. Public Data Reporting Service Cog is expected to be used to aid in this analysis. Any actions for accurate reporting whatsoever are a nearly certain improvement over currently popular systems which in many cases is simple blind faith in one content distributor to provide accurate information.

Traffic Reporting Cog

See Service Cog:Netportal Cogs:Public Data Traffic Reporting Cog.

Content Propagation Network Map

Map of content propagation data. Can be used for a visual representation of content propagation and interest like a "heatmap".

Content Propagation Network Map Provider

A service that renders Content Propagation Network Maps. This service may be valuable to content creators who wish to create content based on evaluator demands.

Content Value Prediction Service

Determines content a participant is most likely to value. This is the primary service of a metastream provider but may be used for other Zeronet (ZNET) purposes. See Zeronet (ZNET) Service Cog (COG) section for details.

Censorship

Participants are individually responsible towards any self-censorship or removal of bad content, and may network with any government of their choice to remove such content and keep it away from their computer. Public Content Network (PCN) participants are expected to develop a way for people wanting content to be removed to request removal of specific content, though such removal does cost time to review and that review time may be expected to be compensated for at a price agreeable to each broadcaster. If the content is removed then any review fee is expected to be minimal to the requester as any profit on such activity is considered hostile, so use of a mediator is encouraged. All participants both broadcast and receive content unless intentionally circumventing the system because broadcasting is essential to the well-being of Zeronet (ZNET).

Content Development:

Open Collaboration Incentives Summary

Original content creators are expected to be incentivized to provide valuable content to the public with awards, rewards, and donations. Those three incentive classes will all be a foundation for the Public Content Network (PCN). Participants are incentivized in ways that encourage providing value to both creators of original content works and the creators of derivative works they inspire or directly use. These incentives are expected to enable collaboration that provides high value to content developers as a whole. To this end, attribution and credit for content is expected to attach with to a specific relay of money streams to those people. When content is created, content creators may use the Creative Credit Cog (Service Cog:Web of Trust Cogs:Creative Credit Cog) to help assign credit to the appropriate content creators. Credited people, either participants or non-participants, are then expected to receive a portion of content money as directed by content creators. Open Collaboration Incentives is an improvement over Intellectual Property (IP) because it is a voluntary system. See Democratic Communication:Collaborative Development section for details.

Open Collaboration Protocol Summary
enables everyone to create or edit content in a group effort. Uses for this network could include content such as encyclopedia entries, educational information, historic records, news, and calculation or software development. Content is expected to be filtered to participants for any given effort according to their individual Web of Trust. The Open Collaboration Protocol is a platform that is expected to use the Public Content Network (PCN) to accomplish its objectives. This component might be an early focus so that other Zeronet (ZNET) components can be built using this component. See Democratic Communication:Collaborative Development:Open Collabortation Protocol for additional details.

Content Title
Word or phrase summarizing content description by content creator.

Content Title Hint
Word or phrase expected to summarize content by content distributor (or creator). Multiple hints may be put in order.

Content Service providers
are encouraged to provide automated recommendations to content creators during development of their content based on algorithms that scan their material.

Content Title Service
matches content with the best fitting title for that content. See Service Cog:Public Content Network Cogs:Content Title Cog section for details.

Content Lead-In
is when a Zeronet (ZNET) participant takes action to select content for download such as a click.

Content Lead Image
is an image displayed to indicate theme of content. The image itself may also have a title or caption.
Content Lead Image Hint
is an image expected to be displayed with title.
Lead Image Relative Map
The appropriate image to use based on an Avatar's topic interest map.
Relative Title Map
Title based on each potential topic of interest of a user.
Public Forum
Participants generally maintain control over their forum posts by creating public posts that may not published with a specific distributor (or website) in mind except perhaps their own Avatar Portal (ref Netportal:Avatar Portal). However, these posts may be designed to "tag" specific content as with Gab Dissenter as a comment instead of being designed as stand-alone content for their Avatar Portal. Forum websites are expected to be converted to forum portals, which are not entirely unlike a Usenet browser. Forum posts may share the same topic system as with other content and may be linked to a metastream service as with other content. The main challenge of Public Forum posts is organization of the posts and their replies. Different Public Forum portals act to organize these forum posts differently. A portal may furthermore distribute a post to multiple websites and harvest replies to Democratic Communication (DCOM) Plain Text Protocol (PTEX) (ref Democratic Communication:Plain Text Protocol (PTEX)) format. Public Forum posts are distributed as described in the nearby section "content pushing".

Content Distribution:
Broadcast Service
A service to ensure plain text messages are available for pull (download) according to contracted terms to a broad range of participants. Other Database Cog can provide Broadcast Service by adding these service features. Also see Service Cog:Public Settlement Network Cogs:Broadcast Cog.
Public Content Broadcasting Encouraged
All Zeronet (ZNET) participants are expected and encouraged to broadcast Public Content Network (PCN) content as a civic exercise of their freedom of speech. To this end, the default setting is to auction resources to the highest bidder on Zeronet (ZNET) without any restrictions on speech, though with a system that offers the possibility of paying the participant to review content for deletion requests of content deemed immoral by the participant. Upon first running of the app, a prompt may appear with checkboxes of content eligible to be deleted.
Zeronet Service Kit

A client-side software package designed to offer a range of Zeronet Services including Public Content Network (PCN) network services and Service Cogs (COG) (as a computer programming API) directly to participants for an expansive array of network access devices. The participant decides which components they wish to install from the pack so that Zeronet (ZNET) component independence is maintained.

Content Pushing

Participants may push (upload) static content to Zeronet(ZNET) by methods including Public File Storage Service Cog (ref Service Cog:Service Cogs and Cogs for Cogs:File Storage Cog), Broadcast Cog (ref Service Cog:Information Graph (Iggy), Database, and Search Cogs:Broadcast Cog), or more generally with Grexcog (ref Service Cog:Information Graph Cogs:Database and Search Cogs:Grexcog). Public posts and pulic forum announcements are expected to be routed to a Public Information Database see Information Graph (Iggy), Database, and Search Cogs:Public Information Database).

Content Discovery Cog

Participants who adding Zeronet(ZNET) content are expected to inform multiple content discovery services about the existence of their content. They are expected to select providers who are sharing and cooperative so that their content is advertised as widely as possible. See the associated Service Cog:Content Discovery section for details.

Content Marketing Service

are participants who help original content creators develop their works in ways other than the direct creation process. This includes distribution, work attributions, titling, captioning, advertising or marketing, reviewing, categorizing, and search tagging content.

Dynamic Content Distribution

Scripted and other interactive content is expected to be processed by an information system that connects together all Information Technology Resource Exchange (ITREX) (Ref Open Exchange: ITREX section) partners needed for content for distribution and delivery of interactive content. See Service Cog:Service Cogs and Cogs for Cogs:Dynamic Content Cog for details.

Browser

Netportal is the default Public Content Network (PCN) browser client to provide Zeronet (ZNET) participants expansive access to the Public Content Network (PCN). (Ref Netportal section for detail.)

Compression Cog

is a COG that compresses content to save internet bandwidth. See Zeronet (ZNET) Service Cog (COG) section for details.

Content Analytics:

Content Evaluation

Upon evaluation of content, all participants are expected to offer some sort of feedback. This feedback is expected to be relayed through a participants Data Negotiation Service (ref Web of Trust:Data Negotiation Service), which maintains participant privacy, to a Public Information Database (ref Service Cog:Information Graph (Iggy), Database, and Search Cogs:Public Information Database) so the evaluation is public. Then it is propagated through the Data Discovery and Synchronization (Disco) service (ref Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization) so the evaluation is discoverable.

Content Evaluation Feedback

Zeronet (ZNET) participant rating of content including any creator donation.

Content Review Service Cog

See Service Cog: Content Review.

Content Priority by Review

Content reviews are expected to be weighted by the participant's level of trust of content sources by the Zeronet (ZNET) Web of Trust client software and/or a Review Service Cog (COG), resulting in a net evaluation score for any given content. The highest rated content as weighted by trust is expected to be displayed prominently by the Metastream Service Cog (COG), while lower rated content if displayable at all, given client preference settings, may offer other content only as alternative information. Furthermore, new versions by the same content creators as those most highly evaluated may be assigned a predicted review score by a user's content priority service. For example, a participant may list their most trusted participant as "Storvan Mollymoo" and therefore any content reviewed highly or authored by or edited by Storvan Mollymoo would be the content displayed for the relevant query. For example, if Storvan Mollymoo composed content titled "The Nutcracker" and also referenced Tchaikovsky to be clear that it is an alternative work, the query would display the piece by Storvan Mollymoo first and may reference work by Tchaikovsky secondarily or not at all depending on the client preferences and Content Title Service Cog (COG) (ref Service Cog:Public Content Network Cogs:Content Title Cog) actions.

Content Evaluation

Content Rank

Currently, "Page Rank" is the leading method of information queries on the internet. This system is replaced in part by Content Rank which expects full transparency of ranking methods for all participants involved.

Private Content Rank vs Public Content Rank

First, content is ranked according to a selected Public Content Rank filter, which sets default rank. Then, the content may be reranked according to a

participants private filter. A limited amount of content is reranked because information inquiries may otherwise have too much data to process on the local device. Each participant determines the result set limit for any specific content inquiry. For example, if there are a million results for a "bridge building" query search, a person may only want to receive the first 700 search results which are then filtered on their local device according to their Web of Trust. In this case, the participant heavily trusts their search result provider not to unfairly bias the result set.

Disqualified and Ignored Content

Content evaluators are generally only expected to disqualify content from ranking if it is indecipherable given its alleged language and syntax or is off-topic. If the evaluator finds the content offensive, obscene, vulgar, insulting, malicious, slanderous, libelous, or otherwise insufferable, the evaluator is generally expected to mark the content as such and defer and decline a more complete evaluation according to their well defined set of content guidelines. So, such content isn't disqualified but rather remains ignored by the ranking participant. Summary information on disqualified and intentionally ignored content and the sources for such content is expected to be made publicly available. If participants object to certain content being disqualified or ignored, they are encouraged to form their own Content Evaluation service in which the content isn't disqualified or ignored.

Public Content Rank Factors

Citations

In replacement of "backlinks" are citations. Citations are like backlinks except in the same human-readable format as any other written citation. so, it works the same way as citing a source in common academic papers, but with additional options for more informal methods. Citations are expected to be in nearly all Public Content Network (PCN) content and affect the Content Rank of that content.

Certifications

Content Creator Certification

Content creators who pass some sort of qualification test are given higher default content rank for their content. However, this factor is expected to decrease as peer review increases. As an example, a participant could expect that creators with higher IQ have higher content quality. So, a content creator may earn a certification to pass an IQ > 119 test for a higher rank than unreviewed content by someone with an IQ 110

score. A participant could then set IQ certification as a factor to rank the content of certified creators higher in their metastream recommendations.

Content Quality Certification

The content itself has passed some sort of scrutiny, expected to be often before publication, and sometimes at the time of publication. For example, content claiming to avoid commercial branding references could pass through a review system which certifies it as avoiding references to commercial brands. Evaluating participants may be expected to grade the quality of the content according to objective and subjective metrics.

Review

Peer Review

Peer review data is expected to be satisfyingly objective by being based on formalized review systems by people considered trusted within their topic domain.

Public Review.

Reviews may be pre-planned (ref Web of Trust:Reviews) which may be paid, unpaid, or a collection of both.

Bond

Content creators may release content under guarantee with a participant expected to be independent. Content Review services could then offer a higher content ranking with the assurance it meets the quality criteria assured by the bond deposit.

Personal Content Rank Factors

Trust Rank

Information displayed on Netportal (ref associated section) is expected to be sorted in part according to the personal trust ranking of those participants. Highly trusted participants may have their information appearing at the top of information queries or metastreams.

Advertising or Postage Paid

Participants may be directly paid to review or evaluate content according to their contract with such advertisers and indicated by the participants Private Postage setting (ref Democratic Communication:Private Messages). When such a postage has been posted, these advertisers may be highly ranked on their information displays according the participants ranking preferences.

Content Cloud Clustering

Content is aggregated to a shared reference point such as in a public database which may have multiple sources of identical or nearly identical content. Sufficiently redundant content may be merged, aggregated, other

otherwise compressed in the stream in a process called content clustering. Content that is similar beyond a certain threshold may also be clustered. Generally the content predicted to have the highest value will be the displayed version, while other versions of the content would be displayed with additional user commands. An example of this service is two different content records with both titled "Hamlet the Movie" with and with audio tracks being indistinguishable at the human level though the records are slightly differently sized. While both versions may actually remain in some circumstances, content references are expected to be consolidated.

Content Translation Provider Cog

A service provider that converts content from one language to another. See Zeronet (ZNET) Service Cog (COG) section for details.

Value Exchange:

Push-Pull Balance for Content

Each participant is expected to be able to have a range of experience from entirely free content to entirely paid content. Each avatar of the participant is expected to be assigned a specific postage price where a message will be received and reviewed in order to receive a specific amount of money if the message isn't considered mutual content by the recipient.

Propagation by Value Exchange

is a system of exchanging content or messages where there is a value exchange based on the value of the message or content. Messages or content may be pushed to a person if they accept payment to view it, such as in commercial advertising where participants are paid to receive an advertisement, such as Paid Content (ref associated entry). Or, messages or content may be mutually exchanged as equal value where there is no net value exchange, such as in a personal conversation, called Mutual Exchange Content (ref associated entry). Messages or content may be paid for their delivery such as paying a news reporter for their report. This more directly paid for content is considered Payable Content (ref associated entry).

Push Content

"Supply-side content" is content sent to participants who expect average/net negative value from the content of the sender. People may expect negative value from sources such as advertisers, people seeking advice, propaganda outlets, unliked people, or other people they don't know or trust. Such content is evaluated in some way by participants in spite of this by receiving value either directly by being paid for receipt of the message or indirectly by any other means. Push Content is used to enable mutual benefit for both sender and receiver of supply-side content.

Push Price

Each participant may set a specific push price for each

of their Avatars. The push price may determine how much money they receive for advertisers to advertise messages in designated zones on the Netportal interface or at a position otherwise determined by a Metastream Service Cog (COG). Upon receipt of the content, the participant acknowledges receipt either automatically or manually as determined by agreement between the pushing participant and recipient.

Mutual Content, Peer Messaging

Users may expect approximately equal value from each other's content that are directed at each other. This would be content such as personal messages from sources such as friends, families, and co-workers. Despite equal value, it may be needed to attach a small postage fee that will be returned if value is acknowledged by the recipient. This prevents unwanted spam. Also see Democratic Communication:General Concepts:Private Messaging:Mutual Exchange Content for more details.

Pull Content

"Demand-side content" is content with expected positive value from specific content sources. People may expect positive value from sources such as philosophers, expert advisers, journalists, teachers, consultants, authors, entertainers, musicians, performers, and councilors. Participants may pay for such content, so Service Cog (COG) providers may be paid to offer ways to match participant's content demands to the content expected to be the most wanted according to the preferences of the participant, which is likely to focus on the donation history of the participant.

Advertising

Content may be integrated within specific data sets as advertised under specific terms as expected to be contracted with the Data Negotiation service (ref Web of Trust:Data Negotiation Service), Topic Search service, and other services supporting targeted advertising. Paid rank is expected to be marked as sponsored. It is considered hostile (and typically a contract violation) to attempt to remove these integrated sponsored results because participants are expected to pay less for Content Evaluation service (ref Content Distribution:Content Analytics:Content Evaluation) which incorporates advertising. If participants want advertising-free results, they should specifically pay the content creators, in cooperation with service providers, to avoid including those results or otherwise use a Content Evaluation service who offers reduced advertising or no advertising included with the service.

Donation Revenue Stream

Zeronet (ZNET) participants are expected to give content they value a certain amount of money based on their rating of the content and their targeted level of donations over time.

Donation Relative Awards

Participants assign from a pool of possible award tokens

with each additional token having several times higher value. The value of all available tokens will increase or decrease over time depending on how much is awarded so that the user can use higher level awards more frequently despite a limited award pool. Each award has an expected frequency of awarding based on how often the user evaluates content. More valuable awards are expected to be issued more rarely. The number of different awards grows the more frequently the user evaluates content and shrinks the less frequently the user evaluates content, and also grows or shrinks based on how much donation funding remains. The user client will provide ongoing feedback to suggest reducing or increasing the frequency of any given award so that awards are distributed normally.

Donation Absolute Awards

Zeronet (ZNET) participant donates to a content source directly upon evaluating the content. Users that may have a higher level of donations available can provide additional rewards by using tokens that are assigned a fixed value such that their account automatically adds from a relatively large pool of funding. So, a donation triggers an automated addition to their reward pool.

Token Pledge

A donation using a donation token that is packaged with others because the transaction fee would otherwise be below a desired threshold.

Dissent

Dissent may occur where there is a perception that the value of certain content is negative. The content is expected to be marked for scorn so that similar content will no longer be received, or "monitor" so that similar content is more likely to be received even though it has negative value. Scorn is an alternative to "thumbs down" and "downvoting" options which can sometimes be found on social media traditional websites. Dissent includes the concepts of disagreement, scorn, rebuke, refute, admonishment, and centure. Dissent is different in this context from disliking.

Traffic Reporting Incentives

For each mode of content revenue, accurate traffic reporting incentives are different because they reflect different benefit types. Content creators have the strongest value for accurate content traffic measurements. For impression-based ads, content providers may want to over-report their delivery of impressions. Users may want to over-report their usage of favored content providers, or under-report to avoid payment. For donation-based content, there is little incentive to provide false traffic data by any party.

Focus Points (FP)

Summary

Focus Points (FP) are a decentralized alternative to central registries like the "InterNIC" registry. To get

Focus Points (FP) as described, sacrifice money to a Focus Portal (FP) while publicly stating the purpose of the sacrifice, and this money is considered to be destroyed in the Focus Portal (FP) as an alternative to paying a registry. This system is used to register internet address and associated reputation information for peer-to-peer communications, as well as register organization offerings. This model of registration is designed to decrease the ability for large registrars to charge high profits for listings by shifting from supply-side to demand-side incentives. This is a collective system by which the people who have been effectively transferred value by that sacrifice to cooperate in agreement to take notice of these entries and consider them valid. Instead of participants paying to be listed in the registry, participants pay registries to discover and list all publicly available listings. Focus Points (FP) are expected to be a factor for the Web of Trust system using absolute numbers assigned in a similar way to trust in the Web of Trust though are considered secondary for consideration as they are purchasable. Points are honored by participants in reinforcement of favorable content or behaviors or discouragement of bad content or behaviors. Focus Points (FP) may be distributed or re-distributed by each participant to each other participant according to their opinions of how much attention to each other participant is warranted. Focus Points (FP) are a factor that generally determine how much attention will be made available by a participant for the content of other participants. So, this registration helps determines the information sources displayed on Netportal.

Negative Focus Points (FP)

Participants may also pay attention to what opponents are saying by assigning negative focus without having them displayed highly on the Web of Trust. People’s focus points are used in compliment to Web of Trust rankings. Because they amount to a personal identity fingerprint, they can be kept private. So, if you want a system to focus on what people including friends, neighbors, allies, and opponents are doing or saying, the Focus Point (FP) system meant to be a good option. This is a system that should be usable both real-time and time-delayed.

Focus Portal (FP)

Casting digital money into the Focus Portal (FP) acts as symbolic proof of commitment toward that stated purpose. Casting to the Focus Portal works as registration, advertisement on Zeronet (ZNET) for a point of contact, advertisement for a commercial offering, or any other information. An important thing to understand is that technical destruction of such money actually does not do economic damage but is ultimately a transfer of money from one person to others. The Zeronet (ZNET) Focus Portal (FP) is an object to which money (and any

attached virtual content) is sent specifically to be formally voided. This is done in such a way that the destruction of the money effectively sends the value of the destroyed money proportionally to all other participants who have money (of the same issuance source) which has not been cast to such a portal. This is expected to be done to increase attention to specific participants or content. This information is used by Zeronet (ZNET) data service providers to influence the information provided (according to the request of the information recipient), in the way the participant requests it to be adjusted. Generally, a "best" money is picked by participants, and its voiding feature is used to destroy the money while referencing the purpose of the sacrifice. That money is then permanently destroyed, while all other holders of the money gain a proportional value according to their money holding on average and all other things being equal.

Focus Portal Sacrifice

Money sent to the Focus Portal (FP) determines a number of Focus Points (FP) granted when the voiding action is designated as being for Focus Points (FP). That amount is then adjusted by each participant according to their Web of Trust. These Focus Points (FP) work on an honor system by which there is collective agreement that the Focus Portal (FP) is a way people effectively donate money to others by sacrifice, because all other money holders of that money proportionally (on average) benefit according to their money holdings of that type at the time of the donation. Focus Points (FP) are dedicated to a specific purpose. However, some purposes allow them to be redistributed in various ways if subsequent additional token or otherwise minimum amounts are sent in additional sacrifice to the Focus Portal (FP). Focus Points (FP) are expected to be controlled by a public key. Messages originating from a "public" signature key specified at the time of the sacrifice may act to direct or redirect (with an additional portal donation) the Focus Points (FP). In exchange for the donation (or simple honor of the money system used), these points are listed in a contact directory by stakeholders of that money.  Participants may also request higher consideration for an internet search to match with a specific result according to the direction of the Focus Points (FP) instructions referenced when the money is voided.

Focus Registrar

Zeronet (ZNET) registrars form public access registries. The focus of these registries will be contact information and offering information (offerings include goods and services, including public information), but registrars can register anything they wish. Registrars are expected to be paid directly by participants to list all submissions that match given conditions. Registrars can be easily created by any Zeronet (ZNET) participant.

Essentially participants simply make a contact list, offerings list, or other listing public and then sell it.

Registrar Listing

The Focus Points (FP) system may be used to create a contact directory. To accomplish this, registrars (which are expected but do not necessarily need to be formed as Service Cogs (COG) help match avatars to Contact Keys. Each registrar will set a minimum Focus Points (FP) for achieving a listed status. All participant on Zeronet (ZNET) have the option to list their (or anyone's) contact information in the registry. This system is designed to reduce the incentive for registrars to compete with each other since the Focus Point (FP) system changes registrars to a pay to list service like "white pages" instead of pay to be listed service like "yellow pages". Both the number of focus points and the Web of Trust resolve listing conflicts according to the participants preferences since anyone can list any information with the registry.

Registry Threshold

Minimum Payment Threshold for Network Registered Contact Query Registration. All registrars set a minimum fee of their choosing. Registrars charge users to see query results on a per query basis. Registrars don't directly receive any money from listed contacts. Rather, they register all queries where the minimum Focus Points (FP) are sent to the Focus Portal (FP) as if they had received the money them self for that purpose. Generally, the registrar with the lowest registration fee will be dominant all other things being equal because its a commodity service. However, this isn't entirely true. Name spammers could register names in mass taking names that are not actually used if registration fees are set too low. Factors for registration priority are expected to be first to register and highest registration payment. Some registrations may require registration name to be unique, while other types of registries may list multiple entries for one name.

Registered Contact

Each network participant is expected to purchase a threshold amount of Focus Points (FP) to consider their avatar (or "real" public identity) a registered participant on Zeronet (ZNET). Since people pay to access this list, its up to the Web of Trust honor system to have Service Providers that provide access to lists of registered contacts. Being registered will cause more default honor since registered participants are less likely to be spammers.

Search Query Influence

Focus Points (FP) may be used to determine how highly a search match may rank for a certain query according to directions of searchers. This is especially useful for commerce including shopping. The proportion of points this entity has relative to all other points designated

as Search Query Influence determine their share of influence. So if someone were to acquire 1% of all honored Focus Points (FP) directed to be used as search query influence, they would have a 1% influence score for the match. The search query influence then maps to the Information Graph (Iggy) nodes which the point donor wishes to create matching content.

Search Rank

Metastream Service Cog (ref neighboring section for detail) servicers are expected to rank results according to their definition of how likely a person is to donate to a the content they stream given the context of the query. However, people may want to know what a commercial marketplace has to say such as when they are making a purchase. In that case, they may want people to have a chance to advertise. This is a setting where people specifically want paid results to appear in place of unpaid results.

Focus Query Service Cog

See Service Cog:Public Content Network (PCN) Cogs (COG):Focus Query Cog.

WEB OF TRUST:

Summary

See Zeronet:Summary section for an overview of the Web of Trust.

Primary Trust Types Summary

Topic Domain Trust  A participant is trusted as being educated or passionate about a specific topic.

Performance Trust  A participant is trusted as being reliable and skilled.

General Trust  A holistic trust consisting of topic domain trust, performance trust, honesty, loyalty, virtue, valor, faith, and other trust.

Trust Rank

Trust rank is general trust information used as a foundation for controlling most Zeronet information flows, including information display, access permissions, and resource distribution. Participants will be given a range of ways to accomplish this focused on ranking participants from most to least trustworthy. More trusted people are granted more control and influence than less trusted people. Each participant is fully responsible to independently determine who it is they wish to trust. Participants rank who they generally trust from most to least. It is encouraged to select and rank at least five other participants to begin using Zeronet (ZNET). It is considered beneficial to rank 30 participants they are already familiar with.

Subject of Trust, Who to What

Trust isn’t only to specific people, but also to the specific information of those specific people. People are expected to either author what that specific

information is them self or link to others who establish what that information is. Encouraged information expected to be included are behavioral governance protocols based on expressed virtues and values, communications and records sharing protocols that enable Zeronet (ZNET) to function, and references to information providers. This is Explained further in the Trust Garden section.

Domains of Trust

After trust is assigned to specific people and specific information providers, it can be furthermore filtered and displayed according to how much each person or group is trusted from those information providers on specific topics. So, anyone is expected to be able to provide information from each Zeronet (ZNET) information provider, but that information will be filtered according to how much each person is trusted regarding different topics. So for example, medical information from a trusted doctor would be expected to be displayed more prominently than medical information from a trusted accountant. This is explained further in the Types of Trust section.

Perspective Development Summary

Zeronet (ZNET) operates efficiently when there is a consensus of a shared perspective, which participants are encouraged to develop by uniting under shared perspectives. (Ref Web of Trust:Trust Garden) for perspective formation methods.

Information Sources

All information sources are considered a person in the Web of Trust even though multiple people may collectively publish information as one Zeronet (ZNET) avatar. So, public identities are expected to be sources of information from both specific people and collectives.  "Public" encryption writing or signature keys are all expected to be linked to one single avatar, and that avatar and public key are considered part of the same identity. See the Democratic Communication section for encryption explanations.

Privacy vs Decentralization Challenge

The Web of Trust involves trusting others in many ways including usage of some of a participant’s resources. So, a challenge for Zeronet (ZNET) privacy is the ability to decentralize a Web of Trust while enabling privacy. It’s a challenge because the more we know about someone, the easier it becomes to verify their claims. However, information about others is restricted for privacy. Additionally, we have limited resources in which identities, transactions, and other claims can be verified.

Evaluation Challenge

Evaluation of content is done to validate information. Participants are not all expected to evaluate every bit of content on the internet for validity. So, participants delegate trust to other participants to

help evaluate content which they don't evaluate them self. This delegation process determines how dependable the information they are provided can be.

Evaluator Participant

Any participant who is trusted to evaluate information for accuracy or compliance with a specific protocol.

Primary Source

A person with direct sensory access regarding a specific experience. The most accurate information originates from a primary source rather than a person who simply learned information from communications with another person.

Foundations for Trust:

Core Trust Foundation

Emancipated participants are responsible for their own beliefs. They are expected to trust their own senses to determine the most trustworthy information. Caretakers of unemancipated participants are responsible for ensuring their access to trustworthy information.

Declared Philosophy

Participants may declare loyalty to a set of virtues, values, morals, and ethics. This declaration may be used as a beginning point for trust development as further detailed (ref Perspective Development:Web of Trust Garden:Trust Garden Seed). Conflicts of core interests may result in conflicts of trust. Loyalties may be undeclared for people who are remaining anonymous, but this may change the perspective of trust by other participants and the related information views. People are encouraged to form and reform agreements of philosophy with others for strength of unity.

Trust Source Information

Trust source information includes public claims and public evaluations (including reviews and ratings). Trust may be delegated many ways which are all able to provide a perspective of information.

Trust Information as Honor

Content and participant evaluations (including reviews and ratings) are used as trust information to help determine honorable behavior of participants and reliability of information. Participants are expected to be provided with critical trust information when being supplied with their Zeronet (ZNET) software. References to trust-sensitive services including Data Discovery and Synchronization Service (Disco), Group Trust and Synchronization (GTS), and Contact Discovery Service (Cdisc) (which are all explained in other sections) may be provided. These references are then used to acquire trust source information. Public information such as from Public Information Database (see associated section) services provide such data as public reviews are not expected to determine accuracy of any data underlying the references submitted to them. Instead, they simply store the information according to

marketplace supply and demands, and according the the contracts they are party to. Instead, it is the task of all participants to actively contemplate information accuracy, and the task of Trust Cohesors like a Group Synchronization and Trust Service (GTS) (ref that section) to help them do so. Reference: Network Synchronization:Data Discovery and Synchronization Service. Service Cog:Information Graph Cogs:Database and Search Cogs:Contact Discovery Service (Cdisc).

Honor and Trust

Honor is expected to lead to trust. Honor is recognition of behavior that is done according to a set of virtues, values, morals, and ethics deemed to be good. Trust is expectations of future behavior to be done according to such a shared philosophy. Honor may establish trust. The degree to which honor establishes trust is good faith as faith in benevolence. If a participant believes another participant has behaved honorably enough to trust them in some way, they are encouraged to formally trust the other participant. This would then lead to joint participation on Zeronet (ZNET) in at least some small way. This is expected to start as a "seed of trust" (ref Trust Garden) and grow over time.

Types of Trust:

Trust Domain and General Trust

Common types of trust are expected to be listed in the Information Graph (Iggy) (ref that section for detail). Expected trust domains include Performance Trust, Financial Trust, Topic Knowledge Trust, and Social Trust.

Trust Delegation

Each trust domain may delegated differently for different purposes. All trust domains are expected to form a perspective for viewing information provided by the trusted participants. Trust delegated broadly is expected to be used as a general filter of information, while trust delegated specifically is expected to be used as a specific filter of information. So, if someone trusts a specific topic expert, their information is expected to take precedent unless a person they also trust, but only generally, has also offered information about that topic, in which case any information conflicts result in a more detailed comparison of trust.

Performance Trust

Performance Trust is a domain of trust regarding avatars who commit to performing a service, task, or other personal commitment. Performance trust consists of factors including transparency and reliability. Being on time is part of performance trust. Doing jobs well is part of performance trust. Completing tasks in reasonable time or the time expected is part of performance trust. Admitting one’s mistakes and discovered risks is a part of performance trust.

Financial Trust

Financial Trust is the reliability of a person when

they commit to providing value in a certain time, handling other people's possessions carefully, treating other people's possessions well, and any other financial reliability. This is another trust domain expected to be common. Financial trust is considered a type of performance trust.

Topic Domain Trust

is a topic paired to a domain of trust, where a person or group is trusted based on assessment of expertise or participation in a specific topic. This type of trust can be a shared passions for networking together. Each topic (in the Public Content Network (PCN) topic map on the Information Graph (Iggy) ) has a set of participants who publish content to that topic on Zeronet (ZNET). Each topic has an associated Topic Knowledge Trust Domain. Trust not delegated to a specific topic is by default assigned to the "Topic Cluster" of that Topic Domain. (ref Public Content Network:Topic:Topic Cluster). If no topic cluster is assigned then by default the most generally trusted participant as designated "most knowledgeable" or "most factual" would be delegated the most trust for the topic.

Social Trust

Social Trust is a domain of trust where a person trusts someone due to life experience such as where a son trusts a mother, a friend trusts a friend, and a neighbor trusts a neighbor. This should not be confused with performance trust. Social trust consists of personal judgment factors including honesty, forthrightness, virtues, ethics, morals, civility, sincerity, helpfulness, generosity, courage, and factors like these in a context of trust may be summed up as integrity. This sort of trust involves trust in the ability to keep secrets, offer help when needed, adhere to civil pledges, and maintain loyalty when loyalty is tested. This is considered in addition to the other trust types to form general trust.

Control Domain

A control domain sets specific resources to a specific trust domain as a specific person or group. Based on a trust domain reflecting different strengths and weaknesses of different participants, authority over resources, such parts (or all) of a participant's computer for example, may be delegated to other participants. Successful delegation depends on people in control of resources maintaining agreement with contracts as agreed maintain in good faith. Computer resources include files, records, processes, and applications. So a trust domain is also a control domain when resources are linked to the corresponding trust domain.

Public Trust Reporting:

Summary

Zeronet (ZNET) relies on public performance reviews (as

detailed in Review section) to determine many to most interactions. Performance reviews for most contracts and purchases are encouraged to be done in a formal way such as according to the Web of Trust review systems. Those formalities are expected to help with fairness and effectiveness. Public Performance Trust is expected to be used to evaluate a participant's reliability with commercial contracts as honor. While some direct social trust information is expected to be made available, it is partially discouraged from from consideration in trading exchange contracts because it is considered less reliable. Social contracts can be formed in ways that allow for more formal performance evaluations, and so under a formal system designed to avoid discrimination and "the court of public opinion", social trust information may be used in limited ways in addition to other trust information in forming Zeronet (ZNET) contracts.

Public Performance Trust Reporting

Each avatar is encouraged to publicize important contract information and publicly review performance of those contracts. This helps others on the network decide who is trustworthy on the network. Contract evaluation is expected to be done in public that gauges transparency and reliability based on suggested metrics for the type of contract. See the Review section for more information about contract evaluation.

Public Social Trust Reporting

For nonorganizational participants, most personal trust information is expected to be kept private. Personal information is expected to be shared with considerations for personal privacy. For public organizations, many actions of the organization associated with their trustworthiness are expected to be shared in public. We encourage forming social contracts which can then be judged as a formal social performance trust measure. So, we only encourage public reporting of social trust information as part of a performance metric formally agreed to by the participant. This allows clarity of what personal integrity issues become matters in the public domain. That formal system leads to less rumors being accepted as fact. When social trust information is expected to clearly reveal an avatar's underlying personal identity, it is generally expected to be named using a participants recognized public "real" name (as assigned by parents). So, an avatar may be designed by a participant to reflect the person's public identity, which may be accompanied by an up-to-date profile photo. The exceptions of privacy (with or without a contract) would be for physical harm on others or otherwise as defined by illegal acts of violence by someone's philosophic perspective. All other social information should be shared only with a confidentiality agreement.

Rumormilling Avoidance

In a society that allows free speech, slander and

libel become serious problems for which the responsibility is fully duplicated to "believers" as much as the liars. It is as bad to wrongly believe a false rumor as to start the lie, because you are cooperating with liars and helping reward the liar for telling the lie. Judging someone informally in ways that cause lost opportunities for the victim is damaging. Spreading a rumor later found to be false is expected to result in dishonor for the rumor spreaders. We encourage confrontation of all Primary Sources (ref that section) involved in any accusations of wrongdoing. While social trust is just as important as performance trust, converting this information into a "social credit score" may be disrespectful of privacy and risks unwarranted ostracism of participants by the ’court of public opinion’. "Social Credit Scores" are less objective metrics and more like a gossip column for rumors. We encourage more formality than that as a basis for Zeronet (ZNET) activity while discourage Rumormilling.

Perspective Development: Web of Trust Garden:
Summary
Trust Garden is a recommended method of visualization (as a metaphor) for identifying shared goals and information that help determine trust for a participant. The Web of Trust is expected to be unique and controllable for each participant based on who they trust, and the Trust Garden is one of any number of Zeronet (ZNET) information screens that help participants decide who is most and least trustworthy. This section refers to Crosslink Metacodes (ref neighboring section) which are a more formal version of this concept. A trust garden enables a shared world view about a specific topic, which begins shared by as few as two people, but may encompass every participant upon consensus agreement. A trust garden can be formed as a public perspective or a shareable private perspective.
Metacode, Crosslink, Crosslink Metacodes Summary
A metacode is an unique identifier tag for a record or record set, as a string of letters and numbers, functioning like the name of a record, that is a reference to a collection or record of information. A crosslink is agreement with others regarding the collection of information represented by the metacode. The agreement may be on who the author is of information is, whether it is accurate, what database the information is part of, and so on. When a metacode itself is used to represent such agreement as a crosslink, it is a crosslink metacode.
(ref Network Synchronization:Crosslink Metacode).
Trust Garden Seed
is a complete philosophic perspective of a specific person expected to include any of their declared virtues and values, which would be well to include definitions

of many words of that philosophy. Reference (Caroasi:Rainbow Cooperative:Philosophic Perspective Matching) for ideas for ways to form bonds based on Philosophic Perspective. A Trust Garden Seed philosophy is expected to be a well detailed written proposal which can be agreed by others. The agreement can be basis for a trusting bond with other participants. For Zeronet (ZNET) beginning Crosslink Metacodes (ref Metacode above) can be considered trust garden seeds. Everyone is expected to have a unique perspective and encouraged to share their perspective in writing as a trust garden seed.

Trust Garden Taproot

Each time someone shares a sufficiently similar philosophic perspective to consider networking together, and someone else approves of that perspective, a Trust Garden Taproot is formed in a first step to forming consensus. The shared perspectives may be merged and summarized as an agreement. Such agreements can be even be formed on single issues where people are otherwise in disagreement on other issues. These Taproots as partial or complete seed crosslinks (ref Crosslink above) can be used to strive to form network agreements such as by sparking discussions. So the Taproot is at least partial agreement with a philosophic perspective. A Taproot is expected to be created with expectations of forming consensus with others for Zeronet (ZNET) core network development, and the complete philosophic perspective as the Trust Flower seed(s) from which it formed is encouraged to be made public enabling people to see the points of disagreement in addition to the points of agreement. Where a participant is in partial but not complete agreement, they are encouraged to also reference Trust Garden Seed showing points where there is disagreement by writing their own alternative philosophy under an identical topic heading.

Trust Garden Rootbranch

is broad agreement with others on multiple philosophic principles including virtues, values, ethics, and morals, and their application to governance of personal behaviors, shared with another participant. After that agreement, adopted communication methods as protocols, contracting methods, and a governance model together for foundation of social cooperative development. Agreement on communications protocols and governance which are encouraged to be based on a specific philosophy. Public agreements with trusted participants include social governance agreements such as agreement to honor intellectual property, and public individual contracts of exchange. This may be formed as a social contract, a world view, or a named perspective upon being given a name. With Zeronet (ZNET), this may be summarized with an identity as a set of agreements as a Crosslink (ref nearby) as a Rootbranch Crosslink and forms a "trust group".

Trust Garden Stem
: Participants form agreement on formatting of information such as to news articles, posts, and social media such as for sharing on the Zeronet (ZNET) Public Content Network (PCN). Data stream formats, including databases of such information, established and developed to protocols by a specific Trust Garden Rootbranch (ref nearby section) are formed as a stem. So, agreement to accept specific format(s) of publication is a Stem Crosslink. Content and records as a shared database entry may then be created to the agreed protocols. The Trust Garden Stem is a key selection for each Zeronet (ZNET) participant as the selection of a Trust Garden Stem determines the information that will be available on their Zeronet (ZNET) browser. Participants may have multiple Trust Garden Stems linked into their Trust Garden. These Trust Garden Stems are also what makes Zeronet (ZNET) portals (which replace websites) possible.

Trust Garden Stembranch
: For Zeronet (ZNET), jointly accepted database (record set) identifiers (as stem crosslinks and/or metacodes) typically refer to a specific database such a a Web of Trust database for an avatar profile. Such a Stembranch Crosslink means that specific data as ready to share is considered part of Zeronet (ZNET) by the participant. The "crosslinked" data set may be referred to as a "Database Stembranch". So, the top-level information layout is a Stembranch topic, which could include Group Records Exchange (GREX) database structures, while the underlying streaming protocols such as TCP/IP are the Stem topics.

Trust Garden Petal
: Content contributions by individuals to a specific stembranch are each considered a Trust Garden Petal. This may be represented and identified with a metacode (ref nearby) on Zeronet (ZNET). Each public agreement with another Zeronet (ZNET) may also be represented as a Petal Crosslink. A Trust Garden Petal public profile information is expected to include any avatar profile information a participant wishes to be public.

Trust Flower
: is a reference to a specific stem,its associated stembranches, and "petals" of data from individuals adding to a complete data set for an individual. It could represent a perspective of Zeronet (ZNET) which could be considered complete, or include the information of many organizations to be a complete perspective of Zeronet (ZNET).

Flower Patch
: As outlined by (Caroasi:Rainbow Civics:Hierarchy of Unification:Perspective Unity Development), we encourage development strength in numbers by forming and joining organizations with joint missions and joint resources. A Trust Garden Flower Patch is an organization formed by developing Unity of Values and Vision, and then

agreement to contribute resources as a Unity of Resources (ref associated sections). Each flower is encouraged to help development of strategies and tactics for advancing organization missions. Participants are expected to form cooperatives based on their perspective. These participants then split and join with such cooperatives fluidly as they feel best suit their goals. These organizations are encouraged to do so as Rainbow Cooperative organizations (ref Caroasi:Rainbow Cooperative). Any group databases which are all crosslinked together (ref nearby) by people by such cooperation is considered a "Perspective Database". These organizations may be formed as Trust Groups (ref neighboring sections). A flower patch is comparable to a group in the Zeronet (ZNET) Group Trust and Synchronization (GTS) service.

Trust Garden

Flower Patches may bond together as an alliance reflecting people and organizations in cooperation as needed to achieve the necessary 'critical mass', for accomplishing goals that can be easily accomplished with strength of numbers and strength of organizational alliance. One expected result of such an alliance is jointly creating databases or set of databases according to a specific social contract, world view, or named perspective (ref nearby section).

Seed Bank

is all trusted information about a specific person or group of people such as a formal organization, including agreements created with that person. For Zeronet (ZNET) this information may summarized as metacodes (ref nearby).

Perspective Development: Establishing Trust

Zeronet Perspective Uses

Perspective Development for Zeronet (ZNET) is important to filter information including topic searching, metastream feeds, collaborative content consensus, open exchange listings, and validations or authentication of records or information of any kind such as contact information, financial records, public events, and so on.

Trusted Perspective, Perspective View

A participants trusted personal perspective view, as one of many possible "named perspectives" of Zeronet (ZNET) may be developed with cooperation with other participants, and such cooperation may help determination of Zeronet (ZNET) network consensus. A trusted perspective may (but is not required to) be shared by each participant avatar. For each participant, each topic domain (see associated section) will have a dominant perspective which may be different from one participant to another based on who they trust for information on those topics. Having different trusted perspectives for different avatars may help a participant become more anonymous. Trust Cohesor

participants may help with information filtering and sorting, result set prioritizing, data filtering, conflict resolution, Competing Perspective Consideration determination, and accuracy assessment so that more trusted information sources are pulled (downloaded) or displayed before less trusted information sources.

Participant Identities

Participant identities are essential for a complete perspective on Zeronet (ZNET). Participant identities are listed in an identity table which matches identities to encryption keys for Zeronet (ZNET) communications. Upon being contacted by another participant for the first time, their Web of Trust Identity Table (ref Zeronet:Democratic Communication:Identity Table) may be referenced or queried to discover information about a participant. Using Search Service Cog (COG) and other Zeronet (ZNET) components, the avatar profile and reputation information is pulled and may be displayed in various circumstances according to preferences. This information may be used in conjunction with the SigilX system (ref Service Cog:SigilX) to match name(s) personally given to a person with their public names for communications with others.

Trust Rank List

An ordered list of identities sorted by trust rank. This list determines content display and helps establish Zeronet (ZNET) security for the participant. Zeronet (ZNET) participants may rank public identities as a source by who they trust and distrust the most to the least. By default preferences, the top of the list shows the most trusted identity, while the bottom of the list shows the most distrusted identity. Ranking may also be determined according to the reviews participants apply to content. Participants regularly rate content, which assigns a certain amount of honor as public Honor Points (ref nearby section) to the authors. This is expected to be referred to as both the trust list and trust rank.

Self Trust

People may trust them self less than others. Be default, self-trust is at the top of the trust rank while the person who supplied the Zeronet (ZNET) software is ranked second. No other names are expected to appear until added by the participant.

Honor Rating

Honor Points are an important public factor in trust ranking for both participants and their Trust Cohesors (ref Caroasi:Rainbow Cooperative:Ringer-Cohesor-Guider Model:Cohesor). Each Zeronet (ZNET) identity as an avatar is expected to be assigned numeric value(s) called "honor" to determine the weight of their trust which may be a positive or negative number. Trust may be determined by awarding honor points to people for specific behaviors of virtue or value, often correlated to performing well for a specific contract of behavior. Honor may also be subtracted and become negative (as

dishonor or shame) under circumstances such as publication of bad information. See further information in the Honor Assessment section.

Honor Distribution Table

An honor distribution table lists how much honor has been designated to each identity by the participant.

Trust Group

A group of people who explicitly trust each other by formal declaration for adding records to a database in a specific form according to a specific protocol is a trust group. Each group offers a shared perspective regarding a specific topic when collecting all their provided records into a database. This is metaphorically stembranching (Ref Trust Garden in neighboring section) and done formally as crosslinking on Zeronet (ZNET) (ref Perspective Development:Network Synchronization:Crosslinking).

Trust Group Leader

Trust tends to cluster around specific people which may be people such as organization leaders, commentators, "authority figures", specialists, cultural icons, celebrities, or other popular people or group leaders. These most trusted people are expected to be considered lead content editors on the Public Collaboration Network (PCN) because their content will be the content expected to be displayed because of their trust rating.

Information systems using the Web of Trust system will tend to have developmental framework boundaries around such web of trust clusters because these people will have enough of a following to influence the protocols and network behavior. In other words, Zeronet (ZNET) may be a fundamentally different system for different groups of people when consensus is not equivalent to unanimity.

Trust groups are expected to correspond to specific topic domains or topic clusters (ref Public Content Network:Topics:Topic, :Topic Cluster).

Perspective Matching Philosophic Perspective

The first encouraged activity as part of Zeronet (ZNET) is to form a Philosophic Perspective upon which participants can have a basis to trust each other. See Rainbow Road:Caroasi:Rainbow Cooperative:Philosophic Perspective Matching for a beginning point of discovering how to initiate relationships of trust with others. Perspective matching is a very large part of whether someone can expected to be trusted.

Trust Starting Points

Starting trust includes trust from being a person such as proof of address, proof of being human, etc. Starting topic domain trust can come from participation in discussions on a specific topic, having a video channel, testing events where a certain score is needed including topic domain certification, and many other such participation in events. Starting performance trust can start with reviews and ratings from other trusted people, performance certification. Social trust can be

according to cultural norms, so starting with family bonds and expanding outward to others. If an avatar is being operated by a bot (of a "bot farm"), they are expected to identify as such as considered an extension of another person as a "bot farm operator". This expectation is because bot farms may be considered unfair monopolistic leverage, especially in voting systems. Children are expected to be identified as such to avoid contract conflicts and apply social or cultural expectations like asking permission for interactions.

Reciprocal Delegation Trust Group, Decentralized Organization

Trust first flows "up" to delegates, who then redelegate authority "up" to any number of delegation layers. Delegates then assign trust laterally to people trusted by others, including the delegate, for the same mission or purpose, with compatible virtues and values, forming the organization. Finally, delegation flows "down" to participants as leadership. (ref Caroasi:Rainbow Cooperative). This form of trust group forms Zeronet consensus including for official Zeronet organization. This is considered a decentralized organization because authority begins spread among participants, even though it may be consolidated for some to all organizational actions depending on negotiated agreement.

Trust Reports by Cohesor

A cohesor is someone delegated in part to help determine who to trust and how much to trust them. Trusted people may act as cohesor by forming trust reports that may be further redistributed by a participants other trusted cohesors (ref Caroasi:Rainbow Cooperative:Ringer-Cohesor-Guider Model:Organizational Role Distribution (RCG) Overview:Cohesor).

Competing Perspectives

In addition to trusted crosslinks (ref nearby section), a participant will be expected to monitor distrusted crosslinks and use them as a source for some Competing Perspective Consideration content (ref Netportal:Competing Perspective Consideration) for details. Participants are encouraged not only to evaluate popular information that has broad consensus, but evaluate unpopular information because the "wisdom of the crowds" is not always correct.

Offering Trust Group Participation

Contact the Trust Group and offer participation to initiate participation in the Trust Group.

Invite Participant to Trust Group

Possible starting points for trust are at (reference Zeronet:Web of Trust:Perspective Development:Establishing Trust:Trust Starting Points). Declare trust to a participant and request a declaration of mutual trust to someone in the Trust Group.

Perspective Development: Honor Assessments:

Implied Trust

Implied trust is relayed trust such that when someone you trust in turn trusts someone else, and then you trust that person more as a result. This creates a second tier of trust. That second tier creates a third tier and so on. Be default settings, implied trust is never more trusted than directly rated trust. Implied trust is weighted by rank. So, your most trusted person assigns maximum implied trust while your least trusted person (though still a trusted person, not a distrusted person) assigns the minimum amount. Distrusted people do not have an impact on implied trust. The amount of specific quantified trust is arbitrary but could be based on the a golden ratio such as 38% (which is 1 - 0.62). So, if one using direct trust to loan someone they trust 100 silver coins, they may be willing to loan someone they don't trust directly but is trusted by their directly trusted person 38 silver coins with a guarantee from the trusted person to cosign the loan. This can be used different ways by Zeronet (ZNET) trust groups such as allowing indirectly trusted people to add information to a database without explicit approval by a central participant as described in neighboring sections.

Implied Honor Score

Participants are provided with a suggested way of assigning honor scores to everyone in their contact list. However, they may change this scoring system by editing honor score settings. Where the participant designates a certain number of total honor points by assignment to a specific avatar, that information is then used to be able to consider all manually unscored participants. For for example, if everyone is unscored, and furthermore if a score of 50 is assigned to the fifth person on the list, then everyone above that person will be assigned an implied honor score of above 50 while everyone below will be assigned an implied honor score below 50. So, there are two different honor scores for each Zero Network (ZNET) participant. There is the honor score and also implied honor score. Implied Honor is automatically assigned while scored honor is directly assigned.

Scored and Ranked Honor

Some avatars are added as directly scored with honor points, meaning their trust depends on objective metrics that are measured and directly or indirectly assigned according to a participant's custom scoring system as they set in their Web of Trust settings. For new Avatars that have been added by honor scoring, they start at the bottom of the list and work their way up the list.

Avatars may also be added directly as ranked avatars by being inserted into the trust list to a specific list position. Each Zeronet (ZNET) participant may adjust the trust system to their own preference, so custom ranking options may be available. Directly ranked avatars will be ranked above scored avatars that have been added

automatically by the act of assigning honor points to a new avatar, unless settings are changed otherwise. If directly inserted and ranked avatars are placed in the middle of the trust ranking, their percentile will be noted and a score will be assigned as an average between the score of the nearest two avatars in the list (as available). Unscored participants are ranked above scored because participants will likely trust their own parents the most regardless of how reliable someone is by earning (scored) honor points. But, all these settings can be changed because of the high variance in preferences for trust ranking.

Popular Rank

People may publish parts or all of their trust rank. This information can be collected from other participants or sources to establishes who is popular as trusted and who isn't. It is considered unwise to adjust one's own trust rankings based on popularity, in part because it reduces individuality of Zeronet (ZNET) participants such as by applying social conformity pressures. Popular rank can also lead to guilt by association, which is often an unfair bias. However, when two people are ranked identically, then the popular rank will be the deciding factor in determining the tie-breaker that decides who has the higher trust ranking for a given participant. And because most people will be unknown to any other person, they will therefore rank zero on a participants trust ranking, and so popular rank will determine much or even most of their content as displayed. So for those who avoid many forms of collectivism, popular rank information is still a net benefit because most people are unknown by any given person, causing hearsay to be a desired factor. To reduce bias in this aspect, Public Pledge Evaluation (ref Pledges:Public Pledge Evaluation section) leading to Public Honor Points should be a more important factor in determining which unknown people are trusted more and less.

Perspective Development:Network Synchronization:Summary

Every participant may form their own perspective of Zeronet (ZNET), but including other perspectives involves synchronization of perspectives. Before a synchronized perspective, Zeronet (ZNET) could be considered unsorted lists of every persons information on every topic as a full collection, while after synchronization, it is information shared by various groups organized into views by those groups, with dominant views more noticeable but dissenting views also noticeable. A collection of all public Zeronet (ZNET) summary records from all online information sources regardless of trust level form a perspective of the full network. Network Synchronization first forms the full collection, then organizes perspectives as "named

perspective" views on parts of that collection which are described further in this document as trust gardens (ref those sections). The full public perspective is the point at which full network synchronization is expected to begin, followed by synchronization of views within the network which are a personal perspective as a trusted person or group. Synchronization is done by exchange of trust information and database summary information by an expansive range of sources. The two Zeronet (ZNET) services responsible for that synchronization are the Data Discovery and Synchronization (Disco) service and the Group Trust and Synchronization (GTS) service. The Group Trust and Synchronization (GTS) service creates and manages public and private domain record sets, so creates critical network perspectives. The Data Discovery and Synchronization service keeps track of all these records together and is therefore is important for network synchronization of the data sets either in one perspective, or many. A participant’s Web of Trust is used to notice explicit trust of participants, then their ratings of other personally unknown participants, and determine trust (as faith) in their information. From the full network perspective, one can look at everything available if they wish, or begin to filter in information by determining which sources are considered trustworthy using a specific view.

Crosslink and Metacode Summary

Crosslinking is information validation beginning with a single Zeronet (ZNET) avatar that forms identity of named trust groups and agreement on what data is on Zeronet (ZNET). A crosslink is a code representing a trust relationship as a shared point of agreement on database records, comparable to signing a page of an encyclopedia if you agree on who wrote it and also (for this example) that it is good information. First an identity (as an avatar) is linked to specific topics data sets (as content and records) such as by the avatar commenting on a topic, and then that data is accepted (as signed) to Zeronet (ZNET) as valid, comprehensible, or otherwise existing on the network by validation of agreement that the information came from that avatar. So, crosslinks can form perspectives on Zeronet (ZNET). A code as a "metacode" is formed based on that validation named a crosslink. Depending on the crosslink category used, a different level of agreement is achieved from acknowledging data to honoring data. Regular crosslinking may be part of an ongoing data sharing arrangements with other participants. So, crosslinking may be used for different forms of perspective. The data content is expected to be summarized by digital hash (ref Democratic Communication:Identity Information:Digital Hash), and a description of that hash is expected to be consistent with the contents. That digital hash is the code as a

metacode. So, a metacode is the hash of all contents of a database or record set in a database. A crosslink is where a metacode is digitally signed to indicate the database content matches to the database identity (as an identifier tag). Key signing in cryptography is also a type of crosslink. With key signing, one digitally signs another person's key to indicate that the key matches to a specific personal identity. Crosslinks only happen with agreement. For example, a database claiming to be a database of music, but containing only videos would be refused to be crosslinked.

Crosslink Table

A crosslink table for each participant lists metacodes and their status as valid or invalid. A Cohesor is someone who helps with trust-sensitive activities. Participants are expected to partner with a Group Trust Synchronization and Consensus Service (ref Trust Information Sharing:Group Trust Synchronization and Consensus Service) and other Trust Cohesors who evaluate trust information to form the crosslink table. A Trust Group creates data sets with metacode references. These data sets are then indexed by a Data Discovery and Synchronization (Disco) service.

Metacode

is a computer programming "hash" (ref Democratic Communication:Identity Information:Hash) used as an identifier for a collection of content or data, and it may be considered a type of summary information and metadata. If all metacodes show that data a participant placed on Zeronet (ZNET) has been distributed successfully, that is an indication the metacode is honored. If a metacode contains references to information that is mathematically contradicted by its own rules of its related protocols, that is an indication the metacode is dishonored. Metacodes may refer to data that follows mathematically provable rules such as a "blockchain". They also refer to data that is opinion, but such opinions might be ignored in the context of the metacode checking. The Zeronet network synchronization services (GTS, Disco) both handle these codes.

Metacode Form

Reference Group Records Exchange (GREX) protocol (Democratic Communication:Plain Text Protocol:Group Records Exchange) for the recommended composition and form for metacodes.

Crosslink Metacode

is a record identifier noticed in some way by at least least one other participant. This is expected to be formed by listing a set of metacodes which all represent a shared agreement regarding a specific record, and creating a new metacode that represents a collection of those agreement signatures as one record. Categories of metacode, also called "signature codes", include

"Acknowledge", "Agree", "Honor", "Dishonor", and "Dissent". (ref Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol:Crosslink Codes). So, some data is accepted with different levels of agreement, from disagreement to honor, because information may be accepted as anything including commentary, disagreed assertions, and agreed facts, so the "agreement" could be as minimal as acknowledging its existence while disagreeing with the information set.

Beginning Crosslink

When a participant begins Zeronet (ZNET) activity, they may select as few as one other participant to trust for reliable crosslink metacodes (see nearby section), which determine what information is accepted as Zeronet (ZNET) content or is furthermore honorable information. This can be done by the Group Trust and Synchronization (GTS) service. A Data Discovery and Synchronization (Disco) service provider (ref Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization) provides content availability references and summary information of data submitted to Zeronet (ZNET), and parts of that data are honored and rejected as the participant wishes. Honor of any of that data is the potential for a crosslink. In that case, the consensus is at least two people, though could be more because their beginning partner participant may share the code with more than one person. Some people may publish information on their preferred metacode sources while others keep such information private.

Snapshot Metacode

Public Content Network (PCN) content and other data referenced and discovered by the Information Graph (Iggy) changes over time. It is often important to know what changes were made and at what time they were made. A Snapshot Metacode is a set of values that identifies one specific database at one point in time. A Snapshot metacode is a point of reference which can be a point of consensus that that data is a valid part of Zeronet (ZNET). Snapshot metacode data is developed to track content changes over time for participants who want to recognize these changes. Content creators are expected to maintain a database of content. For example, digital money broadcasters and evaluators maintain a database of transactions. Each time a record is added, the database changes. A hash tree (ref internet search) reflecting the database state at any given time is expected to maintained and shared with the general public upon request. There may be multiple hash trees for different categories of usage. Reference Data Discovery and Synchronization Service (Disco) nearby for more information.

Cycle Synch

The Cycle Synch process is to enable multiple participants to interact with Zeronet (ZNET) consistently such that if both participants do the same Information Graph (Iggy) based search with the same public avatar profile interest expressions and "named

perspective" or "full perspective", they will both receive the same results. This contrasts with file sharing peer-to-peer networks that produce a different search not only for each different participant, but the same participant with two computers running the same search on both computers at one point in time. It also contrasts with most of the most popular websites which display different content based on the country of information destination. Zeronet (ZNET) Service Cogs (COG) usually maintain public databases. These databases are expected to be labeled with snapshot "metacode" (ref nearby section) code values. At regular intervals, each Service Cog (COG) relays the code values to requesting participants. The contract for such a service is expected to be based on bandwidth costs and be a relatively small cost as bandwidth for metadata is naturally smaller than for the underlying data. Attempting to send contradictory metacode data is considered dishonorable. Reference Data Discovery and Synchronization Service (Disco) nearby for details.

Data Discovery and Synchronization Service (Disco)

Summary

This service tracks what data collections are available, who can provide the data, and when it was added (or removed). This process is expected to be done consistently according to a crosslinking (ref nearby section) protocol which offers a perspective of a viewpoint while avoiding personal bias. An perspective identifier referring to a set of database information is a "metacode" (ref nearby section). Furthermore, this service may filter data as requested from a set of specific sources, considered to be a "named perspective" as a Zeronet (ZNET) view. The number of filters available might be limited according to available resources, so is encouraged to be determined by supply and demand factors in open competition. A database on any specific topic as a "named perspective" could be trusted to be provided by a specific person or organization through this service. Information about such databases is considered "discovery tables" that list each topic and the associated databases.

Role Comparison

In common "search engine architecture" terminology, this service performs the role of "crawler", but differs by building multiple partial "indexes" (as the discovery tables) which are made easily searchable by other components such as the Topic Search Provider (ref Information Graph Cogs:Database and Search Cogs:Topic Search Cog).

Applications

This service is expected to be used by many services including metastream providers, Topic Search providers, and Public Content Network (PCN) databases (such "Broadcaster" databases) to have access to the

most recent content being added to the network. Furthermore, because of the way this service connects many services together, this service may relay requests to add, remove, or tag any type of public or private Zeronet (ZNET) data, especially for broadcast content. In that respect, Data Discovery and Synchronization (Disco) is an information switchboard service which distributes information references to many databases on behalf of a participant such as Contact Directory Cog (Cdisc) (ref Information Graph:Information Graph Cogs:Database and Search Cogs:Contact Discovery Cog) information.

Participant Interactions

Data Discovery and Synchronization (Disco) service is expected to be used by database services to add data to their databases, either as part of a larger group of databases or as an individual database. This service is expected to supply metastream providers with content references for distribution to pulling participants. Data Discovery services track overlapping and disagreeing databases, leaving it up to other services to filter out bad data, in avoidance of bias. Participants are expected to receive summary information from multiple sources to help confirm accuracy and completeness of data sets. Timing information is especially useful for Public Settlement Network (PSN) claim records where timing determines record validity.

Database Summaries

Each database should be summarized by a hash (ref Democratic Communication:Identity Information:Hash) tree where records are organized in a network graph according to the Group Records Exchange (GREX) protocol (ref Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol). So, databases are hashed as metacodes (ref nearby section) and a summary record of the database is noted by the Data Discovery and Synchronization Cog (ref Service Cog:Web of Trust:Data Discovery and Synchronization Cog). This information is expected to be shared among other Data Discovery and Synchronization (Disco) service partners who collectively track what databases are available, when they are updated, and the metacode of the most recent database version. Such service providers are expected to digitally sign each others codes as proof of record timing, forming crosslinks (ref nearby section). When data is removed a record of the data size and hash is expected to remain for a time. Discovery services are a primary Information Graph (Iggy) database source because they are able to link content identifiers to content locations.

Additional Features

Data Discovery and Synchronization (Disco) service may scan other networks for information to be

transferred to Zeronet (ZNET). Participants are welcome to relay content leads. A content lead is information about potential Public Content Network (PCN) content which may not yet be added to Zeronet (ZNET). The service may be prepaid to explore content leads as they come or participants may pay for already discovered content leads. So, this service collates and shares content references expected to be found valuable. The service may also be used to request data or content to be created by participants who seek data on various topics, using "seek requests", when a participant seeks additional data or content. This service is discouraged against offering direct trust information, such as by personally evaluating and reviewing data collections, as a potential conflict of interest. Rather, a participant is expected to provide a references to "named perspectives" or evaluators such as by a trusted Review Cog (ref Service Cog:Netportal Cogs:Review Cog) for example, and that information is used to provide database performance reviews used to filter data according to the participant preferences. All participants are expected to have database records because even a profile is a database record.

View Development Incentives

Pull and Push Directory Incentive

Participants are expected to pay for Data Discovery and Synchronization Cog (Disco) in two ways. Firstly, participants seeking content or data reward Data Discovery and Synchronization Cog (Disco) service providers under a contract to provide information on what content databases are available to them. But furthermore, content creators and data providers (including broadcasters) under a contract may pay Data Discovery and Synchronization Cog (Disco) service to acknowledge and help others connect to the data they have available. So, data providers (and/or underlying content creators) pay for advertising, but data recipients also pay for directory service that reveals data providers they may have otherwise been unaware of. Data providers may filter their database/content listings directly, or they may filter listings according to their customer preferences. A messenger may want to push content to enlighten the world with virtues and values, sell educational materials, and invite the public to an event. While a broadcaster or data provider may want to pull that messenger content, it is only to then be able to push it to others, so a broadcaster is more considered a push participant. Content seekers may want to pull that message to discover virtue and value, educate them self, and be invited to public events.

Push and Pull Negotiations

Unique combinations of push and pull interests are expected for each topic. So, for an encyclopedia, content readers are expected to want accurate data to be pulled about a specific plant. A content creator may want the most popular data about the plant to be pushed for more engaging content for repeat business regardless of accuracy. The Data Discovery and Synchronization Service (Disco) process adopts roles from the Public Settlement Network (PSN) (ref associated section) to allow both sides to balance interests in a way that offers a shared perspective as negotiated between content readers and creators, for higher quality broadcasting. This is expected to be accomplished by agreement of compliance with dispute resolution organizations which resolve disagreements among partnering participants such as content readers, content creators, content evaluators, and content reviewers of varying levels of bias or independence. So, a content readers have a chance to dispute provided data with a formal dispute resolution organization process. Discover and Synchronization Service (Disco) may analyze trust information by such dispute resolution organizations providing trust information by agreement between content providers and content seekers to determine which records are in which database perspective view.

Pushing Data

To push a desired data view as a data source (including as a content creator), a participant requests evaluation of potential data according to the standard set for a "named perspective" by a Trust Group (ref Perspective Development:Establishing Trust:Trust Group). This is expected to be done by the "Trust Garden" model (ref Perspective Development:Web of Trust Garden) model as formalized by the "crosslinking" process (ref neighboring section). Pushing participants include content creators and content distributors (including broadcasters). The participant formats or otherwise adjusts data according to the standard and submits the data to interested participants, such as evaluators, (including reviewers or raters) or any other interested person. This process can be repeated as needed to gain the desired amount of honor for the data (including content). Then, the data is sent to a balancing participant such as a Data Discovery and Synchronization (Disco) participant. If the data sent matches the crosslinking process supported by the Discovery and Synchronization (Disco) service, it may then be added to the database as a named perspective view by also sending the information to a Public Info.

Pulling Data

To pull data of interest for "named perspective" view as a data provider (especially as a broadcaster), existing evaluation records (which may also be reviews and ratings) are searched for through on an ongoing basis such as by pulling data from metastreams (ref associated section) to ensure records are accepted by topic Trust Groups (ref Perspective Development:Establishing Trust:Trust Group). This information enables providers to form a formal perspective as a database that can be relayed to participants. Data may also be provided directly by a "pushing" participant such as a content creator. The evaluators them selves are then filtered based on their level of trust by the person forming the view. Analysis of evaluation data determines which evaluators agree with each other. Data pull interests may also add a "seeker tag" in ways that request specific content or data to be provided or created. These tags may be relayed to trusted Data Discovery and Synchronization (Disco) service for pickup by any pushing participants including content creators and other data providers.

View Balancing

Databases may be pay to read, pay to write, or both. View balancing participants are encouraged to balance payments from both "pushing" and "pulling" participants to be equal, and may change prices on a regular basis to maintain such balance. That is done to avoid an incentive for information bias. Balancing participants include Data Discovery and Synchronization (Disco) (described in these sections) service providers and dispute resolution service providers (see associated section). Dispute resolution service providers are expected to be mutually selected by "push participants" and "pull participants". Participants assign a set of mediators or arbitrators to mark any problem data for further filtering.

Content Honor Evaluation

Any interested participant collects message evaluations, ratings, and reviews that associate to a message of their interest. This will be a combination of push interests and pull interests for each participant.

Perspective Development: Network Synchronization: Crosslinking

Summary

(ref Perspective Development:Network Synchronization:Crosslinking above)

View Filtering, Named Perspective

The Trust Garden (ref Web of Trust:Trust

Development:Trust Garden) is used as a model to form "named perspectives" which allow a shared "3rd party" view of a database which shows records honored by numerous people, as a view of information trusted by a certain person or group of people. Public data on Zeronet (ZNET) can be seen with or without another perspective "3rd party" filter. The group of people forming the perspective are being named, but may be named in relation to a specific topic or topic cluster to limit the view to expertise.

Crosslinking General Purpose

Crosslinking forms agreement on what data is on Zeronet (ZNET). Group Trust and Syncronization (GTS) service, Data Discovery and Synchronization (Disco) service, and other data providers can use crosslinking to join data together to form a database according to a "named perspective" view, and where there is disagreement in data, alternative named sets can be formed in other views. A metacode and crosslink metacode (ref neighboring section) corresponds to a specific data set identified by a data identifier tag. This data might expected to be formatted according to the Group Records Exchange (GREX) protocol (see associated section) for easier understanding. A Data Discovery and Synchronization (Disco) service is expected to have a database of metacodes including crosslink metacodes. Metacode sets are sent to the Data Discovery and Synchronization (Disco) database provider participant along with any timing or metadata. The "disco" provider adds the metacode set to a more complete collection by examining the related crosslinks. The disco service determines all available implied crosslinks by finding data sources that overlap by honoring the same sources, while dishonored sources may be removed from the perspective, but may instead form an alternative perspective. Additional implied crosslinks may form by finding data sources which overlap with a social contract. Then, explicit crosslinking is done by examining trust among the participants associated with the database topic or "named perspective" view being formed. So, participants interested in the database may formally trust each other to form a level honor for different data source participants of shared perspective. Data with both implicit and explicit crosslinking is considered having a higher trust rating. Arbitrators and evaluators are expected to be among the participants honoring (or dishonoring) data collections.

Crosslink by Topic Knowledge Trust Domain

Each participant may assign different people to be trusted with different record types based on allocated Topic Knowledge Trust. Reference Information Graph:Network Synchronization:Crosslink

Metacode for crosslink information. For example participants who are certified as doctors could be trusted to provide medical information. At the individual filtering level, a participant is may most trust their designated doctor to provide them the most accurate and complete health information, while they trust their preferred banking service to offer the most accurate and complete bank balance records and financial market data. This is relevant because information is first provided in a general way and then filtered according to one's personal filters. Doctors and banker's are encouraged to regularly supply the participant with up-to-date Metacodes reflecting their most recent database information so their information can be evaluated with all other information with Zeronet (ZNET) queries.

Metacode Set

Evaluators who have matching evaluations cause an implied "crosslink" (ref neighboring section). Depending on the data, any evaluations that don't match exactly create varying degrees of perspective breakdown which can cause multiple different perspective (views) to form. A metacode identifies each specific evaluation. Metacodes are joined in a metacode set by listing all metacodes in the set and digitally hashing (ref Democratic Communication:Identity Information:Digital Hash) the list. This digital hash could be confirmed by an evaluator by checking the hash and then signing the hash (ref Democratic Communication:Encryption Terms:Cryptosignature).

Implicit Crosslink

Implicit crosslinks are formed when participants each designate honor to a shared perspective, formally as a named perspective view (ref neighboring section). When done formally such a process may be done more reliably and so the crosslink (ref neighboring section) could be considered stronger.

Garden Stem Crosslink

Participants honor the same agreements and protocols.

Evaluation Crosslink

Participants share an identical evaluation of data. Consensus crosslink (ref neighboring section) would occur where all evaluations of one participant are identical to all evaluations of another participant.

Explicit Crosslink, Trust Crosslink

Explicit crosslinking as a trust crosslink is accomplished when specific participants declare trust of other participants as an information source in creation of a shared perspective. Furthermore, a specific participant may agree on dispute resolution participants with another participant. A mutually agreed upon arbitrator may be assigned to resolve

records which clearly conflict with each other, which delegates a participant to help determine which records are accepted as the most accurate. Expected crosslink (ref neighboring section) participants include "pulling", "pushing", and "balancing" participants as referenced nearby.

Trust Chain

Participants can express trust in other participants. This creates a chain of trust where because one participant trusts another, their new data is considered for addition to data collections.

Trust Group

Groups of participants can express trust for one another, which creates a "web of trust". (ref: Perspective Development:Network Synchronization:Crosslinking:Trust Group, Group Trust and Synchronization). Organizations and professional groups or certification networks are expected to use Zeronet (ZNET) by forming a Trust Group that reflects their organization or professional peer group web of trust. See also "Delegated Trust Group" for the Zeronet organization Trust Group method.

Trust Garden Crosslinking

Summary

Crosslinking is explained using the "Trust Garden model" (ref Web of Trust:Trust Development:Trust Garden) as a metaphor.

Crosslinking Seed, Seed Crosslink

A crosslinking seed is a code representing civil agreement of philosophy. Philosophies can be detailed with protocols, language usage, and behavioral codes of conduct including social contract agreements. Crosslinking is done according to the Trust Garden model (ref Web of Trust:Trust Development:Trust Garden). The starting point is a "crosslink seed" as a formal philosophy of a specific avatar. This would be done by declaring honor to a preferred philosophy such as the Rainbow Rock philosophy (ref Rainbow Road:Rainbow Rock). This can be done by signing a digital hash (ref Democratic Communication:Identity Information:Digital Hash) of a complete text or as little as just the title of the philosophy to leave room for broader agreement without agreement on specific details. The hash or title is combined with a Signature Code of honor(ref Plain Text Protocol:Group Records Exchange Protocol:Signature Code) which indicates the meaning of the signature. So "Honor:Rainbow Rock", could be digitally signed (ref Democratic Communication:Encryption Terms:Digital Signature) by the person as an example of a minimal crosslink seed that uses a metacode data name rather than a metacode hash.

Crosslinking Taproot, Taproot Crosslink

is a code symbolizing an agreement among multiple people who share the same philosophy and social agreement. A list of crosslink seeds (see nearby section) is digitally hashed (ref Democratic Communication:Identity Information:Digital Hash). That hash is considered a taproot crosslink.

Crosslinking Rootbranch, Rootbranch Crosslink
is a shared set of philosophies and social agreements which a database can be formed from. Multiple taproot crosslinks (ref nearby section) may be joined by listing them together to reflect additional agreed protocols, language usage, social agreements, and behavior agreements. This set of taproot crosslinks is then "digitally hashed" and that hash is considered a rootbranch crosslink "which indicate adherence to a specific philosophic perspectives or world views, communications protocols, and behavioral protocols." (ref Trust Development:Trust Garden). This could be a set of foundational documents, including communication protocols and data formats, that is proposed by an organization.

Crosslinking Stem, Stem Crosslink, Trust Group Formation
A crosslink stem is expected to include agreement upon which data following a specific protocol (such as set by a shared rootbranch agreement) is part of a specific Zeronet (ZNET) database. A "crosslink stem" is a type of Trust Garden Stem (Reference: Web of Trust:Trust Development:Trust Garden). When cohesive "rootbranch crosslinks" as behavioral and protocol agreements have been listed together to form a sufficiently complete collective agreement to a participant’s satisfaction, the crosslink rootbranch (ref nearby section) becomes a "crosslink stem" by digitally hashing a full list of the associated rootbranch crosslinks. This "crosslink stem" as a collective agreement is the basis for a Trust Group (ref Establishing Trust:Trust Group) as database record standards are be established by all those agreements. A "named perspective" as a Trust Group view can then be created by records from trusted database record sources which share the same crosslink stem. One participant can be part of multiple crosslink stems because each crosslink stem may provide a different perspective which records are part of a database, and different crosslink stems can be used to form different databases as different "named perspectives". This could be a set of foundational documents, including communication protocols and data formats, that is actively accepted by organization participants. This doesn’t generally include any databases.

Crosslinking Stembranch, Stembranch Crosslink
Each different record format forming a data collection of a Trust Group is a Stembranch.
Crosslinking Petal, Petal Crosslink
Data records and content wanted to be added to a public database (on the Public Content Network) by an individual participant may be added as a "crosslink petal". They select a crosslink stem (as described nearby) representing the Trust Group (ref nearby section) they want to be part of to add their data records to. Their data is digitally hashed (ref Democratic Communication:Identity Information:Digital Hash) which is considered crosslink petal as a metacode (ref neighboring section). Each record is identified by a metacode (ref neighboring section). The records of each participant digitally signed (ref Democratic Communication:Encryption Terms:Digital Signature). Each signature of a record is expected to include a signature code (ref Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol:Signature Code) of honor to add records to the data collection. These stembranches form databases that are considered part of Zeronet (ZNET).
Perspective of a Perspective
The data itself may be trusted directly according to the agreement, or just the data sources can be trusted as a perspective of another perspective that may or may not be trustworthy. For example, a neighbor’s journal of what their friend says is a perspective of a perspective. So just because data is in a database, and the person adding it is trustworthy, may not imply that the content of the database is trustworthy unless that is directly claimed by the people who create the database.
Crosslinking Flower, Flower Crosslink
A "flower" represents all data records from a specific individual as an avatar in a form according to a specific set of protocols, behavioral guidelines, and data formats. So, a flower crosslink is when one individual validates the records of another. All data records as "petals" are digitally hashed along with a code representing the stembranch crosslink into a "flower crosslink" metacode.
Flower Patch Crosslink
A jointly formed data collection of all data from participants who form a cooperative to offer a perspective view as a (Stem Crosslink) Trust Group (ref nearby section) and furthermore the Group is a formal organizational alliance of sufficiently similar Trust Groups, for developing content and databases. So, this is a formal version of a Flower Patch Crosslink (ref nearby section) that otherwise might occur without any formal alliance. As the Web of Trust "Trust Garden" model says (from :Perspective

Development:Web of Trust Garden:Flower Patch) "Such an organization is encouraged to help development of strategies and tactics for advancing organization missions. These participants then split and join with such cooperatives fluidly as they feel best suit their goals. These organizations are encouraged to do so as Rainbow Cooperative organizations (ref Caroasi:Rainbow Cooperative)."

Crosslinking Trust Garden, Trust Garden Crosslink
: A data collection of all trusted Trust Groups, according to the perspective of a specific avatar. Trust Group leaders may sign each others Flower Patch Crosslinks to form a more official collection. A full Trust Garden would be a perspective of all relevant content on Zeronet (ZNET).

Trust Crosslinking
: One-Way Trust Crosslink
  : This occurs when one participant trusts another, but the trust is not returned. A one-way trust relationship can help to confirm or help validate content originated by Mutual Trust Crosslinks (see nearby section). A trust crosslink is expected to be formed by a combination of a signature code (Plain Text Protocol:Group Records Exchange Protocol:Signature Code), topic identifier tag(Information Graph:Structure:Topic Identifier), and participant identifier tag(Democratic Communication:Identity Information:Identifier:Participant Identifier Tag), by determining the digital hash(ref Democratic Communication:Identity Information:Digital Hash) of that combination.
: Mutual Trust Crosslink, Mutual Trust
  : Mutual trust between two or more participants allows a Trust Group to begin. Mutual trust crosslinks are considered the origination point for creating, adding, or replacing Trust Group content to a content database. A mutual trust crosslink is formed and identified by combining a pair of one-way trust crosslinks and then determining the digital hash (ref Democratic Communication:Identity Information:Digital Hash).
: Crosslink Hub, Hub Crosslink, Trust Group Identifier Tag
  : Mutual trust among three or more participants forms a Trust Group Hub. A hub ring crosslink is formed by combining multiple Trust Crosslinks (ref nearby section), then determining the digital hash (ref Democratic Communication:Identity Information:Digital Hash). That code represents the Hub Ring as an identifier and a Trust Group identifier tag.
: Hop Crosslink, Hop
  : Mutual trust from one hub ring participant to another participant who is not directly in the hub

forms a hop crosslink that expands the network from the hub (ref nearby section). This participant can contribute to the perspective view, though nodes closer to the middle will consider having a higher precedence for resolving conflicting data.

Hippity Hop Crosslink

Hops (see nearby section) occur until the final "hippity hop" crosslink which may be either the last trust link or a chosen number of hops is reached such as four hops, though many more are possible. The number of hops is expected to be based on the furthest extent of the network expected. Each hub node may declare a number of hops they believe as a hop limit for trust. The most commonly selected number of hops as most preferred could be the number considered to be the "hippity hop" limit. Protocols agreed upon by participants in the hub may also define that number.

Hop Limit

For a network to include a population of 8 Billion, there would be expected to be about "seven degrees of separation" between people as currently commonly believed. This would mean the center hub needs at least four hops for all nodes to connect with all other nodes in the trust network. With an expected number of 12 trusted participants for each participant as also commonly believed to be a number of trusted people for a typical person, nine hops (calculated roughly as ln(8 Billion)/ln(12) ) could be expected to be sufficient to reach a mutually trusted participant with an indirect bond of trust with a "tenth hop" to an untrusted participant. Nine hops would be sufficient to form an indirect bond of trust to any other indirectly trusted participant if each participant in the chain of trust were trusted. For a network limited to a specific topic, the hop limit would be expected to be smaller based on the size of the network. The hop limit could also grow over time with network size, and would be expected to start at one hop, then grow at a predetermined rate defined by mathematic methods.

Crosslink Concentric Ring Band Visualization

Mutual trust from one hub ring participant to another participant who is not directly in the hub ring can be seen as a band ring connection. This trusted participant can in turn then trust another participant. This can be visualized as a concentric circle group, with the Hub Ring in the middle and each hop (see nearby section) to a mutually trusted participant is formed in a

further distance circle from the Hub Ring circle. So after the original "hub ring", each additional trust link to the next participant is one further from the center in a series of rings until the final "hippity hop" ring band.

Distrust, Perspective Splitting

Distrust is used as a factor to determine divisions between multiple perspective views. Where there is complete agreement among all participants, only one shared perspective exists. Each additional distrust provides an additional opportunity for another perspective to form. Because of the resources needed to form trust group perspectives, a limited number are formed. With current computing resources considered, for most topics (ref Public Content Network:Topics:Topic), a single participant is expected to be able to form at least one perspective for most topics if they so wanted to do so. A majority of nodes at any ring being distrusted may be an indicator that a split should take place.

Personal Perspective vs. Trust Group Perspective, Trust Delegation

Personal perspective is one’s own created information and also information from others which is personally reviewed and honored in its entirety. Most information will be provided from other people’s perspectives by delegating trust to a specific person in a Trust Group. From that point, it is the delegated person’s trust of others that provides much of the perspective. So, if someone on one’s personal trust rank is low, their content may still be considered trusted because the delegation of trust is redelegated to the personally untrusted person.

Distrusted Delegate Resolution

Forming a personal Trust Group is one option to preventing personally untrusted people in a trust group from providing untrusted content. A replacement cog (ref Service Cog:Democratic Communication Cogs:SigilX Replacement Cog) could filter could either flag or remove certain untrusted information when it isn’t entirely depended on for proper display. It is discouraged to prevent untrusted information from being displayed entirely to avoid "echo chambers". So, for every content varying levels of competing perspectives can be displayed to help participants be aware of different perspectives. (Reference: Netportal:Competing Perspective Consideration)

Centralized vs. Decentralized Trust Group

A fully decentralized Trust Group (ref nearby section) network has all interested participants

able to add or replace records with freely extending trust. A fully centralized Trust Group network only allows the hub ring to add or remove records without any extension of trust by "hop crosslink". This is largely a function of how much participants are trusted by the people in the Trust Group. The Zeronet (ZNET) network encourages all people who are trustworthy to be added to a trust group for better decentralization and therefore more resilience and participation with strength of unity.

Trust Group Decentralization Incentives

Evaluators (Ref Web of Trust:Evaluator Participant) will naturally be tempted to centralize and so monopolize over time as trust networks are "network effect" organizations. To maintain open competitive conditions, participants are encouraged to select evaluators in ways that avoid unfair leverage. Evaluators who cooperate with many broadcasters as equal partners is encouraged.

Trust Group Evaluator Broadcaster Selection

Broadcasters are expected to keep content and records of a trust group available by cooperation. Evaluators (ref Web of Trust:Evaluator Participant) within a Trust Group are expected to cooperate with many accepted broadcasters to ensure expansive data discovery, and only honor data (as content or records) that is published to at least one broadcast source in the formal Trust Group accepted broadcaster list (ref Public Settlement Network:Broadcasting:Accepted Broadcaster List). A large but not overbearing number of broadcast sources will be used by each trust group for each topic of interest to the group. Too small of a number would be noncompetitive and enable monopolistic leverage by broadcasters. Too large a number would be a burden on resources of evaluators to search with all broadcasters. So, 12 to 60 sources are an encouraged number of broadcast sources for a specific topic. Furthermore, more broadcasters can participate by splitting a topic into parts, and limiting different broadcasters to different topic segments. That division would also add additional reliability in case any given broadcaster fails. This is expected to result in expansive awareness of the trusted topics of the Trust Group.

Topic Partitioning, Topic Splitting

To encourage participation of small scale broadcasters for decentralization and adding reliability, database content or records can be segmented according to an "index file". A small scale broadcaster can broadcast a section of the database without having the entire database. Each Trust Group is expected to establish a database that is sorted by different ways for fast searching. One of the ways in

which the information is sorted may be designated as the way to divide it can be considered as divided into segments defined by the "index file". Evaluators still have a range of broadcasters such as 12 to 60 broadcasters, but a different set of broadcasters may apply to different segments, and the more specific a broadcaster is to a smaller segment, the more encouraged it is to be one of the broadcasters used. Such favorability wouldn't be expected to be used to select all broadcasters for a specific segment, it would be expected to be used for some broadcasters so maybe half of the broadcasters would be selected based on their being very specialized to a specific segment of the topic. This would be considered more reliable because if one of the broadcasters fail, their share of the data storage would be smaller.

Evaluator Multiple Trust Group Participation

If one evaluator (ref Web of Trust:Evaluator Participant) is member to multiple trust groups for the same topic, multiple trusted broadcaster lists, one for each Trust Group, would be expected. At least one broadcaster on each list must be a source for evaluated information before it is considered honorable by the evaluator. So, more publication is needed for honor by that evaluator. This is potentially confusing to participants trying to add an honored record or content because they may expect only one broadcaster to be sufficient and not take notice of the requirement for multiple broadcasters on the list to be used. To avoid confusion, one evaluator is instead encouraged to have multiple avatars, one for each Trust Group they wish to be a member to, in order to avoid a direct requirement for multiple broadcasters to be used for honor of data (including content or records). A general way to publicly connect them together would be use of multiple names assigned to the avatar, one shared name and one unshared name. So, "Verifications R Us West" would have one verification key for one Trust Group and "Verifications R Us East" would have another verification key for another Trust Group.

Honor Crosslinking

Summary

Data (as records and content) are added to a database by collecting and gaining honor by participant in a Trust Group (ref Perspective Development: Establishing Trust:Trust Group). Each trust group is expected to adopt a protocol which determines the level of honor needed to be considered valid data. There may be different standards for different topics, which is encouraged to be done according to the Group Records Exchange (GREX) standard (ref Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol). Each trust group is expected

to specialize in one or more specific topics of interest to the group. Different topics may have different standards for honor of data. Each trust group has a certain number of hops (ref Trust Crosslink:Hop) to the edge.

Honoring Data

Data as content or records is expected to be evaluated for honorability before being added to the database. First, one or more favored Trust Groups (Perspective Development: Establishing Trust:Trust Group) are selected to add content or records to a database of a selected topic. The Trust Group is expected to have many evaluators (ref :Web of Trust:Evaluator Participant) who can review the data to be added. The Trust Group is expected to have a protocol defining the number of good evaluations needed for acceptance. So a group may specify the need for 24 good evaluations before a record is added to the Trust Group. A content creator sends the data or a reference to it to evaluators, and may pay a predetermined fee for the evaluation. If the data is honorable, a combination of the honoring signature code (ref Plain Text Protocol:Group Records Exchange Protocol:Signature Code) and the record metacode (ref Perspective Development:Web of Trust Garden:Metacode) it is digitally signed (ref Democratic Communication:Encryption Terms:Digital Signature). The content creator then lists all the signatures as a set to show sufficient honor to a Data Discovery and Synchronization (Disco) service (as defined by these sections) so it is noticed by broadcasters who add it to a perspective database (Perspective Development:Establishing Trust:Perspective View). The data is added to at least one broadcaster specified by the favored Trust Group(s) before being considered for addition by broadcasters who provide the Trust Group database perspective view.

Cross-Evaluation Honor

Participants may evaluate each other's data (as content or records) for agreement with the protocols agreed to by the Trust Group. The participants who are interested in content accepted request evaluation by multiple Trust Group participants. When evaluations result in honorable content, bond strength between participants may be considered increased. If evaluations are dishonorable, a person may lose trust from other participants.

Time Honor Participation

After a participant is participating in the group a long time, the more bond strength between participants may be considered increased. The bond strength increase is more rapid at first, then the

bond strength increase becomes slower.

Cross-Evaluation Personal Honor Purpose

This personal honor can be used as a factor for invitation to additional Trust Groups (ref Perspective Development: Establishing Trust:Trust Group), or a higher trust level for various special permissions or controls within a Trust Group.

Personal vs. Objective Honor

Personal honor is used to determine someone's status within a Trust Group. Objective honor is honor of content added to the topic domain. This honor may apply as personal honor to the creator, and as objective honor to the data (as content or records).

Maintaining Honor

Summary records (including metacodes) of honored data (as content and records) are expected to be kept with many trusted broadcasters in selected Trust Groups. However, full data is only needed to be kept by one broadcaster by each cooperating Trust Group for evaluation. Participants who want data to stay available over time are responsible for backing up such data to many broadcasters so full data can be retrieved as proven by matching the metacode to the complete record or content data. If an out-of-service broadcaster digitally signed (ref Democratic Communication:Encryption Terms:Cryptosignature) the data metacode as acknowledged, this would prove the record existed in the database so it could be recovered and maintained.

View Filtering

Untrusted participants may be filtered out entirely, though they may form alternative perspectives. Participants who are insufficiently trusted (without being distrusted) may also be filtered out, or form two perspectives including a broader perspective including people of limited trust.

Service Cogs by Crosslink Metacode

See Zeronet:Service Cog for information about service cogs. Service Cogs (COG) are expected to serve participants according to the broadest possible number of metacodes (ref neighboring section) for their given client's Trust Domain Perspective according to a minimum market demand. For example, if a Service Cog (COG) does not support a specific database as inaccurate or invalid, participants may still find another provider to search it and return a record requested by a participant by finding a provider with a matching metacode for the database records they trust. So, one Service Cog (COG) may provide support for different versions of Zeronet (ZNET) databases having dramatically different trust networks.

Web of Trust Avatar Personal Perspective

A participant’s complete Web of Trust avatar personal perspective can be represented by the set of metacodes (ref neighboring section) they use to determine what information is on the internet in the perspective of that avatar, and which organizations they connect to provide the information represented by the metacodes. These metacodes are databases of data believed to be part of Zeronet (ZNET) and also a set of information validations that the participant agrees with. These metacodes also include contracts the participant has agreed with.

Partial Crosslinking

Later versions of Zeronet (ZNET) could consider including partial crosslinking. Because there are any number of databases on Zeronet (ZNET), there are multitudes of metacodes (ref neighboring section) that can be accepted. So, if people disagree on the root Metacode (which would be an agreement on all records) they may still agree on most database sets and so have some level of crosslink without being 100% crosslinked. So, each participant can be perceived as having a certain percentage agreement with each other network participant on which databases are the most accurate.

Partial Honor

A crosslink may be "qualified" and detailed by listing honorability by each record. A qualified listing also means that only part of the database is actually honored. This may be accomplished by ranking sources as most to least trusted as part of the database, and/or assigning specific numbers quantifying trust to each source. See Network Synchronization:Crosslink Metacode section and the Public Settlement Network (PSN) for more crosslink details. Crosslinking information is one method of relaying which participants or information are trusted by one participant to other participants.

Perspective Development: end

Trust Information Sharing:

Record Validation

Because many different types of records can be validated independently, choosing to trust an untrustworthy person may be less damaging when steps are taken to identify and share record validation information. These independent validation steps are expected to be done both automatically and manually. Records considered inaccurate are expected to be Tagged as such with a Public Post.

Avatar Validation

The matching of an encryption signing key to an Avatar name may be delegated as a consensus decision. Such consensus may be developed in any way including by Group Trust Synchronization and Consensus Service (GTS). See the nearby Group Trust Synchronization and Consensus Service for details.

Trust Cohesor

A Trust Cohesor helps evaluate trust information so that participants may better interact with an unknown Zeronet (ZNET) participant or organization. The cohesor is to help estimate how likely a participant is to honor their public commitments. The analyst is expected to evaluate transparency and contract performance for an expansive range of participants. An expected task for Trust Cohesors is to assign a trust grade, much like a credit score to any and all Zeronet (ZNET) participants. The Trust Cohesor organization is encouraged to be formed as a Rainbow Cooperative (ref Caroasi:Rainbow Cooperative). Group Trust Synchronization and Consensus Service (GTS) (ref nearby section) is expected to be primarily tasked by participants for most trust evaluations. However, a range of specialist services are welcome for offering trust reports and evaluation of information for accuracy.

Trust Cohesor Layers

The primary purpose of Trust Cohesor layers is to tailor Web of Trust networks to a shared perspective. Forming a Trust Cohesor monopoly or oligarchy is difficult, as Zeronet (ZNET) participants seek to decentralize authority structures. A Trust Cohesor organization after compartmentalizing, adopts a specific Trust Domain. A Trust Domain is a hierarchal (multi-layer) alliance of Trust Cohesors. Each layer has an ability to determine facts for mediation and arbitration. So, if someone agrees to perform a service in a specific language for example, the protocol league would be responsible for determining if that is the case for the purpose of a contract. The top-level layer delegates such mediation and arbitration to the next lower layer(s) as they deem fitting, though if a layer renders a judgment that a participant deems in disagreement with another layer, they should expect to be able to appeal to that layer, and if being refused, they must decide whether the service they are using is best for them or whether to switch their service. Each Cohesor is expected to have a correlated arbitration and mediation group, and those correlated group are expected to use a Cohesor as a switchboard for mediation and arbitration appeals or objections to ensure accurate performance of those services.

Group Trust Synchronization and Consensus Service (GTS)

Group Trust Synchronization and Consensus is a core database and data unification process of Zeronet (ZNET). This process allows organizations to share a perspective on what information including financial balances and records will be accepted as most accurate and valid.

Groups and individuals are expected to cooperate with each other in building up a record set that at the highest level may be considered "the internet", or at a more private level could be a complete private network. A trust analyst of one group is expected to assemble a list of their most to least trusted other groups or Zeronet (ZNET) participants. This is expected to include all groups they associate with but may also include groups they don't associate with. This list is assembled based on the trust levels of the individuals members of their group, though this may be weighted towards members with higher contributions to the group or a higher stake of ownership over the group. So, a Trust Matrix is formed that lists Zeronet (ZNET) participants and their trust priority and may also assign a specific number to each list item. With this information, the group either uses another trust analyst or outsources to a Consensus Synchronization Service Cog (COG) (ref Service Cog:Web of Trust Cogs:Consensus and Synchronization Cog) to help integrate data synchronizations with other groups to determine which groups will be relied on for which records. Multiple groups may be weighted or assigned Trust Domains for this purpose. The synchronization service is expected to be minimally biased and be able to prove decisions by showing the math formulas used and other proof of work. So, the synchronization service determines what databases will be accepted to organization records. Records created by the hypothetical cooperative group are then added to the records imported, and these records are summarized and shared with partners who have prioritized the group as a valid record source. This synchronization process collects all data sets needed until reaching a root level considered "the complete network" for a specific point of time which is given a specific identifier, which is generally shared to the public domain but does not need to be. When enough people agree with this high-level record being both valid and supported, it is considered agreed by consensus to all those who form the agreement. This trust data sharing will be used for example for any group to form a decision on which transaction chains are legitimate and which are false or otherwise rejected. The hash representing all accepted records at a specific point in time for a "complete network" is a core synchronization record. That record is expected to be distributed as widely as possible for expansive unification. This makes it possible for "the internet" to be different for different people and different groups, who may not be able to interact because of disagreements on recordset validity. But, it is also possible for these differences to be seen and negotiated.

Trust Topic Knowledge Domain Map

A network graph on the Information Graph (Iggy) that indicates expertise of a given participant about any

given Public Content Network (PCN) topic.

Switchboard

A switchboard is a participants list of contact points. A Netportal switchboard portal allows participants to send or receive contact information. Each participant on the Web of Trust may share their list of public contacts (with permission of those participants), matching an identifier to a "public" write encryption key. Each contact in the list is assigned a level of trust automatically based on the trust rank and tier levels which are already assigned, though such trust settings are adjustable. Contacts are expected to be shared only under the directions of the participant whose contact information is being shared. This sharing feature and record formatting is considered the Switchboard system. The records format and sharing method is set under the Group Records Exchange (GREX) (ref attachment) protocol. Switchboard is a direct method that avoids need for the indirect method Contact Directory Service (Cdisc) (ref that section). Participants are encouraged to use their own contact list when practical to do so for the benefits of decentralization including security benefits.

Trust List Sharing

Web of Trust settings and data for one participant may be shared as part of sharing public contact information. One encouraged way to do that is to place the list on portable memory hardware and transfer to another person who trusts the provider to connect them with trustworthy content and/or trustworthy service provider connections. A list specifically for sharing is expected to be established so that other participants can be securely added to Zeronet (ZNET).

Crosslink Partnership

The crosslink (ref neighboring section) partnership involves a regular exchange of data where as newly discovered records are accepted by trusted participants, they are shared and adopted by crosslinking partners.

Trust Analysis:

Trust Analytics Reports

Trust analytic reports on Zeronet (ZNET) include claim validations, cross-audit validations, and trust chain analysis reports. Trust Cohesors including Trusted Evaluators are expected to review information for accuracy. Participants (and specifically their avatar) may be assigned a level of trust regarding specific Information Graph (Iggy) nodes or node clusters because they may be used to determine different aspects of Topic Knowledge. For example, to decide what the best treatment is for a participants sickness, they might use a medical Trust Cohesor rather than their Group Trust Synchronization and Consensus (GTS) Service (ref Trust Information Sharing:Group Trust Synchronization and Consensus Service) which may not provide enough information for a participant to know which health care

participants are most trustworthy. Honor points may be assigned to specific trust domains rather than at large. Or, points may be assigned both to a specific trust domain and "at large". While most trust domains are expected to focus on broad aspects of social cooperation such as contract enforcement, other types may focus on any topic such as Topic Knowledge Trust being based on a shared interest in a specific topic. Trust Domains established on the Information Graph (Iggy) 'Trust Domain Map' can be used to discover available Trust Cohesors which may formalize a trust domain into a trust rating organization of Zeronet (ZNET) participants.

Popular Performance Rank Report

This is a less subjective form of popular rank that assigns honor points to people based on their Public Pledge Evaluation (ref Pledges:Public Pledge Evaluation section) results. These results however are weighted according to popular rank for unknown people. The reason the weighting must happen is that dishonest avatars can positively rate each other to boost their performance ranks. Such badly behaving avatars will tend to become untrusted for their dishonestly, and their performance will not increase and could instead decrease because known trusted people have marked the unknown group as untrustworthy. So, these cheating users will have many positive Public Pledge Evaluation results, but those results will not increase their Popular Performance Rank because of their low trust rating.

Group Relational Trust Expectation Report

Shows how well two different interest groups trust each other, or in the case of organizations which organizations trust each other. For this assessment, participants on the network define their interests. The prospects primary interest group on the Topic Map (ref Public Content Network:Topics:Topic Map) is noted in relation to the prospect's primary interest group. Primary interests are expected to be generally public information. For example, a computer programmer might be expected to publicize their primary interest is computer programming. A person of their interest has reported a primary interest of football. A group trust chain will attempt to be formed by groups of people in these two groups. Generally, a beginning neutral point will be expected to be the "zero point" topic which is a topic which all other topics are considered a member of. For groups, the Relational Trust Expectation Report (ref that nearby section) method is used but for groups instead of individual people. A broad example for this would be a determination of how well people of the interest group "computer programmers" trust the group "football players".

Public Content Evaluator Trust Report

Content creators may pay to have their content publicly evaluated. Evaluators are encouraged to rate content with reduced bias and demonstrating fairness with

content ranking methods. Because Public Content Evaluators have the ability to determine what information is included or excluded to Zeronet (ZNET) participants, so this role is delegated with great care by content creators and accepted with skepticism by participants. Methods described in the Trust Garden subsection are encouraged to be used to form organizations that help rank public content. See Public Content Network:Content Distribution:Content Analytics:Content Evaluation for more details.

Relational Trust Expectation Report

show how well two people on the Web of Trust might be expected to trust each other, or how well one person may trust or distrust a prospect based on public Web of Trust information. This is an automated process of friend-of-friend connections to determine a persons reputation. First, paths of contact to this person are attempted to be discovered where the person is connected to through "friend of friend" connections. As many claims made about that prospect are collected as possible through this connection process including the prospects own claims about them self. The evaluation first 'filters forward' to a neutral point, most likely the "zero point" on the Information Graph (Iggy). This path represents an indirect path of contact to the prospect by searching through people who associate with each other. The neutral point is between the two people determined to be most mutually trusted and associated with the prospect. The 'zero point' isn't directly evaluated, and instead the two points (as people) that connect the two people together nearest to the 'zero point' are evaluated. Then, the evaluation 'filters back' through the Information Graph (Iggy) Topic Map (ref Public Content Network:Topics:Topic Map) "People" topic to the person most associated with the prospect. Claims by this person's associates are evaluated in determining the character of the unknown person and their reputation is noted as well. The 'filtering forward' process collects information by trusted sources about the prospect. This 'forward' chain goes 'forward' through more connected but perhaps less personally known people or groups. The 'filtering back' process collects claims by people most associated with the prospect who are trusted as much as possible by the mutually trusted person or group at the 'zero point'.

Zeronet Permissions and Control Assignment:

Control Domain vs. Trust Domain

A control domain controls Zeronet (ZNET) device resources including records, files, processes, and applications. Reference the nearby Control Domain section for more details. A Trust Domain (see associated section) controls what information is displayed for given internet query, and which information is displayed when multiple competing options are available. Specific Zeronet Service Cog (COG) providers are encouraged to be

suggested by these trusted sources for trust domains. Zeronet Service Cog (COG) providers are specifically granted a control domain to run their service cog on the device.

Control Domain Permission

General Trust and Domain Trust are used to determine permissions for modifying Zeronet (ZNET) devices including accepting, creating, and modifying Zeronet (ZNET) resources such as records, files, processes, and applications. Full permission means a participant is given permission for full device access. General permission means that a person is given all resources delegated to Zeronet (ZNET). Domain permission is for resources dedicated to a specific Zeronet (ZNET) resources. All trusted participants may share any or all of their Web of Trust rankings as a way of helping to delegate trust and permissions for others.

Device Access

Each Zeronet Service Cog (COG) (ref associated section) is assigned device resources under a Control Domain (ref associated section) so they can store and process information the participant's device. Each service cog is expected to request a specific amount of resources for their purpose. Such access is controlled by participants through the control domain permission system. Permissions assigned to specific other participants are considered a Control Domain (see associated section) consisting of resources such as records, files, processes, and applications.

Assignment of Trust Domains

Trust analysis (see neighboring section) is helpful to rank others from most to least trusted. Each of these participants also may share their ranking information, and that information is expected to be regularly updated. Participants in one's own trust rank list (ref associated section) take precedence of another person's ranking of the same participant. If the participant is not ranked on one's own list, the participant is searched for on trusted participant's list, looking at the most trusted participants for such information first. The rank on that persons list as a percentile will then be added to one's own list as implied trust in the same percentile position. However, if a participant appears on the other participant's list below that percentile who is also on one's personal list, then the person sinks in implied trust to immediately beneath that participant. Reference the Honor Assessments section for more detail.

Delegation of Control Domains

Resources controlled by a Zeronet (ZNET) control domain (see associated section) include display space, internet bandwidth, persistent memory, session memory, and user inputs. For Zeronet (ZNET) databases specific tables and records are expected to be controllable at the record row level to allow specific participants to edit

specific records as allowed. Participants delegate a specific amount of device resources to Zeronet (ZNET) which are used through control domains. Control domains (ref associated section) work by giving permission to the holder of a specific encryption key control over specific device resources through the control domain. Computer commands signed with that key or key delegated trust through that key will then be processed if enough resources are available as granted by control domain by the Zeronet (ZNET) device owner.

Essential Control Domains for Zeronet

Zeronet Device Control Domain

Each Zeronet (ZNET) participant is expected to create an encryption signing key which acts to control all device resources. One key could be used to control multiple devices owned by the participant. This control domain is used to dedicate device resources for Zeronet (ZNET) use. This control domain is expected to use those resources to set up a universal API capable of managing and sharing system resources over Zeronet (ZNET). The Netportal app is expected be able to manage this control domain, though it may also be managed by any application which supports this feature.

Zeronet App Control Domains

Netportal Control Domain  The Netportal app enables control over all parts of Zeronet (ZNET). The participant provides an encryption key belonging to their most trusted participant. Data from that source is then used to install the Netportal app. The Zeronet app provides an interface to set all control domains.

Zeronet Service Cog Control Domains

Each Zeronet (ZNET) service cog (see associated section) selected requests a specific amount of resources as a Control Domain (see associated section), which is then negotiated for approval by the participant. Upon Zeronet (ZNET) setup, a list of recommended Zeronet Service Cog (COG) services is offered based on the most trusted person. Participants are encouraged to assign a trusted system administrator to help with that process and answer any service cog or control domain questions.

Essential Service Cog Control Domains

Web of Trust Control Domain, Information Graph (IGGY), Democratic Communication (DCOM), Open Exchange (OX)

Resource Abuse Violations

Resource abuse could lead to missing money and other resources. Zeronet (ZNET) is expected to protect participants from technical security flaws by only allowing trusted participants to access resources through the Control Domain system (see that section nearby). However, participants must remain vigilant in keeping their trust of others in check. We encourage to

regular monitoring of resource flows including any digital money on their device to ensure that no abuse of trust is taking place. Upon a violation of trust, changing trust ratings and being more cautious with resource delegation may fix future problems.

Privacy-Transparency Balance:

Avatar Compartmentalization

Since all avatars known to be owned by one participant will share the same Web of Trust trust rankings of others by default, profiles might be recognized as having the same owner on the basis of their level of trust for various participants. There are various ways to protect against such spying activities. To reduce that type of spying, each avatar is expected to have interactions limited to specific topic domains. Bond is always eventually returned to the bond poster unless they violate their contract and either agree they violated the contract or their designated mediator and arbitrator agree the contract was violated. This compartmentalization may be able to be partially automated by setting Avatar Topic Range. Multiple avatars with separated trust rankings will be encouraged therefore in some mix such as personal, shopping, career topic, topic of favorite interest (outside of career), topics (plural) of other interests, and one avatar for each controversial topic interest. A statistical analysis service cog (COG) could then alert the user when avatars have substantial overlap in trust rankings as to be able to link them together.

Avatar Topic Range

When developing, contributing to, or otherwise interacting with specific topics including by commenting, tagging (ref Netportal:Content Tagging), and reviewing content, a different Avatar is expected to be automatically activated for ranges of topics based on the number of avatars available for the participant and other information. Specific topics also lead to a participant being encouraged to create an avatar for the topic for increased privacy.

Transparency Trust

Currently, most people regularly trust unknown computer programmers and technicians with their private information. Zeronet (ZNET) encourages ways for this trust to be explicit and controllable by actively encouraging transparency in methods. Furthermore, organizations often keep important information regarding their methods private for competitive reasons. Such organizations are expected to be disfavored by participants in favor of transparent organizations which share most of their ways of doing things with the general public, such as the exact method for determining what content to recommend for example. Zeronet (ZNET) is composed of people who agree to interact in ways that at least maintain social and ethical behavior, and may go

further to explicitly favor connections with people and organizations who match their moral values too. So, virtues and values of all organizations are encouraged to be shared in public through ethical shopping practices, increased involvement, and increased attention to transparency.

Privacy vs Public Transparency Classification

We wish to help people keep their identity secret to protect our right to remain silent, but at the same time, the more transparency that exists, the more trust there can be among participants. So, a balance is encouraged. This balance is done by classifying each type of information to private or public by each participant. Types of information expected to be private include information such as personal location information, personal health information, contact information, and most passwords and decryption keys. When such information is shared such as for public summary statistics, it is expected to accompany carefully controlled confidentiality agreements negotiated through a Data Negotiation Service (ref Web of Trust:Data Negotiation Service). Personal topics of interest are generally expected to be compartmentalized by the usage of multiple avatars by each participant for additional privacy. Topics of public transparency are expected to include any social contracts for each avatar (which may be different for each avatar) and partial information about commercial exchange contracts. Such contract information is shared so as to be able to post and receive public reviews to hold the other participant to account for their performance. Parts of a commercial contract generally expected to be made public are the avatar, the value of the contract, the person the contract is formed with, the mediator of the contract, the arbitrator of the contract, the agreed protocols of the contract, and information regarding the ongoing performance status of the contract.

Open Collaboration Trust:

Collaborative Content Peer Review

After Collaborative Content is published, it is expected to be reviewed by others. This review establishes the trustworthiness of that content on network reputation systems such as the Web of Trust.

Highest Trust as Rated Trust

When trusted people publicly honor content under peer review of a less trusted or untrusted person, the referenced content becomes the same level of trust as the trusted person. The statement of public honor also is expected to add honor to that less trusted person. Likewise, when someone trusted publicly dishonors content, the same effect applies in reverse to reduce trust.

Trusted vs. Untrusted Content

Below a certain trust threshold according to participant

preferences, content isn’t expected to display except as marked lower trust Competing Perspective Consideration.

Web of Trust Consensus:

Summary

Most importantly, Philosophic Perspective Matching (ref Caroasi:Rainbow Cooperative:Philosophic Perspective Matching) allows participants to cooperate with others. A participant may develop a Trust Perspective (ref Web of Trust:Perspective Development::Trust Perspective) enabling them to form organizational bonds. Organizational interactions are encouraged to develop proposals for allocating organization resources, collective expression, and collective action. For suggestions on how proposals can work, reference (Caroasi:Rainbow Cooperative:Proposal Development). Proposals are expected to be achieved by Consensus Negotiations. Reference (Caroasi:Rainbow Cooperative:Consensus Negotiations) for details.

Cooperative Consensus Topics

Trust Cohesor organizations such as Group Trust Consensus and Synchronization Service (GTS) (ref Web of Trust:Trust Information Sharing:Group Trust Synchronization and Consensus Service) build consensus on root identity and names of blockchains, claimchains, public writing encryption key matches, routing, protocol agreements, and other information important to participants security and well-being. Participants are encouraged to develop Rainbow Cooperative interest groups (ref Caroasi:Rainbow Cooperative), and using those to join or create Trust Group Synchronization and Consensus (GTS) organizations. These two platforms help a person form their perspective of Zeronet as a Trust Perspective Domain (ref Perspective Development:Trust Perspective Domain). The primary purpose of this for Zeronet (ZNET) is to form consensus on the definition of what information is honorable on Zeronet (ZNET), especially which reputation records are accepted as honorable and which cryptocurrency public ledgers are accepted as most valid. Reputation records are important so that people do not cooperate with malicious people who may want to use their resources for bad purposes like spamming. While this system could be used to "stick one’s head in the sand" regarding any number of events by forming a "consensus cult" which only acknowledges "cult content" while auto-ignoring content from "outsiders", the system is designed to form consensus on honorability of content for cooperating with those who agree on such honorability.

Crosslink Consensus

See the Crosslink (Information Graph:Network Synchronization:Crosslink Metacode) section for a definition of crosslinks and metacodes. A Metacode will most often represent a database, but can also represent a protocol, government, contractual agreement, or any

other information where the Metacode is a summary value used to develop consensus by crosslink. See Public Settlement Network:Claim and Transaction Validation for details on how crosslinks may be used to form a consensus.

Consensus of Claims Validation

(Ref Public Settlement Network:Claim and Transaction Validation.)

Conflict Resolution by Consensus

Each Zeronet (ZNET) participant may be involved with interactions including financial exchange and travel safety as they physically connect with other participants. Financial exchanges may be enforced by a governing body of the participants choice as they agree for purposes of more harmonious exchange. For such agreements to take place, a consensus first forms around which people belong to and control each governing group. This enables people to properly form contracts with arbitration and governing enforcement to resolve conflicts. Governing bodies, especially Dispute Resolution Organizations (DRO) wishing to have influence on Zeronet (ZNET) may join in the same way as any participant, which is expected to be the creation of a "public" writing and signature encryption key. The matching of a "public" Shareable Key to a specific organization relies mostly on the formation of consensus regarding which people are the rightful participants in which organizations so that random, malicious, or unwelcome people are not able to wrongfully act on behalf of an organization. For transaction with arbitration, consensus on definition of rules and governance is critical. Governing bodies are often expected to be listed on each participant’s Web of Trust. This information is used to assemble certain important governing databases such as geopolitical boundary databases. A governing body or any participant may publish such data using a Zeronet components like the Public Settlement Network (PSN). Each of these data records may be considered accurate or inaccurate to a specific participant, and honorability may be determined an information service. So, participants attempt to build consensus with each other on which records are most trusted. For example, flying a drone in a specific location may lead to a person being detained and their drone confiscated if a person were to receive inaccurate information regarding drone flight restrictions. So, developing a consensus on what areas are safe and which areas are unsafe for such activity could be extremely important. The Crosslink Consensus process described in that nearby section is encouraged to be used as the method of developing such consensus.

Alternative Consensus

When a participant has been accepting consensus agreements from a certain source, but discovers problems with the data set, they are expected to reject the

Metacode as invalid and attempt to form an alternative consensus. So, all Zeronet (ZNET) participants do not need full consensus for the network to operate. Rather, each participant develops the broadest available consensus which they agree with and participates with those people while generally ignoring others they disagree with (though still monitoring them through Competing Perspective Consideration ). See Netportal:Competing Perspective Consideration for details.

Contracts:

Contract

is when multiple participants exchange pledge(s). Multiple parties mutually agree to fulfill their conditional pledge(s).

Public Pledge

A participant publicly promising to fulfill a pledge. Unlike a contract, a pledge does not require an exchange of pledges.

Contract Alternative

Alternatives to a contract would be the other opportunities available for general success in life without the contract. This becomes important if a contract is unfulfilled.

Contract Criticality and Opportunity Expense

Contract Criticality is the difference in the state of well-being of each contract participant should the pledges be unfulfilled, in the context of available alternatives by each contract participant forming agreement with alternative providers. Opportunity expense would be a (nominal) value placed on this difference of fulfillment from any specific unfulfilled pledge to the most likely alternative. The larger the difference between a filled and unfilled pledge, the more critical the contract is.

Contract Cooperation or Duress

Contract cooperation is the ability of each participant of a contract to participate in the forming of the contract such as by authoring and modify each term of the agreement. Contract duress is the degree to which a party is being penalized or ostracized for failing to agree to each term of the contract, in consideration of alternative options.

Sense of Value Capacity

The degree to which each contract participant is capable of determining the trade value of the offering of the counterparty(ies) of a contract, in the context of an equitable trade. A child may have great difficulty in assessing values, which is one reason why contracts signed by children are typically considered invalid.

Negotiating Power

Combining the factors of contract alternative, contract cooperation, and sense of value determine the negotiating power of a participant to a contract. A

threshold of each element is needed for all contract participants for a valid contract. More accurate assessments of negotiating power lead to less conflict.

Contract Type

The type of agreement. A contract may be signed or oral. Furthermore, a contract may be expressed or implied. Therefore, the contract types are oral, signed, or implied. The possible contract categories are expected to be stored in the Information Graph (Iggy) and are determined by Web of Trust consensus (ref Web of Trust:Trust Information Sharing:Group Trust Synchronization and Consensus Service).

Contract Binding

A contract is binding upon a mutual agreement where the participants involved have negotiating power. A strongly bound contract is signed, a moderately bound contract is oral, and a weakly bound contract is implied.

Contract Seal

A personally identifying part of a contract designed to indicate that a contract is agreed to by a specific participant. On paper, this could include a raised/embossed stamp, a logo stamp, or another signature type.

Contract Terms of Enforcement

Depending on the value of the contract, usage of dispute resolution help is specified. The strongest possible contract would include all of the possible dispute resolution help options for a contract including multi-tiered dispute resolution appeal options. An invalid contract would specify that any form of dispute resolution help is disallowed by one or more participants. A weak contract might be missing any terms of enforcement.

Contract Strength

A strong contract should be both strongly bound (ref Contract Binding section nearby) and strongly enforced. A weak or invalid contract might be neither bound nor enforced.

Dispute Resolution Organization (DRO)

Participant promising to resolve disputes using such tactics as auditing, escrow, mediation, arbitration, contract enforcement, and physical force.

Arbitrator

The arbitrator is given final say in how any contract disputes should be best resolved. The arbitrator may be delegated authorization to use physical force to resolve a conflict among contract participants. This should be a different participant than the mediator.

Mediator

Participant who is assigned to assist contract participants to resolve their conflicts.

Escrow

Contract participant whose only role is to hold funds for other contract participants and then release those funds upon the terms of the contract being fulfilled, as

authorized by the participants of the contract or under any dispute as resolved by the auditor, mediator, and arbitrator. The escrow participant is expected to fulfill some mediation disputes such as whether or not an item is shipped based on provided tracking information.

Contract Auditor

Person assigned to assisting contract participants in measuring contract performance.

Claims Evaluator

A trusted agent that determines whether a technical claim is true or false. Applies to situations where a claim is either true or false according to the agreed math and/or logical rules, metrics, measurements, axioms, and a given data set that is available to all relevant participants of a given contract.

Contract Enforcer

Person who is guaranteed access to property to transfer that property to another participant in resolution of a conflict. Expected to be a different participant as the arbitrator and mediator in a contract.

Security Guard

Person who is given permission to restrict one's movement in the event that they are a danger to others. This person is expected to be a different person as the arbitrator and mediator in a contract. This person may be employed by contract participants.

Appeals Delegate

Participant delegated to resolve disagreements with judgments by any Dispute Resolution Organization (DRO). The primary Dispute Resolution Organization (DRO) is expected to honor the decisions of the appeals delegate Dispute Resolution Organization (DRO). There may be multiple tiers of appeal, and for contracts valued over specific amounts there should be such multiple tiers of appeal.

Pledges:

Public Pledge Claim

A formal pledge or claim for the public record. A pledge is expected to most often be a contract (ref nearby section) but may be another category as described here.

Public Pledge Claim Category

The Public Pledge Claim possible categories are stored in the Information Graph (Iggy). These may include such categories as social contract, transaction, goods warranty, service warranty, goods contract, service contract, rental contract, loan, business partnership, charity pledge, partnership contract, labor contract, performance warranty, collective contract, and exchange contract. See Web of Trust:Trust Information Sharing:Group Trust Synchronization and Consensus Service for details on how categories are developed by consensus.

Pledge Common Contract Term

Common contract terms are stored in the Information Graph (Iggy). Common topics of a pledge or contract and their associated metrics and objectives. Contract terms should reference all relevant communication protocols. Examples of common contract terms include cancellation options, timespan, and arbitration availability.

Public Pledge Evaluation

A formal evaluation of performance of a Public Pledge Claim. The evaluation should include measurements of contract performance for each term including metrics and objectives.

Summary Public Pledge Evaluation

A formal evaluation of performance of a public pledge claim consisting entirely of a binary decision of whether or not one or more pledges have been fulfilled.

Pledge Metric

Within a pledge, a measurement used to measure contract performance. An example of a pledge metric is "completion time in hours".

Pledge Objective

Within a pledge, a targeted state, behaviors, or feelings to be achieved by the pledge. Usually one word or a phrase such as "3" in reference to a 3 hour time metric contract.

Reviews:

Service Review

Service reviews are important to establishing Web of Trust rankings (see associated section). Participants are encouraged to use a formal and consistent review process for all Zeronet (ZNET) services so that quality issues can be resolved and poor quality services can be avoided if improvements are not achieved.

Service Audit

When a Zeronet (ZNET) service is to be done according to an predictable and exact set of metrics, the service can be audited. This is encouraged for all financial services on Zeronet (ZNET).

Triggered Review and Preplanned Review

A Triggered Review is a review done without a prior agreement to review because of being emotionally triggered by a positive or negative experience, or otherwise a spontaneous or unplanned decision to broadcast the review of a public pledge performance. A Preplanned Review is arranged under contract such that all people who participate as using a contract have guaranteed to conduct a performance review of the public pledge(s) of the contract. Preplanned reviews are encouraged for most contract types to promote good social behaviors and to set proper expectations for reliable trading experiences. Contract participants may be expected to receive review notifications as defined in a contract. Funds may be escrowed and then released upon the review completion as the contract specifies. Participants who fail to follow through with reviews

should expect a lower value to their information because their reviews are considered more like a Triggered Review as they wouldn't be expected to miss reviewing an extreme emotional experience as much as other experiences related to a Public pledge Claim.

External Review

A review done by someone who has no direct trading relationship with a participant or offering being reviewed other than any publicly stated funding related to the review process itself. So, an External Review is considered an independent reduced bias review, and may be either paid or unpaid.

Sponsored Review

A review where the recipient of an offering obtained a discount or other value in exchange for the review of content or an item. This is review type is considered moderately biased.

Paid Review

A review where a person reviews a contract performance in exchange for value. This is considered low biased if it is a pre-planned review as part of a contract in which a participants are always offered payment for reviews.

Public Honor

Honor points assigned to a person due their fulfillment of a public pledge, expected to affect their Web of Trust rank.

Review Data Flow

Review data is expected to be formatted according to Group Record Exchange (GREX (ref attachment) format and posted to a Public Content Network (PCN) Public Information Database Cog (ref Information Graph (Iggy), Database, and Search Cogs:Public Information Database).

Assurances:

Posting Surety Bond

There are multiple resolutions to the Privacy vs Decentralization Challenge. One method is that before being trusted with a resource, a participant is expected to Post Surety Bond which guarantees a range of behaviors such as cooperation to avoid malicious network attacks. Web of Trust participants are expected to be able to cooperate by easily forming contracts with each other. For formal contracts, participants are expected to designate a mediator, designate an arbitrator, and post bond. Posting Surety Bond is an activity that can be done anonymously and provides some assurance of behavior. For example, when selling bandwidth resource over Zeronet (ZNET), participants may be expected to attempt to halt traffic from people who claim to be harassed by the bandwidth (typically by technical network attacks such as DoS attacks). Participants may Post Surety Bond by relaying money to a mutually trusted participant with a guarantee that they won't participate in harassment. Should they violate the agreement, they

may lose some to all of the money. The trusted mediators and arbitrators are the people who determine if the agreement has been violated. Posting Surety Bond has potential to resolve any situation where damages are limited to the amount posted.

### Open-Ended and Close-Ended Surety Bonds

Surety Bonds may be limited to one specific contract as a close-ended, or be posted as a general assurance covering multiple contracts that may have yet to form as an open-ended bond. Each additional contract is expected to be known to all other contractors using that bond so that if the bond becomes divided into a high number of contracts, a contractor can request additional bond postage before signing the contract.

#### Surety Leverage.

In an Open-Ended Surety Bond, multiple contracts are formed under one bond. The participant who posts the bond limits to specific leverage. So, a 1oz silver bond may be limited to 8oz silver worth of contracts, so the leverage would be considered leverage of 8. This leverage is expected to be acceptable when contracting with participants who seem to have a history of trustworthy contract performance.

### Cohesor Organizations

As detailed by the (Caroasi:Rainbow Cooperative:Ringer-Cohesor-Guider Model:Cohesor) section, a Cohesor is an auditor who who helps determine consensus and enhance cooperation. The Web of Trust encourages many people to form organizations which accomplish this for purposes of helping validate information about participants while also protecting those participant’s privacy.

#### Negotiations Cohesor

A Negotiations Cohesor helps decide on routes of appeal when two people in a contract cannot agree on mediation or arbitration.

### Trust by Certification

A mutually trusted person, expected to often be a Cohesor Organization, may be tasked with validating claimed characteristics of a participant. Some participants want restrictions on behavior such as one avatar being controlled by one and only one physical body, or one avatar being associated with one specific "real" public identity. When participants agree to such limitations, they may do so by using Certification. It is expected that Posting Bond Surety is good enough for most Zeronet (ZNET) interactions, but for some relationships it may be considered an insufficient level of security. For such circumstances, certifications are expected to offer a higher degree of security, but in sacrifice of some degree of privacy.

### Limited Private Certification

When Zeronet (ZNET) participants wish to interact physically with each other they may want assurances of certain information being true. For example, someone who

is seeking a business partnership may want a picture of the prospect's claimed physical location to be confirmed as being recent and accurate. Or, if someone is considering a romantic meeting they may want to confirm a picture of someone is recent and accurate. With Limited Private Certification, a participant such as a Cohesor Organization determines certain information about an avatar. Additional possible uses include declaring an underlying dedicated physical body to an avatar, casting a vote, declaring loyalty or allegiance, or DNA diagnostics. A Limited Private Certification is generally a one-time (or otherwise limited) verification, test, or other information validation. So, the limit of the certification is the access to limited information regarding the participant by the certifier over time. Multiple identical certifications for the same person are restricted to maintain some privacy. Certification expiration is set by either the certification contract, or if no contract is in place then by the participant. The certification then includes expiration information. To prevent someone from completing a certification more than once (except when the certification expires), a custom hash of identifying data may be computed such as a series of photos and iris scans. That specific identifying information will prevent participants from completing the same certification multiple times. The certifier is expected to avoid recording any information that matches that hash data to the results of the certification, which provides privacy. The certifier may, upon request of the participant, sign a statement that does provide a match from certification to its specific avatar, and provide the participant with the one and only copy, so the participant does have that evidence of the specific match of avatar to certification result, should they wish to share it with others. So, the certifying person can then claim that a specific avatar completed specific requirements for certification, but not be able to say which physical body that avatar matched with without further information from the participant. In the case of voting, the certifying organization will also not be able to say which avatar casted which vote for secret ballots. The reason why privacy may be protected is that the participant seeking certification declares their avatar to associate the certification with, then the certifier stores an association with the avatar to the certification but does has the duty to avoid recording the "real identity" of the participant. A weakness of this system is that avatars can be used by people other than the person getting the certification.

Ongoing Certification

Ongoing certification is generally expected to be a public declaration of information offered by a trusted certifier where the certification expires and is then may be renewed as desired. The certifier verifies any

information according to their chosen domain of information. Examples of certification include administering an IQ test, verifying a participant's primary residence location, inspecting a bathroom for cleanliness, and confirming a contract is being completed as pledged. This service is expected to be used when physical property is being offered as bond, and for a declaration of defense of physical property. This service is also expected to be used when one's physical property (including a participant's physical body) is being placed under trust of another participant. This service may offer limited privacy because the certifier is often expected to be able to match an avatar to a physical body for purposes of arbitration judgments. The certifier may also accept a duty to ensure location information is current. The certifier is expected to be formed as a Data Negotiation Cog (COG) (ref Web of Trust:Data Negotiation Service) provider to restrict access to private information. The certifier may maintain contact data over time on the underlying physical body of a specific avatar. This data is released as agreed when conditions are met such as if a participant loses an arbitration case and property is to be transferred.

Proof of Humanity

For certain purposes, people may want to restrict participation to humans. Or, they may want to allow any intelligence except robot intelligence. One method of such proof is key signing. Key signing is where a public key is expected to be human. That human then signs statements that other humans write attesting to their humanity. These statements are made public and then evaluated through the Web of Trust. Proof of humanity is also expected to be done through certifying organizations. People could pay to have their biometric data scanned into the proprietary database of the certifying organization. That certifying organization would then be expected to save a specially designed hash of the data rather than the data itself and leave the actual full data scans with the participant. The organization then makes the fact that the participant is a human made available to all those who the participant wishes to know. Generally, this would be a public database that costs a small fee to access on an ongoing basis. The preferred method of identification is birth certificate only. However, there may also be photo, video, and voice recording. Those methods could be done by the participant them self. Retina, iris, fingerprint, body shape scan, can also be done by participants with the associated equipment. Body scans could be used for gaming and simulation purposes as well.

Data Negotiation Service:

Summary

Data Negotiation Service serves several purposes. The

primary purpose is to prevent monopolization of data by large organizations. This service also helps protect participants data from being transferred to potential adversaries when a participant does chose to share personal information. This service is designed to offer an alternative to intrusive spy advertising networks that would otherwise naturally form without it. Rather than having a spying network chose you as a target, it is expected to be preferred to have a trusted participant who shares data under your specific instructions only. We hope that Data Negotiation Service causes statistical information regarding, health, wealth, and well-being to be widely available that can be used for researchers which we hope to advance societal goals. Participation in surveys and polls is more controllable for all participants with Data Negotiation Service because each participant specifically manages all their information sharing with one specific trusted Data Negotiation Service provider. Participants may participate in reporting of various economic, health, and cultural information for summary statistics to forward social studies including economic health, personal health, and cultural enrichment. Information expected to be most commonly shared includes web searches, shopping decisions, content pulls (downloads), content pushes (uploads). The Data Negotiations Portal is expected to enable control over participant information distribution. See Service Cog:Web of Trust Cogs:Data Negotiations Cog for details.

Data Negotiation Service Selection

A participants Web of Trust is expected to be used to select trusted service partners to relay provided information without revealing personal identity. The partner chosen is expected to be an intelligent, generous, and honorable social group peer or community member (such as local or interest-group specific person) who makes their summary data available for a fixed price to any participant. Any Personal Protected Information (PPI) (ref Democratic Communication:Secrets Protocol:Secrecy:Protected Personal Information) is expected to be relayed only through their Data Negotiation Service. Related: Web of Trust:Privacy-Transparency Balance.

Data Negotiation by Avatar

Participants are expected to consider a different Data Negotiation Service for each avatar. This develops a separation of identity between avatars and the underlying person controlling them. Data Negotiation Service is expected to avoid attempting to connect avatars together to a single identity as doing so is considered a violation of duty to protect users identity to the degree possible. A Data Negotiation Service is expected to establish a public identifier number for each avatar which could allow advertisers to individually target a specific avatar.

Avatar Data Service
: is a Data Negotiation Service which stores avatar data at the instructions of a participant and then transmits avatar data upon request as approved by that user. The purpose of this service is to provide a way for participants to carefully manage their privacy, especially their contact information.

Commercial Advertising Access Negotiations
: Participants are expected to have a strong degree of control over receipt of commercial offers. Their Data Negotiation Service is expected to protect access to participant data to the degree that participant instruct the service. Participants are encouraged to enable at least some commercial offerings because this enables content creators to be better paid for their content, which means more and higher quality content will be available. Participants may appreciate at least some information about helpful offerings they would otherwise not find out about. For this reason, at least a minimal amount of advertising is considered a net positive for participants and moderate advertising levels are supported by Zeronet (ZNET). We also actively seek to reduce advertising deemed highly interruptive in negotiation or discussion among advertisers, content creators, and content evaluators. This negotiation process is encouraged to be acknowledged and considered to be done formally. Also, participants may be directly paid for review of commercial offers to ensure everyone a chance of mutual benefit with such advertising. It is also expected to be easy to directly replace sponsored advertising revenue with donations to the content creator. Endorsement advertising is more difficult to replace unless the content creator has included a system to replace endorsements with donations. This difficulty in removing endorsements gives an advantage to endorsed advertising because anti-social and greedy participants may remove as much advertising as possible while donating less than what their financial well-being morally obligates them to donate in the honor system.

Data Negotiation Service Advertising System
: Data Negotiation Service has most demographic and other information which a participant has shared with any organizational participant. When a participant loads content that contains advertising, a request for the appropriate advertisement is relayed to the Data Negotiation Service specifying the formatting of the advertisement. The Data Negotiation Service selects an advertiser on the Advertising Exchange (Adex) (Open Exchange:Standardized Exchanges:Advertising Exchange) which is the highest ad payout given the demographics of the participant, and relays the advertisement to the participant with a claim number for having delivered the advertisement. They relay a copy of that claim to their preferred Public Information Database Service Cog (Ref Service Cog:Information Graph, Database, and Search

Cogs:Public Database Cog). The expected process for advertising is for participants to either directly buy advertising them self using the Open Exchange (OX) or to indirectly buy advertising from an advertiser on the Advertisement Exchange (Adex). Content creators include embedded instructions for advertising in their content regarding where, when, and what types of advertising are to be displayed. Revenue directions and creation credit are also included as to who is expected to receive advertising revenues. This information is expected to be packaged as a content attachment for all content on Zeronet (ZNET). Any missing information is expected to be tagged in a collaborative effort to encourage content creation and reward.

Data Negotiation Data Validation by Conversion

Conversion statistics are used to help prevent fraud in advertising. Participants are encouraged to automatically report their purchases with their Data Negotiation Service based on an online advertisement because it encourages honesty in advertising, and therefore prioritizes content creator's ability to earn advertising money that the creators are expected to use for continued content creation. When an offering is accepted based on an advertisement, the participant automatically reports offering acceptance with the Data Negotiation Service and also the Data Negotiation Service of the advertiser, while the commercial participant also reports the acceptance to both their Data Negotiation Service and the acceptor's Data Negotiation Service.

Data Negotiations Privacy Violation

If a Data Negotiation Service were to ever sell data that they are not authorized to sell or sell data outside of the agreed contracted terms, the organization is expected to be dishonored and abandoned by all participants. A Data Negotiation Service is expected to be carefully trained or otherwise adept at information security. To prevent large-scale breaches, Data Negotiation Service is expected to be contained with an interest group domain or geographic location.

Data Negotiation Blind Encryption

When Data Negotiation Service is used for any authorizations, the associated encryption keys or passwords are expected to be Blind Encrypted (ref Democratic Communication:Secrets Protocol:Blind Encryption).

Survey Participation

All participants are encouraged to participate in statistical surveys or opinion polling because by doing so, we can accurately measure the success or failure of different aspects of society. Content creators who use this data are expected to show gratitude in any number of ways to participants who have provided this data while citing their sources. Surveys do take time to complete, but we hope that everyone involves them self

in providing feedback about their state of affairs so that we can collectively learn to improve society. Information about health can improve health and information about economics can improve economics. An example of economics would be offering review where if a participant makes a purchase, they sometimes agree in advance of a purchase to review the performance of the offering as part of their civic duty or for other reasons like a discounted purchase. An example of health would be offering feedback on how a proposed treatment for a sickness works for a specific participant.

Network Searching

Search Service Goodwill Forum

Data Negotiation Service (ref neighboring section) is expected by Zeronet (ZNET) participants to post each search query as an anonymous public post (unless a searcher marks the search as extreme privacy needed). See Democratic Communication:Public Messaging and Content:Public Messaging:Public Post for details about public posts.

Search Query Data Flows

Expected search data flow is first to the Data Negotiations Service who relays the search query to a Topic Search Cog (ref Information Graph Cogs:Database and Search Cogs:Topic Search Cog) and Public Information Database Cogs (ref Service Cog:Information Graph Cogs:Public Information Database Cog) who wish to have a database of internet searches. The Public Information Database Cog updates the search count with Data Discovery and Synchronization Database Cogs (Disco) (ref Service Cog:Web of Trust:Data Discovery and Synchronization Cog) who keep counts of search records. The Topic Search Cog then processes the search and relays the result set to the searching participant. That data is then filtered according to their Web of Trust and expected to be displayed on the participant's Netportal search query portal (Ref Netportal:Portals to Replace Websites). The result set is rated by the participant much of the time. This rating is relayed to the Data Negotiations Service and also relayed to the Topic Search Cog. The Data negotiations Service sends the data to any subscribing Public Information Database Cogs where the review is stored.

DEMOCRATIC COMMUNICATION (DCOM):

General Concepts:

Protocol Definition

In the context of Zeronet (ZNET) the word "protocol" describes a voluntary communications method based on consensus or widespread adaption.

Protocol Consensus

Forming agreement on the meaning of words, symbols, and

language is the most important step of Zeronet (ZNET) participation because it defines Zeronet (ZNET) itself. By default the protocol used to communicate with other network participants is encouraged to be with their most preferred protocol accepted as valid and "comfortable". Protocol preferences are expected to be developed with a profile record that is shared either publicly or privately. If the record is valid and honorable by another participant, then then the two participants can communicate with one another on Zeronet (ZNET). If the protocol record is unknown to the participant and peers (as evidenced by not being in a shared database), then a manual review would have to take place for the participant to determine the acceptability of this unknown protocol proposal. If accepted, then the record will be adopted and may be shared with peers as agreed. As the record is accepted by more participants, a wider consensus of protocol develops. After enough people have accepted the protocol, it may achieve the broadest known consensus and then be used as the preferred protocol, but until that point still may be used to communicate with people who disagree with the broadest known consensus protocol but do agree with a less popular protocol.

Comprehensibility Overhaul

Much of computer programming is perceived as "reinventing the wheel" by programmers. Zeronet (ZNET) involves an aggressive expansive reinvention of much of the internet. However, there is expected to be great benefits in doing so. By prioritizing the ease at which each Zeronet (ZNET) protocol can be learned, the number of developers is expansive. Zeronet (ZNET) is meant to be a highly inclusive platform to give opportunity to as many people as possible to participate. With rapid calculation now fitting in any pocket, considerations for efficiency can be much lower while considerations for system comprehension using plain language and plain text can allow more security and more programming participation. The more people who can understand a computer code, the easier it is to confirm the security of the code.

Content Types (Metaclass)

Zeronet (ZNET) content types (also considered "metaclass") include video, audio, interactive (including executable and script), document(text & images), plain text, simple text message, survey, Group Records Exchange (GREX) (ref attachment) record, and any number of other custom types. All content classifications are expected to be listed on the Information Graph (Iggy).

Interactive Content

Examples of interactive content include Zeronet (ZNET) portals (replaces websites), surveys, data entry forms, a calculator, any app, and any video game. Executables may be remotely executed, which is generally done for

proprietary or high computing resource loads. Or, the execution may be local for open-source applications when the computing resource load can be handled by the participant.

Private Messaging: Postage

Participants are expected to set a postage rate to send them private messages using an interface such as Message Portal (ref Netportal:Portals:Messaging Portal). Participants set a public postage rate either for their entire system or by avatar. Postage is set by participants limit unwanted messages like spam. This postage is expected to be relayed as a token through the participant's messaging delegated private message service.

Private Messaging: Mutual Exchange Content (Mutual Messaging)

In order to send a message to a participants Zeronet (ZNET) private metastream (like an "inbox"), any fee set by the recipient must be sent along with the message. This postage is expected to be returned if the message was received and found to be valuable. As a security feature, substantial postage is suggested to be required for everyone because if a trusted participant is hacked, the hacker would be able to spread malicious content more easily. If a hack is suspected such as receipt of a malicious message from a trusted person, postage isn't returned as a way to communicate a security problem. After a hacked device is resecured, the postage can after that point be returned. A calender-linked process is expected to handle automatic returns of postage including how to handle vacations.

Postage Tokens:

Each participant who wishes to be contactable for individualized private messages may create their own contact token packs using their Web of Trust functionality. The token applies to one or more channeling methods including text, video, audio, and any combination thereof. For a public contact, the tokens are sold at a set price which is expected to be refunded should the participant find the contacting person to offer sufficiently valuable interaction. See "Token Pack Service" section for details about how it may work.

Public Messaging:

Public Post

A public post is a message with an unlimited target audience. These messages may be pushed (uploaded) to a public databases such as a Public Information Database (ref Service Cog:Information Graph Cogs:Public Information Database Cog) and announced as available by sending a reference to a Data Discovery Service (Disco). Public Messaging categories are set by Group Records Exchange (GREX) (ref attachment).

Broadcasters

are participants who distribute messages or content over

Zeronet (ZNET). The Public Settlement Network and Public Content Network heavily rely on broadcasters for content distribution. All participants are encouraged to broadcast Zeronet (ZNET) content of some type although they can change their settings to avoid that.

Retrocast Messaging Summary

The purpose of retrocast data is to prioritize ability for people across a wide geography to access content simultaneously for intentionally timed messages and also to prove certain content was created before a certain point in time. Releases may also be staged so that participants cannot skip to the end of a data set.

1 Data is encrypted according to an shareable encryption key. Or, the hash of the data may be released but not yet the full data itself.

2 If a certain release time is targeted, that time is stated as the target release time. A data set could contain multiple release times for staged releases.

3 For a fully timed release such as for transactions, only after the sender is satisfied with the number of recipients, is the full data is released.

4 Decryption instructions to unscramble any scrambled data, and any unsent data to complete the data set, are released as close to the target release time as possible.

5 Messaging, especially decryption instructions, may be timed according to expected latencies such that recipients receive messages closer to simultaneously.

Language Choice

All symbol and word meaning is based on the most commonly believed definition according to the target receivers of the message, unless otherwise redefined in the message. Language choice should be that of the message receiver rather than the sender when the language is known.

Implied Context

Where message context is implied, or symbols or words are omitted, the receiver is to guess the context and request any context not understood. For example "Meet me today at 12:00PM Central Standard Time for lunch in our workplace cafeteria." may be restated as "Meet me at 12 for lunch" given the context that the sender and receiver are humans on planet Earth who have eaten lunch together two days in a row at the same cafeteria and there is now an invitation for a third meeting.

Abbreviations should only be used after the target audience is given at least one abbreviated version. In a training/reference text where it is presumed that people will read only parts of the document as needed for practical understanding, both the full and abbreviated versions together are expected for future understanding of the abbreviation.

Privacy

People are sometimes hostile, so privacy is important. Communications spying enables hostile others to gain a harmful advantage over us in general. It also can

incentivize normally friendly people to act to take advantage of valuable information. Temptation of others should be avoided. So, communications should be encrypted where feasible. When someone directs a message at a specific audience rather than the general public, effort should be expended so that only the targeted receivers get the message. Furthermore, the contact information and location information of any person are considered personal, and should only be shared with permission of the owner. Implied permission should only happen when there is a clear reason to believe that the permission has been given beyond "I know this person well and therefore have permission to give their information". That is wrong. Only when there is a perception that the information holder wishes for certain contact to be shared should the information be shared. Today, those who most intensely say "If you have nothing to hide, share everything you know!" often act as agents for those with the greatest number of secrets including military and fiat government organizations. It is those organizations who keep too many secrets.

Overview:

Encryption Summary

is communicating in a scrambled message code so that messages are only understood by the target audience. See neighboring Encryption Terms sections for more details.

Identity Information Summary

A Zeronet (ZNET) identity is a source of information formally established simply through the creation of a set of encryption keys without any other information necessary. See neighboring Identity Information section for more details.

Contact Security Section

Protocol Establishment Section

Cooperative Development Summary

Zeronet (ZNET) participants are expected to cooperate together by forming Zeronet organizations. Zeronet (ZNET) aims to replace Intellectual Property government systems with a much more efficient system of incentives through carefully crediting contributors, leading to donations and advertising revenue incentives through an honor system. See Cooperative Development section for details.

Conflict Resolution

Title Resolution

Title resolution establishes agreement on names, definitions, and contact directions,

Zeronet Protocol (Zerp) Summary

All Zeronet (ZNET) communications are expected to involve establishing agreement on protocols. Many existing protocols are recommended to be adopted for Zeronet (ZNET). Some of them are recommended to be modified for Zeronet (ZNET). Many of them are intended to be replaced entirely with more fitting protocols.

This section includes methods for Distributed Computing, Data Traffic Strategies, Network Connectivity, and Topic Searches. The section also describes how Zeronet (ZNET) is expected to focus development efforts over time. See Zeronet Protocol section for more details.

Security Suggestions

Secrets Protocol (Sproc) Summary

This protocol is a set of methods and suggestions for enhancing privacy and security both on Zeronet and in general. Exercising freedom of speech may put people at risk of persecution in places of hostility and wrongful censorship. People may want to avoid having speech connected to them by police agencies or other hostile people operating in tyrannical jurisdictions. Additionally, there is speech that people would be willing to share with some people, but not the general public. There is expression that is willing to be developed in exchange for money, but not given away for free. Secrets are also important for banking and authentication of identity. The Zeronet (ZNET) supports all such efforts in part using the Secrets Protocol (Sproc). This protocol establishes techniques of sending and receiving information anonymously, and likewise remain anonymous as a member of a group. This protocol also includes ways of identifying secret leak sources in an effort to contain future leaks of secret information. See the Secrets Protocol (Sproc) section for details. Usage of Encryption is outlined by the Secrets Protocol:Privacy by Encryption section. Organizational privacy is encouraged as detailed in the Secrets Protocol:Organizational Privacy section. Messages can be distributed globally with almost no risk identity unmasking using strategies outlined in the section Secrets Protocol:Security in Numbers and also the section Secrets Protocol:Security in Numbers:Local-Global Wheel (Loglo).

Physical Security

Use open Delivery for secretive and secure logistics including pickups and deliveries. See the Open Exchange:Open Delivery Section for details.

Plain Text Protocol (PTEX) Summary

Ease of understandability is helpful for transparency and information security. A text format that is meant to prioritize and satisfy readability and ease of authorship, with suggestions for formatting text documents to be displayed on Netportal. The formatting includes organization of text into a tiered hierarchy that assigns titles to specific content. See Plain Text Protocol (PTEX) section for details. This includes Group Records Exchange (GREX) (ref attachment) which is a common record format

Group Records Exchange Protocol Summary

Multiple organizations are encouraged to use the same data formatting for their database records, for the purpose of sharing those records. This is a method

under Plain Text Protocol (PTEX) for Zeronet (ZNET) services to freely exchange records with one another. Organizations use an identical file format for common records such as personal identity records. This allows data to be shared seamlessly by multiple data service providers. See the Group Records Exchange Protocol (GREX) section as an attachment for details.

Encryption Terms:

Cryptosignature, Digital Signature
: A series of symbols proving who authored certain messages or content, by proving which Shareable Key (ref that section nearby) was used to create the encrypted content.

Crypto Key
: A digital code used for secure communication.

Crypto Key Set
: A set of crypto keys. Multiple keys are needed with sharing key encryption... one "sharing" key is freely shared to anyone wishes to privately exchange messages, while the other "heritage" key is secretively kept. The shared key is used to send messages to a participant or interpret the included codes to verify that they wrote the message, while the secretive key is used to read the messages or add codes to the message to prove they wrote the message.

Sharing Key
: Shareable encryption instructions enabling a person to write encrypted messages to the person with the matching heritage ("private") key. This is more often called a "public key" but the term is misleading when a "public key" has not been and will never be public information.

  Sharing Publication Key
  : A shareable key used for everyone to write encrypted messages to a specific person.

  Sharing Verification Key
  : A shareable key used for everyone to verify the cryptosignature of a specific keyholder.

Heritage Key
: Instructions for decrypting messages sent using a creation key. This is currently called the Private Key. Because a "private key" could be publicized making the key name confusing, we call it instead the "heritage key". This is renamed the "heritage key" so people will be less inclined to mistakenly share it.

  Heritage Passcode Key
  : A key used by a specific person allowing the keyholder to read the encrypted messages, and by some methods also to write a message to others.

  Heritage Signing Key
  : A key used by a specific person allowing the keyholder to sign a message.

Buddy Key
: For communications with one other person, a shared encryption key. For ongoing communications it is

expected to be paired with an avatar identifier. The key may be generated based on a hard to guess circumstance under which the pair meet to be regenerated by memory.

Group Key

Like a buddy key except limited to two or more other people.

Contact Key

Single or limited use key to begin communications with someone. Used so that you can give contact information without excessive risk of unwanted messages or unwanted contacts. The key is enabled by a person until either they are contacted successfully or the key otherwise ends its service life.

Scrambler Keys

A shared secret code used to scramble an unscrambled message or scrambled an unscrambled message. Anyone who knows the code may unscramble the message. Traditionally called a "symmetric encryption key".

Asymmetric Key

A key split into shared and unshared parts (see nearby Heritage Key and Sharing Key sections). The shared part is instructions for the message sender to scramble the message. The unshared part is for the receiver to unscramble the message. Only knowing the unshared part enables the message to be unscrambled. Knowing the shared part is of minimal help to unscramble the message.

Identity Information:

Avatar

Avatars are a form of personal identification that can allow privacy, especially while participating in group activities. Participants assign them self any name of their choice to be called by others. Avatars are also used as a way of pretending to be another person for example to play a game. All people have the freedom of expression and so may identify them self using any name as a natural right.

Public Personal Identifier

is a dominant name as designated by most trusted people or one’s self to represent one individual person. Currently, Governments seek to assign people a "real name" as their negotiated and shared identifier reference based on the choice of parents, then lock control as a name authority over the person. On Zeronet (ZNET), all people may have one or more identifiers, with their root identifier (detailed section nearby) being any one of their choice. If the identifier or associated identifier name is not unique, more symbols may be attached to render the name unique when others note their name in their records. For example, a birthday, a place of birth, or a place of residence (ie "Jesus of Nazareth, Year 0"). Identity is sometimes shortened/compressed such that context may become necessary for name recognition such as calling someone by their first name only. While identity is generally

non-negotiable because all identifiers are personal opinion, names are to some degree negotiations between each personal identity and the potential identifiers. All people have the freedom of expression to match any identity with any name as a natural right.

IP Contact Point

A private contact point using an IP may match an avatar name to an IP address and encryption key for a contact.

Hash, Digital Hash

A series of characters calculated from specific content that is expected to be unique and randomized. Hashes are used used as an identifier to refer to specific content. The symbols are approximately randomly distributed by the algorithm that generates them with the hash calculations.

Identifier (ID)

A code for referring to an entity such as a message, transaction, agent, etc.

Identifier Hash, Hash Tag

An identifier creating by using a digital hash of content. This allows for fast searching through information that is "hash tagged".

Participant Identifier Tag

A participant using a publicly shared encryption key can be identified by their shared encryption key or a hash of that key.

Short ID (SID)

The minimum number of characters in a hash to be unique at the time of its creation. A Short ID (SID) may also be unique within a specific domain. Considers the first characters first. A reference database is either assumed or directly stated. The hash of a message is calculated. The minimum number of ending characters of the hash to be a known unique message identifier becomes the Short ID(SID).

Namespace

A domain in which a specific set of names correspond with a specific set of meanings. Any given language can be considered a namespace.

Public Short ID

A short ID (SID) based on a public registry of IDs.

Party

A specific person or a specific group of people.

Avatar Name

Everyone on Zeronet (ZNET) can assign them self any name they wish, and also assign others names such as using Web of Trust may internally on their computer call other people by specific names, but then are expected to directly call them their preferred name when they contact the other person directly. So, there is a list matching one unique internal name to a corresponding external contact name or contract address (such as encryption Shareable Key (see nearby section) and identity contact reference). This allows other people to (internally) use Avatar names that are unique and allows

people to nickname other people without necessarily calling them that directly. By default the unique name assigned to them will be their preferred name followed by a number, but the participant is expected to edit that name. Each participant is encouraged to create differences between Avatars details such as avatar picture so that similar names doesn't create confusion. Participants may create multiple identity tables for different purposes.

Avatar Identifier

Avatars are used to access Zeronet (ZNET) information systems. A unique component of a Web of Trust avatar for identification purposes is the public encryption key. While the profile may change over time, the first time the public profile is hashed, that hash is expected to always be used as the identifying code (ID) for reference. The hash includes all readily available data for the avatar, especially the encryption key. The hash becomes especially important if an avatar's encryption key is voided or changed. So, the hash of all avatar public data including encryption key(s) are considered the Avatar Identifier.

Identity Privacy

People are expected to provide other people's avatar identifiers and other contact information only with permission of all contacts involved. Also, multiple avatars are encouraged to be used for different types of interactions for each major interest for each participant to prioritize and satisfy privacy. So, Avatars are expected to be compartmentalized according to the topic interest of each avatar.

Avatar Public Record

A participant may broadcast their existence as a network participant with a cryptosigned profile. Each participant who wishes to publish a public avatar is expected to post their profile with their favorite Zeronet (ZNET) topic interest group.

Zeronet Root Identifier

Participants on the Zeronet (ZNET) create their own root identifier. A root identifier can either be individual person or collective of people. This identity is considered to be able to have multiple other identifiers, but other identifiers are not considered owners of a root identity. This root identifier is encouraged to be a reference to a specific cryptosignature key, specifically the hash of such a key. A collective identifier uses a web of trust to link people and contact points to specific shared cryptographic key or static data content. Root identifiers allow full anonymity but do not necessarily allow a change of cryptographic key or signature confirmation, while other identifier types may be more dynamic.

Anonymity Encouragement

The Zeronet (ZNET) is an anonymous-capable network and

encourages participants to maintain a high level of privacy to keep everyone safe.

Identity Change of Key

A key change for an individual root identity can only take place when alternate keys are defined in advance. This is done by releasing alternative Heritage Key (ref neighboring Encryption Terms section) before a key changes.

Identity Backup Key

A backup key allows any identity to change keys by using an encrypted message creating with a backup key to create a new key or keyset. This process will also work with root identities if the change is accepted by peers.

Identity Termination of Key

A Shareable Key (ref neighboring Encryption Terms section) may be considered ended on a specific time by a cryptosigned declaration of the key being ended. Any "expiration date" of a key is not considered valid until such a declaration is published and cryptosigned by that key. The reason is that Zeronet (ZNET) keys are expected to be held forever without an expiration date unless the Avatar is linked to one human being, and that human being physically dies.

Avatar Death

If activity is expected to permanently cease from an all active Shareable Keys (ref neighboring Encryption Terms section) of an avatar such as by a loss of the key(s), the avatar linked to that Shareable Key is considered dead.

Hard Forked Identity, Reincarnated Identity

If a participants encryption keys associated to an avatar are all lost or stolen, they are expected to generate a new key and use the new key to claim the previous identity to be their own as a reincarnation. The new identity is not expected to be able to directly transfer any property as if they are the previous key user. However, they may have property transferred to them as if they are the previous key holder after evidence is sufficient to the relevant people to be accepted as the previous keyholder, and the property appears to have been abandoned otherwise, at the discretion of those participants. Zeronet (ZNET) has little support for hard forked identities because the encryption key is considered part of the root identity. Forked identities are considered rumors of a "previous life" on the Zeronet (ZNET). So, avoid theft and hacking of your keys with many security precautions. Don’t lose your key, or you sort of lose your Zeronet (ZNET) "life" and must then begin a new "life".

Independent Avatar and Proprietary Avatar

A proprietary avatar is used to access one system designed for a specific purpose. Using a proprietary avatar, the avatar record is exclusively generated and stored not by the avatar holder but rather another person. An independent avatar is used to across the

different systems of multiple domains. An independent avatar generally proves identity by cryptosigning a login prompt or other statements including content requests, and those signatures are accepted as proof they are a specific person. An independent avatar is a record generated by their own (client) system based on a public encryption key as proof of avatar ownership. Zeronet (ZNET) encourages independent avatars while discouraging proprietary avatars. This eliminates the need for signups on Zeronet (ZNET) as participants are able to sign them self up simply by declaring a public signature key.

Client Avatar Privacy

Under an honor system, information system providers do not permanently store independent avatar profiles remotely except as indicated by the user. These records are transmitted as wanted by the user client system or a third party avatar records system controlled by the user. This system my apply to systems that provide public avatar information on demand, where information systems are instructed to be set up in such a way that avatar data is not automatically stored for the long-term. An example of an application of this system would be to a get price quote depending on certain personal information, especially health insurance where data is better if unremembered by other parties for security reasons. This would only be a reliable system where such parties are audited by mutually selected independent agencies to check for stored data.

Contact Security Considerations:

Topic Interest Pool

Most interest pools tend to be widely diffused globally because people have vast numbers of specific interests some of which are quite rare. There may be many more people in a local area than the number of topics in existence. So, find sufficient number of locally interested people is a challenge. This leads to a privacy challenge whereby if you discover evidence of a rare interest in a specific area, its easily matched to a specific person. This quickly compounds with multiple rare interests that collectively identify a person. A partial resolution to this issue in terms of presence on the internet is the Single Interest Identity. See that nearby section for details.

Single Interest Identity

Fully anonymous avatars which are persistently used are based entirely on one and only one topic of interest. That interest could be one virtue or value, topic domain, etc. The participant loads different content using different avatars. The complete history of the avatar can be made to be copied so that other people can assume a functionally identical perspective and so appear as the same person though with a different avatar name. Internet traffic routing may be automatically different for each avatar for

the highest level of security. Each participant is encouraged to use many Avatars to prioritize an satisfy their privacy.

Public Avatar

With a public avatar, the heritage key ("private key") is shared to the public domain. Any person can then assume the identity of that public avatar. This process may enable full anonymity, though the avatar usage becomes limited because its behaviors cannot be predicted. Some hostile people would be expected to control such an avatar.

Shared Avatar

With a shared avatar, the reading "private" key is shared among a group of people. Any person in the group assumes the identity, giving a higher level of anonymity than if only one person had access to the avatar. Anyone could transfer assets owned by this shared avatar to another avatar of their choice, so this is best used for avatars that do not control specific properties, either virtual or real. However, if exceptionally high levels of trust are earned and warranted, people may used a shared avatar even when such an avatar controls valuable assets.

Guest Avatar

A new encryption key (including read and Shareable Key) for a participant is generated for one browsing session. This helps grant anonymity to users.

Contact Information

Advertising a way to contact you creates risks of hostile or malicious opponents contacting you. So, listing your contact information should be done using all available security steps such as Zeronet (ZNET) Democratic Communication (DCOM) Contact keys (ref Encryption Terms section). When the contact identity is an avatar, it could be linked to your root identity in the Web of Trust, so this should be done just as carefully. Personal information may be an asset or a liability, so thinking about how this information will be used is important. It is recommended that you have a trusted mentor help decide what contact information you make public. Primary contact information may include any or all of your location information and contact numbers. Secondary contact information is personal relationships and organizational relationships and those people’s primary information. All information has some chance of revealing its creator. So, privacy and publicity are to be balanced.

Identity Contact Reference

Participants store methods to contact other people on their computer as a contact database. Participants are also encouraged to store encrypted copies of this database remotely and keep that database synced with their local copy. The contact database has an identity contact table. Each identity consists of a contact identifier which is typically computed as a hash of the

participants original public avatar profile or their encryption key. If the original avatar data is not available then the first known profile connected to the identity is used instead. If a person reveals they are owner of multiple avatars and states a root identity, the association is recorded as hierarchal secondary information. So, the root identity is marked as root identity, then the associated avatars associate with that root identity. Each avatar may also be considered to control other identities as a data tree structure. Each participant may assign a different unique name to each contact.

Protocol Establishment:

Protocol Declaration

A document associated with an identifier declares preferred protocol specifications. The document is expected to reference the source of those specifications. Common declarations include start date and expiration date. This document is cryptosigned by participants as a factor to indicate their support for the protocol, and may be referred to by its hash. The Protocol Declaration document is expected to be public and widely distributed.

Protocol Specification

A document specifying a method of communications to be used by the message author. This may include references to protocol packages, including Protocol Declarations and any settings or other specifications used with those packages. It may include encryption algorithm selection and the settings for that algorithm. This Protocol Specification (PS) document may be referred to by its hash. Any type of protocol can be specified including English, PGP, and x86 assembly.

Protocol Package

A full set of files which may include messaging and encryption applications. This package may include references to a protocol source package.

Protocol Build Package

High-level computer code which can be compiled for a protocol package with commonly available software and hardware. It is considered more secure to have source code that builds to a protocol package.

Character

In the context of communications, a character is a letter, number, or other symbol treated as one semantic entity.

Avatar Data Service Cog

is a cog that manages participant profile data for privacy protection. See Service Cog section for details.

Cooperative Development:

Contract Agreement Communications

Participants are encouraged to form agreement on behaviors including communications behaviors. Such

agreements may be established through systems such as the Web of Trust and participation in Rainbow Civics. (see Caroasi:Rainbow Cooperative).

Contract Foundation:

Conduct Contract

Participants who consider trading with each other negotiate an agreement on a set of rules and regulations expected to be followed by all contract participants. This may reference a common set of rules or regulations or any alternative concepts the participants imagine. Collectives forming a contract with other collectives may be expected to agree to more rules and regulations than individuals than otherwise because the contract can be processed reviewed by multiple people having different types of expertise by each contract participant.

Declaration of Force Initiation

The scope of this declaration of contract enforcement is expected to be declared so that it may apply to a range of specific contracts, or all contracts as specified. Participants declare circumstances which they will consider physical force which might be destructive or interfering to achieve their (contract) objectives. For example, someone may declare them self to be a pacifist, where a pacifist has no determination to use damaging force against another person under any circumstance. Another example would be a declaration of being a despot, which is a person who has every determination to use force causing damage to another person to achieve any goal upon any will of the announcer. Another example would be someone who agrees to use force only in accordance with the non-aggression principle (NAP). These declarations are generally based upon a universal consensus of morality, which is generally based on game theory, which is generally based on our instincts of fairness, which may be considered based on connection to a higher power or other spiritual entity. These declarations are expected to include declaration of natural rights and ethics, where those beliefs would generally be expected to be defended by physical force. Each participant is expected to post such a declaration so others can create contracts with expansive information about how the contract may expected to be enforced if at all. This is expected to be part of Conduct Contract terms (ref section nearby).

Governing Civil Code

This is part of the Conduct Contract (ref section nearby). As with a Declaration of Force Initiation, the scope of contract enforcement is expected to be declared either to a range of specific contracts or to all contracts with those participants. This contract defines governing or "self-governing" behaviors for a participant. Participants may

voluntarily govern each other as in a civilization. These voluntary social contracts may govern social and economic behavior. Participants may request or declare participation in a specific contract, and then their participation might be acknowledged or rejected by the other participants depending on successful negotiations by the participants involved. These contracts may involve claims of certifying authorities, where participants consider acknowledgment by those claimed authorities important to accept the contract as valid. For example, an organization named "UL" could be a trusted authority to certify an item to be safe for household use. Forced participation by people who overpower others to force them to behave either for or against their result in an invalid contract. This includes imposing rules on someone by force for being in a specific region or associating with a certain group of people.

Service Offering Collaboration

For purposes of Zeronet (ZNET), organizations of many participants are expected to perform cooperatives for services which require a large resource pool to achieve. For example, Content Evaluation Service (ref Public Content Network:Content Distribution:Content Analytics:Content Evaluation section) is resource intensive because there is much data available from every Zeronet (ZNET) participant that each participant values differently. Cooperatives are expected to form for services requiring large databases including metastream (ref Public Content Network:Key Features:Metastream) provision and topic searches. Other cooperatives expected to form include transaction databases, open exchange databases, secure message distribution, content classification, content metadata tagging (ref Netportal:Content Tagging), and content ranking services so that service providers (especially metastream providers and topic search providers) can offer content meeting quality guidelines requested by their clients. Organizations are expected to form to offer advertising services to match advertising with the appropriate audiences.

Collaboration Encouragement

Collaboration creates good bonds with other people on Zeronet (ZNET) for proper security and accurate information. Each participant is expected to be part of organizations that operate by consensus. If they strongly disagree on any substantial issue, they are expected to leave the organization in favor of a new one, which they may create them self.

Collaborative Resource Allocation by Consensus

Cooperative Consensus is useful for allocating organizational resources to achieve the purposes of the organization.

Cooperative Development: Creative Content Credit

Creative Credit

Good content is expected to be paid for at least by donation, so credit for development done is important. When a creator submits content, they are noted as the original content creator. When a content is edited, all people involved are expected to be listed as collaborators. Generally the order listed will be the order of most data contributed. However, the original author may allocate more or less credit as they believe due. Modifiers may likewise allocate credit to comodifiers who did not directly submit their own content.

Content Credit Distribution Profile

Content creators and content evaluators are expected to evaluate content to estimate a distribution of creative credit to the content creators involved for the purpose of assigning reward fractions. This credit profile is expected to affect content donation flows. Donors who award content creators can also suggest a credit distribution profile, though it isn't expected to be given as much attention as an expert evaluation. The original content creator's own self-assessment is expected to be given the most attention.

Shared Credit

When someone modifies content, they are expected to be cited as being a creator. Credit is considered to be the percentage of data submitted under a specific title up to the amount the original creator contributed unless otherwise granted by that original creator.

Software Creation Credit

When creation software is used, it is expected to be cited in credits. If the software is AI generation trained on prior works, then only a fraction of that donation credit such as 15% then going to the software creator if the creation software is open source. If closed source, then instead a donation of half that amount should instead be rechanneled to an open-source initiative (ref Open Collaboration Incentives).

Stock Works

If an creator creates their own content for the purpose of being modified or reused for more complete or other content, the resulting works may mark the base content as Stock Works. This would be the case when for example someone begins work by creating a general outline of something that is to be later detailed. It would also be the case for content that consists of questions where answers are to be the main content. So, another content creator may take the content and after editing or appending to it, the content creator of the resulting works claim and are considered an original content source while crediting to the inspiring content creator, although such credit may be honorably ignored by at the will of both the stock works and the inspired content creator.

Default Credit

Differences between original work and it's derived work are estimated to determine the percentage of content that has been changed or added to. The original submitter will be considered the largest contributor unless they grant otherwise.

Granted Credit

When someone has a high percentage of data submitted to a specific content, but considers them self a lower value contributor because of the higher quality of data by other creators, they should grant higher credit to other specific creators. They announce which authors have the higher credit.

Citations

When someone uses another creator's content as part of their own, they are expected to list the other creators involved unless there is a request otherwise.

Collaborative Content Trust

Collaborator trust determines which authors are trusted as content sources by each participant. See the Web of Trust section for more information.

Content Patch

When content is modified the creative credit can be modified accordingly. See Collaborative Development:Open Collaboration Protocol:Content Patch section for details.

Intangible Content

Examples of physical (or tangible) content include apples, monkeys, shirts, water, air, and hammers. Intangible content is something other than physical (or tangible). Examples of intangible content include cooking instructions, what a monkey did as written, directions for tailoring a shirt, a historic recording of fact that someone swam the Amazon River, the process of bottling water, a breathing meditation technique, and the way someone hammers a nail. Intangible content can also be ordinary actions such as eating an apple, watching a monkey, or putting on a shirt, so long as that action is shareable with others such as by a stage performance. Intangible content is something that can be copied purely by one's actions. Copying is never stealing as the Intangible Property (IP aka intellectual property, intangible content) law concept erroneously claims, so we find many alternative ways of rewarding creative people for their valued creativity. Morality really does work, and Zeronet (ZNET) shall prove this. Creativity can be rewarded in peaceful ways without resorting to violence.

Public Domain Content

is intangible content made available to the general public without attempts to restrict distribution or redistribution of the material either by force or attempting to restrict who can access the content.

Original Source

The first person to release a unique media as either the creator or under the permission of the creator is an original source. Original sources are important because

they are expected to be credited for work done and expected to be rewarded for their works when those works are appreciated.

Credit Due

Those who create content based on other people's content are expected to ensure it is known at least to some degree what people were involved in which parts of the content.

Honored Distribution

New content distributions are either released to the public at no requested donation, or they are distributed with requests for a voluntary donation especially to the original source(s). Additional favor requests may be attached including review request. They may also be released upon the good faith that any embedded commercial advertisements will be viewed.

Dishonored Distribution and Harmful Content

Content is given without permission of the original source and also has no associated request for donations and is otherwise unrewarded to original sources. Such content may be found to have advertising removed as well. Generally this is considered a dishonored copy. These sorts of behavior are considered antisocial behavior in general. Harmful content itself, such as evidence of a crime, might be distributed for monitoring or investigation purposes only, without any rewards or awards, though added criminal analysis of such content could still be awarded or rewarded. If such analysis content is made available, particularly sensitive content parts might be noticeably blurred or otherwise censored.

Dishonored Software and Adblockers

Software designed to avoid requests for donations or cooperation for rewarding creators is dishonorable. Particularly obtrusive or irrelevant advertising (bankrupt company for example) can be in some way edited or made unobtrusive, but if it is cut out entirely for personal preference and redistribution, it is considered a dishonored copy. Adblocker software is considered dishonorable software when the removal of ads does not accompany adequate financial compensation to content creators. Adblocker versions that well support full compensation of content creators, such as by verifying minimum ongoing donation amounts, are honorable, though that should already be done normally by the Zeronet (ZNET) donation, public content network (PCN) cogs, and metastream cogs.

Value Distribution Review

Content often builds on other existing content. Furthermore, multiple people are often involved in creating content. Reviews of the content should estimate how much value is derived from each different creator, so as to ensure those creators may be compensated for their authorship either by just having credit for the work or more than that. All content stakeholders should

be incentivized to participate in content reviews by content creators and content distributors using any system of their choice that offers value or perks, especially to those who agree to a review before interacting with the content.

Alternate Collaborative Content

After a content title exists, another identically titled content may be submitted, and such content is considered Alternate Collaborative Content in addition to being Competing Perspective Consideration (ref Netportal:Competing Perspective Consideration). For any collaborative content existing as a titled content node on the Information Graph (Iggy), there is expected to be author information, and these authors may submit alternate content. These discords are resolved individually (and relatively) by determining which authors are most trusted by any given Zeronet (ZNET) participant, and will display to that participant according to the viewer's trust ranking on the Web of Trust.

Cooperative Development: Open Collaboration Incentives:

Public Content Rewards

These are open reward offers for developing wanted content which is expected to be distributed to the public domain. A person posts funds to escrow, bond organization, trust fund, or a Public Collective Content Reward Escrow Organization. The person either directly or by the reward organization requests development of Public Collaboration Content to a certain specification. When this is accomplished, the accomplishing author of the Public Collaboration Content receives the reward. This reward is designed as an addition to, not replacement of, additional future compensation for the content development.

Continuing Development Award

Each award for content, either part of an award such as 50%, though as much as all, as donors choose, go to a escrow, bond organization, trust fund, or Continuing Development Escrow Fund, designed for their preferred content creators to develop further content either directly them self or by establishing Public Collective Content Rewards. Money spent is to be approved by the fund, with the only consideration being whether the money is being used on content development or not. So unlike a regular donation, this donation is conditional upon the release of further content. No further development effort is required by the author as they may hire another party to do the work such as by using an Public Collaboration Content Reward, and there are expected to be no restrictions on what or how work must be done except for the domain of development. Anonymous authors may establish a Privacy Trust to receive such awards and remain anonymous.

Continuing Development Escrow Fund Organization

is an escrow organization focused on open content rewards. These organizations may receive escrowed funds to be released upon certain Public Collective Content development. Escrow organizations will apply a predetermined fee to funds for management. Zeronet (ZNET) participants are expected to select funds that make good decisions about what awards were given appropriately, as well as their fee for doing so. Also encouraged is maintaining diversity in escrow options, such that if a given Continuing Development escrow organization is taking up more than 1/3rd of the market, another option should be used as to encourage option diversity. This organization can be run by participants who enjoy a specific type of content covered by the preferred content topics of the escrow organization. So, someone who enjoys documentary movies can involve them self in an escrow fund who helps reward documentaries as agreed by escrow contracts.

Collaborative Development: Open Collaboration Protocol:
Summary
Open Collaboration Protocol enables joint editing of content by more than one author.
Collaborative Content Node
Collaborative Content Node is data designated to be jointly edited. Any Titled Content that is assigned an identifier on the Information Graph (Iggy), has a metadata file, and is accessible to the public by Zeronet (ZNET) may be considered a content.
Collaborative‘ Content Title
The Information Graph (Iggy) may be used to create nodes that are associated with Collaborative Content. Each such content is expected to be assigned a title. Collaborative Content Node is identified by title text and the hash of that title text, and are then expected to be associated with one or more Information Graph (Iggy) nodes that appropriately summarize the content as a category.
Content Hierarchy
Collaborative content is assembled from a specific foundational Content Root Node (ref Content Root Node description nearby) of the Information Graph (Iggy). Nodes (subnodes) associated with that Content Root Node, down to a certain level of detail, are compiled and displayed based on their level of trust.
Content Branch
is a Collaborate Content Node that contains an ordered list of other collaborative content branches or nodes for display. These nodes act as instructions to assemble other nodes into a group so as to form a content hierarchy or layout.
Content Trunk
The referenced Content Branch marked as the beginning of a group of content branches for a given display perspective.

Web of Trust Display

Web of Trust information is used to determine what collaborative content will be displayed as the most trusted content for any given Collaborative Content Title. Furthermore, content will also display according to the principle of Competing Perspective Consideration (ref Netportal:Competing Perspective Consideration). Because anyone can edit collaborative content, only people ranked well enough on the Web of Trust will have an impact on a participant's perspective of the collaborative content.

Author Trust Equivalence and Publication

The trust level of submitted content begins at the same trust level of the author. So, content submitters are expected to be the authors of their own content. In submitting content, an implication is made that it is of a certain quality. This level can also be stated by the submitter. For these reasons, content authored by another person without any modification is not for this network but rather the Public Content Network (PCN).

Content Signature

Content submitted to the network is expected to be cryptosigned by the submitter as evidence of authorship.

Content Data Structure:

Collaborate Content Node

Content is encapsulated in Titled Contents (ref Democratic Communication:Plain Text Protocol (PTEX):Titled Content). Content cells may be divided to multiple cells by content creators.

Collaboration Garden

Within the Information Graph (Iggy) is the Collaboration Garden. The Collaboration Garden is Information Graph (Iggy) nodes that are associated with content cells of the shared content of the Open Collaboration Protocol. Each content cell is titled (ref "content title" sections such as in Public Content Network:Content Development) and the authors are noted (ref Shared Credit at the Cooperative Development:Open Collaboration Incentives:Shared Credit section for more information).

Content Root Node

is any content node which is used to create other content, but itself may not have displayable content but rather just links to displayable content. This is a summary, see the other entry in this section for details.

Content Patch

If an author wants to edit part of a content node without claiming to trust the full content of the node, the author should create a Patch Node which contains only the edited portion of the content. A patch node contains information that corresponds which parts of the original node are unedited by the author. For example, a person may read a news story and want to correct a single fact while leaving much of the story unread. So, the person creates a Patch Node linking to the original node that defines unedited content parts by reference

while also containing the edited content. Patch nodes may also edit other patch nodes. Patch nodes do not change primary authorship information regarding Collaborative Content or the trust level of the full content. Information about secondary content creators is appended to a new content metafile describing all patch node credit. Commentary of such edits is expected so that an editing timeline can be dynamically added to the end of the story with information in the content metafile.

Content Branch

Content branches are designed to add information to a specific data content node, where the new information is titled as its own node. This is a summary, see the other matching entry in this section for details.

Content Merge Node Group

A list of Titled Content content that is designed to merge branched content into one titled node.

Content Edit Lock

A content editor has indicated a cell is being edited by that editor. By default the node and all subnodes are then considered locked, which indicates to other editors that it may be a bad idea to try to edit the node at the same time.

Collaborative Development: end

Information System Conflict Resolution Responsibility

Conflicts generally cost resources to resolve. Depending on the philosophy of the participants, these costs are the responsibility of different people. Current governments prefer to force Information Service Providers to pay for the costs of censorship. Under that system, a judge generally commands an information service to remove or halt a specific information system under threat of imprisonment for noncompliance. However, Zeronet (ZNET) only supports voluntary methods of censorship. If a network supports even one case of mandatory censorship, it isn’t Zeronet (ZNET) and could call itself "Oneweb" for example representing their 1% "gunpoint" censorship level. The burden of cost of Zeronet (ZNET) information conflict resolution is set by the service provider. The service provider itself may volunteer to pay all conflict resolution costs, which naturally results in the costs being paid for by all service users in proportion to the resources they pay to the service provider. Those requesting changes to the information service may be required to pay the cost of those changes. For example, if someone posts an off-topic comment on a message forum where participants agree to only post on topic, then the people who want the comment removed for being off-topic pay for the removal costs such as the cost of a moderator to review the comment. Another option is for the person who violated the contract to pay for the removal of the message. This would be an easily enforceable provision

with all participants required to post a civility bond where participants agree that if they post an off-topic comment, they must pay for removal of that comment. The person to pay may be based on the outcome of the decision. If a an information system is contested and found to be compliant with the contract, the person requesting review pays for the contest, whereas if the information system is noncompliant, the violator pays for the decision. Because such decision systems are challenging to implement or for other reasons, all these participants may pay a percentage of costs including a percentage of costs based on the outcome. And, all of such costs might be bonded such as using a Civility Bond Service to help ensure that conflict resolution cost burdens are paid as due.

Wrong Information Resolution

Information systems conflicts especially regarding abuses are expected to be outsourced to an Information Systems Conflict Resolution Service. This may reduce corruption incentives such as the incentive to overcharge a complaining participant to remove content they found in violation of a contract. Service providers are expected to create contracts determining what information and processing is supported and unsupported. Service providers are expected to authorize dispute resolution participants such as mediators and arbitrators to modify or halt unsupported information systems to ensure compliance with participation agreements.

Conflict Resolution Cogs

See Service Cog:Democratic Communication Cogs.

Protocol Resolution:

Namespace

is a domain matching words to meanings. So, a dictionary may establish a namespace. An encyclopedia may establish a namespace. Any table of values matching one semantic value to another may be considered as a Sigil Namespace.

Title Sourcing

is the process of establishing sources for providing titles to entities that match a namespace definition. Identity sourcing could be considered the same thing or a specific type of title sourcing, matching an entity with a name that identifies it. Examples of title sourcing include phone books, birth certificate repositories, and domain name registries.

Protocols and Namespaces

A protocol is a set of rules that are established within a namespace. A namespace can be a dictionary while a protocol can be a grammar or syntax. So a specific grammar would be a "grammarspace". A protocol has a context of authority while a namespace has a context of semantics.

Sigil is an expression implying cooperation as shared meaning on namespace, title source, and protocol. Unlike an

authority, a sigil does not imply a potential for conflict. A sigil implies the representation of one or more other symbols such as the use of a flag to represent a culture with multiple specific values.

SigilX Protocol

SigilX is a sigil protocol as a service providing automated translation, text replacement, information insertion, and text deletion according to any protocol as support becomes available. The translation system with a varying degree of automation can control both language and the emotional impact of words. Using this system without understanding may be dangerous because many security breaches can occur when translated symbols are reinterpreted, misdirecting, or otherwise misleading. So, SigilX settings should be checked by participants regularly such as once a week to ensure proper security.

Use Cases:

1. Translation of a less known language or grammar to a better known language or grammar.
2. Translation of a lesser known system of metrics to a more known system of metrics.
3. Fixing grammar and spelling errors.
4. Translation of an unpreferred perspective to a preferred perspective.
5. Replacement ciphers for discreet communications.
6. Information augmentation: Such as automatically "hyperlinked" text and information popups.
7. Tagging: Retrieval of comments, reviews, and ratings related to specific content.
8. Replacement of offensive language with less offensive language.
9. Deletion: Removal of repetitive or unwanted expressions from a set of other expressions. Deletion can also be used for censorship and so is discouraged.

Automation Cautions

Enabling of translation is not expected to be fully automated by fixed algorithm with perfect translation. Participants should easily be able to see the original versions of any item. Otherwise, participants could falsely attribute displayed information to a person that was actually provided by someone else. The display should make any alternations noted.

Code Words

Words on the Information Graph (Iggy) may defined by hashes redefined by a secret code set by an organization of the participant’s choice. These code words are encouraged to be set on as as much as an individual basis for the purpose of private commercial exchange. This may be used in addition to Nautilus (NASH) encryption (ref Secrets Protocol:Organizational Security:Nautilus Shell Distributed Service Protocol). Interest groups or other organizations are expected to assign a code set for such purposes. Allied participants are expected to know the meanings of such words based on

the context, while opponents are expected to be confused or mislead by such code words.

Translation

Translation is encouraged to be done on the participant's computer, but some advanced translation may be better done remotely.

Automatic Word Replacement and Spelling Correction

Basic versions of this are lists of source words with target words. Any instance of a source word is replaced by a target word in the order it is listed. This may be managed either client-side or server-side by a service cog.

Encryption Service

The SigilX Service Cog running on the participants local computer should replace cypher text with plain text given the key sets. See Service Cog:Democratic Communication Cogs:Security Cogs:Encryption Cog.

Tagging Service

All published content is expected to be commented on, rated, and reviewed. This information attaches to any other information on Zeronet (ZNET) or other networks as referenced. Participants form consensus on protocols for comment systems, rating systems, and review systems. These tagging protocols expand based on consensus. A tagging service generally uses a public post (ref Public Messaging:Public Post) to reference content on the Information Graph (Iggy). This post is linked to the content by being posted to a Public Information Database (ref Information Graph Cogs:Database and Search Cogs:Public Information Database Cog) and then linked to with Database Discovery and Synchronization Service (Disco) (ref Web of Trust:Network Synchronization:Data Discovery and Synchronization Service).

Protocol Short ID

A protocol reference that uses first 'N' number of letters of Protocol Declaration (PD) hash rather than full hash, where N is the lesser number of characters used instead of all characters. The number of characters expected to be used is the minimum number based on whether or not another identical hash would already be in use.

Zeronet Protocol (Zerp):

Information Decentralization

If you choose to share personal information with an organization, we encourage also sharing the information to an "antitrust" organization like a Data Negotiation Service (ref Web of Trust:Data Negotiation Service) so the information isn't monopolized. Participants provide valuable data to trading partners in various ways including web searches and shopping. This data currently is provided more to large organizations that have a market advantage by having large volumes of such data, and are disincentivized from sharing it with others while being incentivized to monopolize the data. This

amounts to an unfair advantage for large organizations which is a reason such organizations currently have centralized monopolies. To counter this, any time data is given to a large organization, that same data is to be provided to a data provider whose job it is to also make the data available to organizations of any size such that the cost to them is generally based on the file storage and bandwidth costs. That data is expected to be provided using the Open Exchange Data Exchange. See Open Exchange:Standardized Exchanges:Data Exchange section for that system. The data data is useful for economic studies, health studies, and advertising.

Censorship

Participants can expect a higher degree of control over the content types they help provide than current web hosting service. While Zeronet (ZNET) never mandates censorship, individual participants may self-censor their own content as they wish. Data doesn't hurt people, people can hurt people. So, people are encouraged to resolve conflicts at the personal level rather than shooting the messengers or destroying post offices. Reference the Rainbow Rock philosophies for explanations of our reasoning.

Sponsored "Free" Services

The phrase "free" in context of "free service" is discouraged to describe any Zeronet (ZNET) function because all services cost energy to provide and so are not free to the provider. Instead, words including "subsidized", "sponsored" or "included" are used. Some Cogs (ref Service Cog section) are expected to provide sponsored services in exchange for message recipients interacting with advertising content. A few Cogs may provide sponsored service as public charity. The word "free" on Zeronet (ZNET) is discouraged because it is considered more confusing than these alternatives.

Secure Communications

Signed Message is a message ending with a cryptosignature ("digital signature") that only the person holding the "heritage signing key" is able to create for any given message. See the Democratic Communication:Encryption Terms section for definitions of these terms. See the Group Records Exchange reference for encouraged formatting of such messages.

Technical Support

Because Zeronet (ZNET) is a decentralized system, Zeronet (ZNET) technical support people are all independent participants. We encourage organizations to form that offer independent technical support of all types including Zeronet (ZNET) support, especially using the Caroasi:Rainco model. Such support service is generally expected to be pre-paid on an hourly basis. Participants unfamiliar with Zeronet (ZNET) are encouraged to purchase 3 hours of technical support which convert to digital money if not used within one year. We expect cards to be available at retail

locations world-wide where communications service cards are sold. The logo is expected to have "Zeronet" in the same size text area space or font as the name of the independent support provider.

Zeronet Consultation and Development

Zeronet (ZNET) is basically a replacement internet and can be used for any information system purpose. Any information system provider can become specialized in applying their domain of knowledge to Zeronet (ZNET). Because some Zeronet (ZNET) service cannot be automated as a Service Cog (COG), such people with specialized information systems knowledge are valuable. Participants who want to be involved in developing Zeronet (ZNET) are expected to benefit by providing or requesting consolation and development services through the Open Exchange (OX) (ref Open Exchange:Standardized Exchanges:Data Exchange section for details).

Metastream Service

See Public Content Network:Key Features:Metastream.

Metastream Comparison

Metastream service is currently somewhat comparable to Steemit.com, though unlike Steemit the system is a peer-to-peer-capable decentralized system that intends to support all content types and also be much more effective and fully featured. A metastream service is like a much more expansive version of "Youtube" recommendation lists, "Reddit" upvoted listings, and "Twitter" trending listings.

Public and Private Metastream

Public Metastream is content where the recipient is a broad public domain of people. When there a recipient is specific people or a private group, a Private Metastream service is used. A participant client device is expected to merge both public and private streams in various ways according to the participant’s preferences. Metastreams may be loaded differently by the avatar (Ref Democratic Communication:Identity Information:Avatar) in focus on a participant’s Netportal internet browser interface for example. See associated section for a description of the Netportal internet browser.

Cog Service Provider Profile

Service Cogs (COG) and content service providers are expected to post a profile to a contact database such as Service Cog:Information Graph Cogs:Contact Discovery Cog summarizing their services offered to participants. The list should include records of services provided and their associated prices.

Navigation Control

All Zeronet application navigation options which are not considered entirely essential are expected to be removable both indefinitely and permanently. All navigation options are expected to be easily customizable by editing Plain Text Protocol (PTEX) (see associated section) formatted navigation data.

## Zeronet Protocol: Protocol Development:

### Paid Service

Over time, new protocols are wanted including by forking existing protocols. Protocols designed for unpaid routing (like Tor for example) are more viable for lower bandwidth network traffic such as text but less viable for high bandwidth content like video. Most Zeronet (ZNET) connections, and all streaming video and high-speed connections, are expected to be both pay-to-push (upload) for the sender and pay-to-pull (download) for the receiver. The costs involved are expected to be small because services offered are expect to generally match services received. Each participant with available bandwidth and other computing resources is expected to make those resources available to Zeronet (ZNET) users at open-market prices, and also use other participant's resources while paying them for those resources. On average the cost for resource-weak participants is expected to be about USD $2.50 per month for intermittent users while the resource-strong always-on participants may gain USD $2.50 per month for services offered. So, connections will be available for small fractional amounts.

### Token Pack

The 'token pack' system is able to handle transactions of these small amounts. Token packs for Zeronet (ZNET) services (ref: Token Packs) may be available for USD $1 or less.

### Pay It Forward

Participants are expected to "pay it forward" when using public voluntary services such as TOR and BitTorrent. So, Zeronet Resource Control (Zerco) by default is set to match downloads by these protocols for a ratio of slightly more than 1:1 to 1:2. So, for every one bit pulled (downloaded) at no cost, two bits will be uploaded (pushed) at no cost. Because of the increased participation rate of Zeronet (ZNET) which is all but demanded as participation in every way is strongly encouraged, this should be sufficient to cover leeching participants.

### Browsing Experience

Netportal (NTP) is only a browser plugin, but Zeronet (ZNET) services are expected to be always-on, so a Zeronet (ZNET) app is also expected to be available. Netportal will be an application expected to be developed for all operating systems with a substantial user base including Linux, Android, Windows, and MacOS. Furthermore, Plain Text Protocol (PTEX) is presented as a viable alternative to HTML which browsers do not support.

### Protocol Replacement

Display and formatting protocols are proposed to be replaced by more comprehensive languages to better meet Zeronet (ZNET) goals of comprehensibility. However, that goal is expected to take a long time. Meanwhile, Zeronet

(ZNET) is expected to be developed by common protocols including HTML and CSS. As time goes on, these protocols will be replaced by the more comprehensive and more verbose protocols.

Plain Text Protocol (PTEX) to replace HTML and CSS

Plain Text Protocol (PTEX) is designed to replace HTML. PTEX is designed to be as human-readable and comprehensible as can be feasible. PTEX is designed to replace more specific structures like tables with more generalized data structures formed by nodal networks for better comprehensibility. See Democratic Communication:Plain Text Protocol (PTEX) for details.

Plain Text Protocol (PTEX) to replace XML and JSON

Plain Text Protocol (PTEX) is a more human-friendly format than XML and JSON. In most cases records are self-explanatory as to the structural meaning.

Group Records Exchange Protocol (GREX) to replace MyISAM and partially replace HTTP

Group Records Exchange Protocol (GREX) is a plain text record format as a subset of Plain Text Protocol (PTEX). Transfer of sets of records among Service Cogs (COG), software, or (more broadly) organizations is encouraged to be done according to this protocol. See the Group Records Exchange Protocol (GREX) attachment for details.

Secrets Protocol (SPROC) to Supplement TOR and VPN

Traffic shaping and traffic padding are strategies which may be implemented on Zeronet (ZNET) for high security data transfers. See associated Democratic Communication:Secrets Protocol section for details.

Protocol Development States

Plain Text Protocol (PTEX) is currently considered under revision. However, it should be complete enough to develop most Zeronet (ZNET) components. TOR for standard content traffic is also an option, especially by paid higher speed nodes. Plain Text Protocol (PTEX) is expected to develop more formatting syntax to replace HTML and CSS. Group Records Exchange (GREX) (ref attachment) is also usable for basic purposes but is expected to develop more syntax to replace XML.

SemanticWeb Stack

Zeronet developers are encouraged to consider how components may be developed in the modular pattern suggested by SemanticWeb. Many of the protocols involved however are expected to be shifted to more human-readable formats. The Web of Trust is a definite match for the protocol’s Trust module for example.

Compatibility Considerations

Generally, the most common device capabilities (as a median value) will be targeted for protocol standards. If developers believe another setting is both preferable and generally accessible or can be expected to be made accessible, then they are encouraged to first develop in the preferable setting. Developers secondarily then attempt to offer a way to develop for cross-platform compatibility. For example, display resolution is a

development capability to be considered. The most common screen resolution by device is then a consideration. 1920x1080 is among the most common computer desktop display resolution. So, that would be the beginning point for a protocol. Specific applications may target specific devices, and in these cases different protocols will be considered. For example, the most common display resolution for mobile devices is currently 360x640, and so a protocol designed for mobile usage would generally target that resolution instead of the more common 1920x1080 display resolution.

Zeronet Protocol: Topic Search Protocol:

Search Inquiries

Search inquiries are a set of search queries all designed to discover the same targeted information. The inquiry ends when either the targeted content is discovered or the search is abandoned without finding such information. Search inquiry data is wanted to be shared by searching participants to request specific content because it does not exist, and wanted by content creators to notice where there is demand for content that does not yet exist. Queries that return a miss (no search results) are expected to be made available on the Open Exchange (OX) Data Exchange (Datex) system (ref Open Exchange:Standardized Exchanges:Data Exchange). See that related section for details. To help this effort, a search query box is expected to be replaced with a button prompt with a slider saying "bad" on the left, "good" on the right and a slider down the middle that the participant is expected to slide or swipe, generating a -1 to +1 rating for the search. Upon rating the content the search result set will close.

Search Engine Development Plan

Incorporation of existing search technologies can be done more quickly than creating any customized search solutions. However, Zeronet (ZNET) emphasizes comprehensibility of as much as the system as possible. So, attached is a possible type of search solution for Zeronet that may be more comprehensible. See the Topic Search attachment for details. We would like to support a broad range of search service providers. There are at least three public domain open-source peer-to-peer search engines being actively maintained. A number of options can be employed for Zeronet (ZNET) searching capabilities, although a critical mass of peers would be needed for each search service to begin as hundreds of peers might be needed to start such a service that can offer a search of the entire Zeronet (ZNET) content. These peers would have to all agree on the content which would be discoverable, which would also be a challenge. There are also privately maintained but open-source search service options that could be implemented, though corporate governance conflicts with different IP philosophies would be expected to be addressed to

harmonize such relationships.

### Topic Versus Channel

Because all channels are also topics, and all topics are channels, participants decide whether they are searching a given token as a channel or topic by specifying the channel followed by a colon. Metastream providers (ref Public Content Network:Key Features:Metastream) are expected to create channels with a dedicated domain of topic nodes on the Information Graph (Iggy) (ref Zeronet:Information Graph). Furthermore, all content posted to Zeronet (ZNET) is expected to be assigned to one primary topic by those metastream providers. The Search Query Improvement Service is expected to add a prompt when it is suspected a participant intends to search a specific channel only but didn't use a colon (:). That assessment of intention is based on data that is expected to be based on data shared on the Data Exchange (Datex) (ref Open Exchange:Standardized Exchanges:Data Exchange).

### Search Engine Focus

Search focus is on the probability of participant interest in specific content as it is associated with a specific topic, not relevance because that would require a search engine content bias which is discouraged. It is up to people's web of trust cogs (see associated section) and review cogs (see associated content) rather than a search engine to determine accuracy and relevance of content. Competing search service DuckDuckGo has suggested they will censor content they personally disagree with for political reasons. Zeronet cannot do such a thing or it wouldn't be Zeronet at all, so rather participants must take an active role to censor all content except for sexual crime evidence videos which are censored by default but can be uncensored by participant actions.

## Zeronet Protocol: Network Connectivity:

### Peer-to-Peer Communications

The Contact Directory Service Cog: See Service Cog:Contact Directory Service Cog for contact directory plays a key role in matching participants to their IP address for immediate communications.

### Registered Contact Point

A participant's IP may change from time to time. Each participant chooses a Contact Directory Service Cog (Cdisc) (ref Service Cog:Contact Directory Service) to have an up-to-date record on their current location so that users may contact them either directly for a sufficiently trusted peer or indirectly for less trusted peers.

### Bandwidth Usage

Compressed video bitrates are recommended as follows:
240p 400kpbs  extra-low quality
360p 750kbps low
480p 1mbps medium, recommended

720p 2.5mpbs high
1080p 4.5mpbs extra high
Compressed audio bitrates are recommended as follows:
16kbps low quality
32kbps medium
64kbps high, recommended

Protocol Selection

Each Zeronet (ZNET) connection may use a different protocol depending on the content type being transferred. Direct connections may accompany an alert for who is being connected to directly. So, if people are known to have a relationship such as family and friends which are expected to be widely public such as by public family tree records, then the direct connection is considered appropriate. However, connecting to unknown people or business partners, then video and voice streams generally should only be done on higher latency indirect connections. If a need is felt to connect outside of family and perhaps locally met life-long friends for video and voice with low latency, it is encouraged to either anonymize the voice and video, or use that physical connection for voice and video only but no other internet traffic. So, one of the lines could be for a publicly known connection while the other could be for less public and private connections. Default content includes static content like weather reports and news articles, and dynamic content such as shopping websites and mapping websites. Default content is anything but specific types of content which are trafficked differently like video streams.

Security Level by Content Type

Low  Direct Peer-to-Peer
Primary Purpose - Two-way real-time audio/video with close family and friends.
Lowest Latency
Routing Networks - ISP / Internet
Locations / personal information expected shared.
Connection Access: ISP, Authorities with Warrant, Hackers

Medium-Low  One to Two Hops
Primary Purpose - Two-way real-time audio/video with neighbors. Real-time Gaming
Minor latency
For sharing insecure information.
Routing Networks - ISP / Internet and a Rendezvous or Other Server
Connection Access: Authorities with Warrant, High Skill Hackers

Medium-High  Three to Four Hops
Primary Purpose - One-way streaming. Local Business engagement. Generally secure, but delayed, real-time audio/video.
Moderate latency
For local business with moderate security.
Routing Networks - VPS or Neighborhood Cloud,

Rendezvous Server
International Hop to Top 8 Privacy Jurisdiction
Connection Access: Cooperating authorities with warrant for major international crime.

High Six Hops or More
High latency
Routing Networks - TOR, Loglo
Banking, Transactions, Shopping, Public Content Uploads, Loglo Broadcasts, Text & Voice Messaging
High Latency
For secure business.
International hops through top 8 privacy jurisdictions.
International hops through uncooperative jurisdictions.
Connection Access: Unlikely, but theoretically possible by vast fortunes of funding of international hacking efforts, or years of cooperation by competing international interests with multiple search warrants against major international crime activity.

Bandwidth Shaping Goals
Standardized rate selection 360, 480 recommended, 720
Prepadding and postpadded data to help avoid timing analysis
Rendezvous server should be intended for the same traffic type among video, audio, chat,

Neighbor Discovery Query
A cryptocurrency token password set sent to nearest unqueried neighbors, giving the first respondent with that password a small reward for noticing the message correctly. If the recipient participant finds value in exchanging information with the newly discovered sender, the token is redeemed, then another token of equal value is expected to be relayed back to the sender to create a neighbor relationship. Otherwise, the token is kept. If the token is redeemed without any value being relayed back, the location is flagged as uncooperative. If value is relayed back, the location is flagged as cooperative. A set of tokens will be used at any given time to avoid a situation where a token fails redemption because the token was handed out twice in short order without the expectation that two different people locations would claim it. If that happens anyway, a second valid token is expected to be issued for the recipient who claimed the token too lately. So, two attempts might be made at each possible address in case of such an event.

Zeronet Port Selection
PTEX prefers to use port 80, 110, and port 443 because they are expected to be quite common statistically. If port 80 is blocked, other ports are attempted to be used. This may be port 587 as is a common SMTP email receiving port. PTEX may use alternative ports automatically for security reasons according to participant settings. For example, port 80 and port 443 could be used to emulate common internet traffic such

that it isn’t known that Zeronet (ZNET) is being used on the network by hostile entities. A stenographic backchannel can further mask such traffic. Other statistical pattern-matching can also be employed. Port 12345 should be used when no low-numbered ports are available.

Zeronet Neighbor Discovery

TCP Port 25 Connection

Standard Messaging:

Sent: "Hello? Seeking neighbors. Token X"

Received: "Yes! Hello."

Zeronet Peer Connection Steps

Using Plain Text Protocol (PTEX):

1 Purchase Zeronet service connection kit with a one year supply of standard specific service tokens CDisc, Disco, Metastream, GTS, Topcog, PSN, and generic unspecific small service tokens usable for many different cogs or portals.

2 Purchase one month to multiyear supply of content download tokens, medium-low security Rendezvous service tokens, high security Loglo and (high-bandwidth) TOR tokens, and VPN service tokens.

3 Subscribe to monthly content creator donation budget. Subscribe to individualized diagnostic/help service.

4 Load or otherwise set avatar list using the Web of Trust cog.

5 CDISC (Contact Discovery) tables determine initial network contacts.

6 Data Discovery and Synchronization (Disco) tables determine peer contact point.

7 Peer Contact

Establish connection to Rendezvous server or Loglo gateway server.

Exchange contact token(s).

Obtain encryption key(s) including secure line key(s).

8 Data Communication such as GREX records exchange.

Zeronet Protocol: Data Traffic Strategies:

Extension of OSI as OSI 2

Open Systems Interconnect (OSI) is a data traffic protocol set. This set is extended as OSI 1.1 for Zeronet. Instead of layer 7 being the application layer, Layer 7 is instead the "App Interaction" or "API" layer which for Zeronet is Intercog. Layer 8 is then the (discrete) app layer. Layer 9 is the gui (Graphical User Interface) layer which for Zeronet is Netportal.

Multimodal Data Transmission

Traffic is expected to be routed using multiple protocol options determined at a Zeronet (ZNET) OSI application layer. We expect to "slightly" fork existing protocols to specially adopt Zeronet (ZNET) traffic, or otherwise add Zeronet (ZNET) functionality to those protocols. While awaiting these developments, we will directly use existing protocols until replacements are developed. The primary platform adopted is expected to be Tor for HTTP

traffic. However, Tor tends to be too slow for some purposes like real-time voice and video. Also, Tor is not yet fully developed and for example does not yet have traffic shaping available. For these reasons, traffic is routed using multiple methods.

Distributed Service Locations

If a Zeronet (ZNET) location is physically attacked, the damage may be limited to the location of that physical damage as with other internet connectivity strategies. The number of locations depends on the available resources of each service location and the number of people who adapt Zeronet (ZNET). A satisfying level of security is for all Zeronet (ZNET) participants to offer a service location, which makes service availability very high for satisfying reliability. So, it is encouraged for all participants to offer resource sharing of their available computing resources whether donated or sold.

Transparent Reporting and Verification

It is valuable to have accurate traffic and other information on Zeronet (ZNET) such as pull (download) counts of content. Privacy is also valuable which can be a conflicting value preventing the knowledge of such information. Data Negotiation Service (ref Web of Trust:Data Negotiation Service) is a compromise of privacy and information sharing that is hoped to keep participants from being individually identified while still being able to know traffic statistics such as the view count on specific Zeronet (ZNET) content. In order to encourage accuracy, all information from any Zeronet (ZNET) interaction which is made available by at least one person for statistical analysis is also expected to be made available by the other people involved so that it is more difficult to falsify information. For example, a video view is generally reported by a Metastream Provider (ref Public Content Network:Key Features:Metastream) for content creators to know the number of views on their content, so it is expected that the viewing participant also reports the view, preferably through their Data Negotiation Service, so that the information content creators have can be verified by as many people as possible. The Zeronet (ZNET) Web of Trust is expected to enable participants to provide valuable information to the world at large while revealing their identity only when considered appropriate to do so. Usage of auditing and review services including the Contract Performance Review Cog (ref Service Cog:Web of Trust Cogs:Contract Performance Review Cog) and similar services are designed to keep participants in check regarding information accuracy. Cross checks with multiple statistics reporting outlets will be relied on to prevent inaccurate data sources.

Protocol Adoption

While we may develop a Zeronet-specific protocol slowly over time from the software level to the physical layer

of the OSI model, we will begin by routing most internet traffic over existing protocols to become operational as quickly as possible. Initial internet protocols expected to be directly used initially include HTTPS, TCP, TOR, BitTorrent, and VPN. Standard web browsers may be used for Netportal with Zeronet(ZNET) initially being browsed with a plug-in to a browser. HTML, CSS, and ECMA scripting (as Javascript) is expected to be supported. We expect to also evaluate Freenet, eDonkey, and Gnuttela2, and others for network incorporation. After replacement internet protocols are developed, such replacements will be encouraged over these adopted internet protocols. Data compression protocols to be evaluated.

Zeronet Protocol: Computing Distribution:

Computing Domain

A computing domain is a collection of computer resources assigned to a computing process. One computer may be divided into multiple computing domains to be used for specific purposes. This may be done to limit resource used by any one process so that it does not interfere with other processes on the same computer. Also, multiple computers may be assigned to one Computing Domain to increase total resources available for one process. Computing Domains are expected to rely on a Web of Trust for resource distribution and usage.

Computing Subdomain

A Computing Domain domain may divide and subdivide into Computing Subdomains.

Control Node

A control node is control over Computing Domain(s) as they are assigned to an avatar for update access or other modification reasons. Control Nodes may act as a process with an owner that has control over any and all features, benefits, and aspects of an application or process. For example, a certain computer programmer participant may be able to change the location of a navigation button after being assigned control over that button. A control node may be created to allow a certain programmer to locate and relocate the navigation button. Participants who like more control can remove that programmer from their list of trusted people, and instead put them self or someone else in charge of that feature.

Control Node Interface and Design

Control nodes may grant functionality to other nodes. Either specific other control nodes by specific other developers, or all other control nodes. Which control nodes have access to which other control nodes is always customizable by Zeronet (ZNET) participants. This concept is also not unlike the computer programming concept of executables being passed arguments and delegating an executable to a specific participant to be updated. Control nodes are more fully featured concepts

than (.exe) executables as a single node may have multiple executable functions, whereas (.exe) executables are not typically designed for more than one function at the command line level (except on versions of Linux). Zeronet (ZNET) control nodes can be assigned access to any or all Zeronet (ZNET) components, which allows a control node to behave somewhat like an computer programming API giving access to any Zeronet (ZNET) functionality. All Zeronet (ZNET) coding begins by focusing on permissions. The author decides who will be permitted to access and replace their code. But, authors assigned a higher trust rating by a Zeronet (ZNET) participant will have access regardless of these settings.

Control Graph

A control graph defines how system resources are distributed and assigned to people or groups of people. The purpose is to restrict or otherwise assign specific people to use specific resources for specific computer application behaviors, which may be in limited amounts. Participants can then adjust how their applications behave or delegate that to others either generally or in specific. When a person develops computer code, they mark them self as the author. So, their set of instructions is attributed to a specific person. That specific person can then be associated with one or more groups of people. A person's Web of Trust can be used construct a chain of trust automatically by deciding which coders they trust the most.

Service Command Interface (SCIN)

A set of mechanical, electronic, or Graphical User Interface (GUI) controls over the processes of any given information service. This would be generally expected to be in the form of a Zeronet (ZNET) portal (ref Netportal section) as a software application control. With 3D printing technology, one might be able to devise a mechanical system for many different portals.

Control Domain Rank

When multiple people are assigned control over a single control node, the person with the highest Web of Trust ranking shall be the person to control any changes or updates for nodes under the control of that person.

System Updates by Control Graph

The control graph is used as the main factor in participant's Zeronet (ZNET) system updates.

Benchmark Function

This function runs a series of tests to determine available resources for Zeronet (ZNET) and the performance characteristics of each resource.

Control Node Security

Because control nodes can be used for any purpose, testing for security weakness is important on an ongoing basis.

Default Computing Domain Architecture

IO Computing Domain

Access to hardware inputs and outputs.
Processing Computing Domain
Access to operating system processes.
Front-end Interpreter Computing Domain
Access to operating system inputs and outputs for scripting and security. This would have plug-ins as a participant sees a purpose for. A screenscraper could have access to video output for automated processes that read the screen. A security utility could access the internet uploads/outputs to ensure unwanted data leaks are being prevented. A keylogger utility could be used for keyboard shortcuts, or monitoring of system users.
Back-end Interpreter
For extracting data from computing applications and reverse engineering computing applications.
Scripting Domain
For shell scripting, API interfaces, cross-application interfaces, and keyboard/mouse macros.
Additional Domains
Applications may be assigned a computing domain by another control node such as the Web of Trust control node. Expected application control domains include Netportal and Tor (ref those sections).
Zeronet Protocol: end

Security Suggestions:
High Security Streaming Encouragement Civic Duty
Sending high-security streams (VPN, TOR, Loglo, etc) should be encouraged to be common so that if a high-security streams can be identified, they will be less likely to be targeted for special analysis by malicious people. So, all business and organizational activity is highly encouraged to be done using the high-security streaming option. Security is limited by the hardware and participant security practices, so high-security streams are not high-security unless also on high-security hardware with participants who are aware of basic security rules. Participants are encouraged to always match the highest level of security which is reasonable for their purposes rather than considering security to be a secondary consideration.
Security Affirmation
High-security should only be reported as high-security by software after a series of hardware checks and participant "security drill competence checks" are passed. One example of such a test would be to see if a participant would assign high trust to a randomly generated identity. This security affirmation may be automated by some degree by the Social Security Tester Cog (Service Cog:Democratic Communication Cogs: Security Cogs:Social Security Tester Cog). If the participant does assign the high trust, the participant is prompted with advice on using their local network of family and

friends and searching the Zeronet (ZNET) Public Content Network (PCN) for public reviews to help decide whether a particular person is trustworthy. Their security is then reported as medium rather than high, and another test may be performed at a later time for another test. Service Cogs (COG) may be incorporated into Netportal or other systems with more elaborate checks which could include anti-scam testing such as by emulating a malicious email with instructions that if followed to completion, would otherwise have been a scam except for the prompt alerting the participant to handle these messages differently. High security involves a broad range of safe and intelligent behaviors more than reliance on specific people or components.

Encryption Protocols

To be determined.

PGP Protocol to be Replaced

PGP is considered incompatible and will not be used. PGP involves email, which is replaced with text messaging on Zeronet (ZNET). Furthermore, Avatar profiles are expected to follow a record formatting set by the Group Records Exchange (GREX) (ref attachment) rather than PGP profile format.

VPN Anonymity

A VPN service is encouraged to only be honorable when it accepts money that can be transacted with anonymity without any personal contact information whatsoever. A mutually agreed mediation and arbitration service may be able to resolve service complaints for further honor. VPN service is only considered secure when it is paid for by digital money or mail-in cash or cash-equivalent payments.

Additional Privacy Methods:

Download Pools

As described in Secrets Protocol (SPROC) (ref Democratic Communication:Secrets Protocol) download pools are a shared downloading point for multiple people to download the same data. Such download pool points offer an alternative or supplemental concept to rendezvous points such as thoose in "Onion Routing". These download points may be able to adopt existing proxy server protocols and packages without substantial Zeronet (ZNET) proprietary protocol and software development.

Secrets Protocol

See Secrets Protocol section for private communications protocols and recommendations.

Denial of Service Protection

Denial of Service (DoS) Attack is when unwanted messages are sent to an opponent device to jam their device bandwidth to its limit such that it cannot accept most wanted messages. The most cost-effective solution is to change the location address of the device. However, it can also be mitigated by distributing the information system the device offers over multiple location point to increase the total bandwidth and information needed to

conduct the attack beyond the capacity of the opponent. This would only work if the opponent has sufficiently low bandwidth available to attack the system at large.

Privacy Mailing Instructions

For improved privacy, create a company, trust, or other organization for which you can receive mail at your address. Currently, in most legal jurisdictions, no paperwork is demanded for the creation of either a company or trust. Depending on your location, you may also be able to create a fictitious name and tell the post office to accept the mail of that person if necessary. It is recommended that you test that address by sending a letter to that fictitious person to ensure delivery is successful. If the letter worked, follow up by mailing a small box.

Information Security

(Ref Netportal: Security)

Secrets Protocol (SPROC):

Secrecy

What do you have to hide? If you don't have something to hide, you are likely risking nothing, and so having a low impact on the world. For people without any desire to change their communities or the world, or who see no purpose in life, secrets may not help them. But, for every goal there is an opportunity for an exactly opposite goal to work against you. The greater your victories are, the greater your opponents may become to be able to challenge you. The more or stronger opponents, the better you need to keep secrets. Secrets can be created and used to protect your property and protect your self. Openly informing opponents of certain weaknesses will lead to exploitation by and temptation of your opponents, so upon discovery of such information you should consider whether the information shall be a secret. Christians will note that even Jesus did have secrets. Some people have nothing to say, and yet want freedom to speak. Some people have nothing to do, and yet want the freedom to act.

Personal Secretive Information

Data is fully owned one and only one way, by never sharing it with any other participants. Any data shared at any point with any other participant outside of a specific confidentiality agreement with people with a high level of trust and a high ability to keep secrets, it is better assumed to be likely publicized and therefore unowned. If data is transferred unintentionally, other participants should be asked or otherwise expected to delete the private data. Upon claiming deletion by all the additional receiving participants, the data is then considered owned again unless or until there is reason to believe otherwise.

Protected Personal Information (PPI)

Protected information includes health information, finance information, relationship information, and

contact information including location. Only one specific highly trusted participant should be trusted with such information. When a participant wishes to share such information, they are expected to relay the information through a trusted Data Locker Service (ref Web of Trust:Data Negotiation Service).

Trust Development

Selecting participants that are trustworthy to network with is important to be able to manage secrets. See Web of Trust:Perspective Development:Trust Garden for safe networking ideas.

Digital Secrets Management

Your Zeronet (ZNET) identity is a transferable digital asset that you are encouraged to never transfer, even after death. So, we encourage you to keep passwords to your digital identity exclusively in your brain by learning memorization well. When you believe you will soon lose competence that will not return to be able to make major decisions, then having a trusted guardian memorize your passwords for you is encouraged.

Expansive Connectivity

All Zeronet (ZNET) participants are encouraged to have their connectable devices running as much as possible. Always-on devices offers location privacy when combined with Masking Service Provider (ref Service Cog:Masking Service) and pull (download) pooling.

Recommended Computer Encryption

For better security, all of your media files and digital assets are expected to be encrypted on your computer. Some information systems on your computing devices may be kept open while others are better to be secured against other people using without a password, depending on whether those applications can access your private information such as personal location information.

Secrets Protocol: Local-Global Wheel (Loglo):

Summary

Local-Global Wheel (Loglo) is a way to send messages anonymously using a concentric network rings connected like target practice rings. All network messages are sent to a hidden central server and then redistributed from that point. This greatly increases the number of possible sources for a given message to anyone in the network. In this client-server relationship, clients may pay the server to relay messages. The central hub server uses many intermediary relay servers (all in multiple network ring configuration) with encrypted connections so its location cannot be easily determined, so the network is difficult for a hostile person to attack. One goal for this is to allow public-audience messages, especially Public Settlement Network (PSN) messages, to be broadcast in such a way where determining the location of the message sender is too difficult for malicious snooping. This generally centralized system can also be used to relay private messages (ref

Democratic Communication:General Concepts:Private Messaging) to any other participant in the pool, with the broadcast service provider being trusted with information regarding who is being contacted, though the message itself may be encrypted if it is a private message. This is the only specifically centralized Zeronet (ZNET) system, and minimizes the number of participants who need to be trusted for the system to function to as few as one single participant. This compares with Tor which having the weakness of having at least some trust in at least two participants (entry and exit nodes). Multiple masking services (VPN, proxy, etc) can still be used in conjunction to such services in ways that would generally require all services to fail for privacy to be breached.

Message Distribution

A central hub node relays client data to the receiver "inbox" destination point of the sender’s choice such as a public broadcast database or message recipient for private messages. For broadcasting, messages are relayed to a broadcaster who is expected to then rebroadcast over their distribution networks. They may also be taken without rebroadcast as a private message by a specific client. After the recipient acknowledges delivery, the message is deleted. Without delivery acknowledgment, the message is deleted within an amount of time negotiated by the recipient and service provider. The hub node is the primary messaging service provider that decrypts messages sent to the service. The outer edge ring is responsible for relaying all push messages to the client recipient, and is also responsible for accepting messages into the system. The nodes on that outermost ring are considered "edge nodes". These nodes are possible destination points as inbox locations.

Network Topology

As the name of Local-Global Wheel (Loglo) suggests, the "hub-and-spoke" network topology may be mapped as concentric rings forming a "wheel". The client nodes can be considered a surface layer ring outside the system. In that system, the client connection ring is the outermost ring of the messaging system containing "edge" servers. Each clients connects to one of these edge servers as a message sender, message receiver, or both sender and receiver. The edge servers connect to spoke servers that lead to the central hub. Spoke servers connect more outer rings to more inner rings, and connect the inner-most ring to the hub server. The hub server(s) are expected to design and direct the full network topology, and route all client messages to any edge server believed to be ready to deliver a message to its destination through each ring. If the edge server doesn’t report the message received and ready for delivery to the client, the message is attempted to be resent to alternative servers up to a specific number of tries before failing. The lateral ring connection paths

are a function for redundancy rather than a common data path, so most data is expected to be transferred by the "spoke line" path links. When a spoke node loses a connection to an inner ring node, it relays the message further through the ring in hopes another ring node will have a connection to the next ring or hub. Client nodes are not given the location of the inner ring nodes because publication of inner ring locations could lead to DoS attacks. The central node has full management control over all server node connections, so directs each server link. Each inner ring layer has a multiple of bandwidth from the more outer layer. The central hub could have for example a 100Gbps symmetric bandwidth, followed by the next ring with 10Gbps per node, followed by the next ring with 1Gbps, and so on until the final (edge) layer expected to be perhaps 1Mbps. No path shortcuts are used for message delivery among client connection edge servers so that network nodes are more difficult to discover by unwelcome network intruders in addition to being a more comprehensible routing method. Topology is also arranged so that the central hub has an ability to outsource all other nodes to third parties because only the central hub server (or server cluster) is expected to have the decryption key to read the desired message and it’s destination. Untrustworthy partner servers have minimal options to unmask any participant’s identity even with majority network control although they could help initiate DoS attacks by learning the ring or hub server addresses. Having the decryption key in multiple locations would be a security risk. If spoke nodes are outsourced to others, they will may be unable to determine which server is the hub node. Only the hub node can know which node is the hub node unless a network spy is able to analyze the network traffic to a sufficient number of inner nodes. The central hub may actually be made of multiple nodes in close physical proximity for redundancy and load distribution reasons.

Setup Servers

A setup server determines the lowest latency paths from the edge server to client. The client will then have three edge servers to choose from. This way, edge server locations are not entirely public. Clients are asked not to publish edge server locations (physical location and IP address).

Network Data Flows

Clients are given a list of available outer edge ring nodes to which they can establish a connection to the Local-Global (Loglo) network. Client nodes establish a connection to one such node with a low latency time. Clients generally send a message at least every 5 seconds, though it may be more often one per second depending on their bandwidth dedicated to the Local-Global Wheel (Loglo) service, or on a different pattern entirely if the client is in a heavily censored

place where they must use traffic shaping without strong connection levels. Clients are expected to use a message relay service to send and receive messages while their local machine is offline. When no message is ready to be sent at the scheduled interval, a generic message will be sent as padding with instruction to the hub server to be deleted. The message will be encrypted according to the provided instructions for the hub server to decrypt. A Zeronet (ZNET) destination for the message is expected to be in the message. The message is relayed to any edge server. Each edge server connects to one server in the inner ring server and one "next node" on the ring in case the connection to the inner ring fails. If the next node also fails no further connection is attempted and the message fails. So, all nodes send a predetermined amount of traffic regardless of whether messages are being sent. Inner ring nodes collate all messages from outer ring nodes and relay them to rings closer to the hub until the message reaches the hub. The same token used to send the message can be used to cancel the publication if such a request is made using the same token, though another token will generally be needed for cancellation request to be read by the server. The hub decrypts each message to know the destination, and data path reverses to move from the center to the to outer ring. The hub determines the preferred path to be taken though the hub-and-spoke system to reach the message destination point inbox. This path is added to the message. The message is then sent by the hub according to the predicted best path. Each spoke and edge server has an encryption key. Only the next hop on the path is decodable by their respective encryption key. If there are less than five hops from the edge to the hub, random data will be in place of hop information. This allows ring servers to be outsourced while revealing only one hop.

Message Sizing and Delay

Message size is expected to average perhaps 800 bytes and so connections to edge servers are expected to be a perhaps 1kbps Padded Stream (ref that nearby section for details) as a result. Because having a large message size could limit who it was that sent the data to high-bandwidth participants only in some cases (such as where the data reveals the time at which the message was sent), any connection using more bandwidth than the minimum should be used with caution by participants with information on proper usage provided to participants. This is resolvable by specifying a delay for longer messages of for example one second per 100kbs so that any connection with 100kbs or more could have been the source for the message by that factor. Extended delay messages are expected stored at the hub for up to a maximum amount of time such as 72 hours. After reaching the hub, messages enter a random delay time from 16 to 32 seconds or longer if the message specifies an

extended delay time. The delay ensures that the message could have been sent by any node even if that node has a higher than average latency. So, any streaming data will have a substantial delay and so wouldn't be expected to be usable for voice conversations.

Inbox Message Receipt Registry

Client destination points for messages to be received to their "inbox" are expected to be registered at their preferred edge node, selected from the set available to them. If no preferred node is stated, then a group of edge nodes will be selected based on network latencies. If the preferred node is at capacity another node will be assigned. If a destination point is not registered to receive message, the message will not be sent. So, clients request with their database services to register to receive messages from the service if that service is not yet registered. This registry is to prevent the messaging service from sending unwanted messages. High participation is encouraged to further enhance the privacy of the service because it may be discovered who is participating in the network, which limits potential destinations for any given message to those accessing the edge servers. Any client may receive private messages through the system by registering as a destination point, but clients may still send messages without doing so. Bandwidth to receive messages to an inbox is unrelated to any sending stream limits. Receiving limits will be much higher than sending limits because all messages sent are limited by the bandwidth of the hub node, while receiving messages are limited to the bandwidth of the edge ring node as shared with the other clients connected to that node.

Message Receipt Identity and Privacy

Each client sends their encryption sharing key using their external public IP address to the service provider, relevant most of all to the center hub. A hash of their sharing encryption key is used to identify potential recipients and establish a unique identifier for their message destination "inbox". The sender is not identified unless they wish to publicly name them self as a potential recipient with a name (that does not have to be unique), that may be kept on public record with any or all edge ring nodes. The data set with with encryption key hashes any any matching names is available to be looked up by any client. Server client connection ring servers keep a list matching encryption keys with clients as inbox receipt destination nodes for their local delivery zone. It is up to clients to use their Web of Trust to determine which name best matches with which encryption key.

Service Distribution

Message recipient clients are provided token packs where each token is used for 5 minutes of connectivity at a specific bandwidth to any of the outer edge ring servers, a dedicated symmetric

encryption key correlated with each token, and a reference to the edge server contact directory which is generally expected to be public information. Tokens expire in an amount of time such as 30 days. No other data is expected to be needed for the connection. When less than 40 seconds of service is remaining another token is expected to be activated. Tokens will be for a specific bandwidth depending on the bandwidth being broadcasted. Tokens are expected to be purchasable on the Open Exchange:Information Technology Resource Exchange (ITREX) using a digital money. The Local-Global Wheel (Loglo) is expected to avoid storing any records reflecting which buyers purchased which tokens at the soonest opportunity after the sale.

Service Token Validation

Messages from any address are expected to be relayed to the hub at least one time without token validation. However, if the token provided to the hub is invalid, that address will be blacklisted at the edge server used for a number of minutes that increases according to the Fibonacci sequence beginning with 30 seconds which allows for innocent mistakes to be corrected.

Carriage Service

Each network "wheel" is one of many options to chose from for message sending. With Local-Global Wheel (Loglo) it is encouraged for all clients to form connections to multiple organizations which together form one third to two thirds of the market share meeting their trust requirements for Local-Global Wheel (Loglo) or sufficiently similar service. The more important the message is, the more wheels are expected to be used. So low importance messages might be sent on "local wheels" whereas high importance messages might be sent on "global wheels". This global wheel network option provides the needed strength in numbers since a given message could then be from anyone in the selected one third to two thirds of participants who use those Loglo service providers. This is also a cost consideration. Someone with a value orientation may select one third market share minimum, but someone with a quality orientation may select two thirds of the wheel options, and a balanced approach would may be to select half the available "wheels". Because a limited bandwidth is dedicated to such messaging, and because each service provider would need to be evaluated before first used, this service is likely to be in a natural state of monopoly or oligarchy but participants can none the less use multiple services to encourage some competition. To avoid trusting all wheels to keep contact information private, only one wheel is selected as the primary wheel, which relays the message to the other wheels. The protocol for this is as-of-yet undeveloped. All wheels are expected to cooperate with all other wheels to an

expansive and satisfying degree. Uncooperative wheels are discouraged to be used.
Secrets Protocol: end

Plain Text Protocol (PTEX):

Titled Content Examples:

Cell 1
Cell 1 Content
Cell 2
Cell 2 Content
CELL 3 Cell 3 Content
CELL 4 Cell 4 Content
Letter-Identified Cells
Cell A
Cell A Content
Cell B
Cell B Content
Cell X
Cell X Content

Tiered Cells Explanation
In the enumerated example cells notice that "Cell A" and Cell B" are on the same tier, but "Cell X" is on another tier as a subtier. "Cell X" is content of "Cell B" and therefore a subtier of "Cell B". The subtitle "Cell B" applies to all three of those (sub) cells. Cell content can be empty if none is provided. The empty line after those example cells ends the set defined by the title. In that specific example the "Titled Content Examples" title, which ended, is still accurate to describe these following lines, but only by accident, as a new cell set was titled "Tiered Cells Explanation". Also, in the example, both the numbered cells and lettered cells share the same tier, but not the same subtier. The numbered cells actually have no subtier while the lettered cells do have a subtier.

Another Titled Content Three-Tier Hierarchy Example:
Fruit
Apples
Red
Oranges
Orange
Bananas
Yellow

Subtitled with Full Titled Content Set Example:
Color:
Color is an electromagnetic spectrum measurement in the visible range of lightwaves.
Color: Fruit:
Information of Fruits by Color (second tier)

Color: Fruit: Apples:
  Red (third tier)
Color: Fruit: Oranges:
  Orange
Color: Fruit: Bananas:
  Yellow
Color: end
Note  Only One empty line is now needed to end this "Set example" section because "color" was explicitly ended by "Color:end". Otherwise, two empty lines would be needed to first end the color subsection, then end the "Set example" main section.
Note  Use of both a trailing colon for nested tiered items is redundant because the leading triple space is also used. So, the triple space could be considered decorative. Alternatively, the trailing colons except the colon in "Color:" could be omitted. If the colon in "color:" was omitted then leading space would need to be added to the four content lines to keep the same hierarchy meaning.

Like previous example but with nesting and more tiers:
Color
  Color is an electromagnetic spectrum measurement in the visible range of lightwaves.
Information of Fruits by Color.
Fruit(tier 1):
Apples (tier 2)
  Red (tier 3)
Oranges (tier 2)
  Orange (tier 3)
Bananas (tier 2)
  Yellow (tier 3)
  by Ripeness (tier 3)
    Ripe (tier 4)
      Yellow (tier 5)
    Unripe (tier 4)
      Green (tier 5)
    Spoiled
      Black
Note that the tier numbers are relative to the color title, not absolute to this whole document since the color information is itself already in a tier level of more than 1.

Example of empty space delimiting:
Fruits:
Apple
Banana

Vegetables:
Carrots
Onions
Note  Two empty lines needed to end this section because this "Example of Tier Title Alternative" creates a first tier. The empty line is needed to end the "Fruits" tier,

otherwise "Vegetables" would be considered a type of "fruit".

Example of title-content pair series with empty content:
Fruit::
Apple:Red
Banana:Yellow
Onion:
Carrot:Orange
Note  Onion has nothing (null) as content. If fruit had ended with a single colon ":" then Red and Banana would be considered a type of apple and other nonsense.
;

Following here is an example of incorrect title tiers where "vegetables" have been listed is a type of fruit. So, lists must come to a definite or discrete end rather than an implied end with a "replacement title". Furthermore, the leading spaces after "vegetables:" will be ignored because tiers shouldn’t be created with both colons and leading space.
Food:Fruits:
Apple
Banana
Vegetables:
  Carrots
  Onions
Food:Nuts:
Walnuts
Hazelnuts

Plain Text Protocol (PTEX): (continued)

Human Language Compatible
  Plain Text Protocol (PTEX) is expected to mix well with human language. So, Plain Text Protocol (PTEX) is an extension of common scripting convention. This protocol is a format as semantic structure for titling, labeling, and referencing text. The protocol rules are more complex than competing formats, so the simplicity is in the ease of comprehension rather than the syntax rules. The protocol allows for hierarchical multi-tiered content and title-content pairings.
Title Methods
  The three content title methods include 1) Leading spaces that reflect traditional paragraph and listing conventions 2) Lines or line segments with one or more colons (:) reflective of traditional titled content and 3) Empty line spacing reflecting of traditional title and verse spacing.
Competing Protocols
  XML, JSON, CSV
  Competing protocols allow long lines of compact data, while Plain Text Protocol (PTEX) generally requires

multiple lines for readability.

Group Records Exchange Protocol

Group Records Exchange (GREX) is a subset of Plain Text Protocol (PTEX), using more specific structure, so that data tables and related data structures will have an identical format when shared across organizations. Plain Text Protocol (PTEX) is a way authors can write text for easy referencing such as in a book or article, while tables within such a text would be encouraged to be written using more specific syntax under Group Records Exchange (GREX).

Delimiters

A delimiter is using a character to define information structure rather than data content. The Plain Text Protocol (PTEX) uses the colon (:), double colon (::), semicolon (;), newline character (
), the triple space (   ), period (.), colon equal (:=), "quotes" , (parenthesis), and the Downslash "Backslash" (\) as delimiters. "end" and "(continued)" are also delimiters in some contexts.

Whitespace

Includes non-visible characters which are used to create distance between visible characters. The space ( ) and newline (
) is used for Plain Text Protocol (PTEX).

Escape Sequence Summary

Escape sequences using (parenthesis) and quotes ("") allow any delimiter character to be temporarily repurposed as detailed in that nearby section. The downslash "backslash" (\) is also use in the common "escape sequence" such that any character preceeded by "\" is to be printed literally without syntactic analysis.

Titled Content

Titled consists of two basic parts: the title and the content. Content having the same number of leading spaces as the previous line is an additional content segment rather than another title. Commas in a title jointly establish multiple titles for the same shared content.

Cells

The content of titled content may be referred to as a "content cell", "content", or "cell".

Titled Content Example, Title-Content Pair

This text is an example of titled content. Titled content is similar to a paragraph in writing. This content consists of the content title "Titled Content Example" followed by a newline and a triple space as three space characters, then the content, then finally ends upon a newline character. For text data display the triple space forming the content cell may form an indentation margin that is expected to continue to the end of the content as a paragraph when displayed in a cell editor as a block of whitespace, or otherwise display the content gracefully according to the Zeronet

(ZNET) participant preferences. See the next Titled Content for an example of proper formatting.

Titled Content List/Series:

Content like the above line ending with a colons (":") followed by a newline character indicate a titled content as a content list, which allows multiple content cells sharing the same title. This list is ended by "end" but could also end with an empty line. (See also: titled content pair series.)

end

Hierarchical Tiers

Cells can be subdivided further into subcells with hierarchal tiers. Titles can be assigned a subtitle (My Title:My Subtitle:) and the content is then considered on a subtier. On the other hand "My Title: My Subtitle" without the terminating colon wouldn't by itself establish any subtier but instead establishes content for the title, so the second ending colon is needed to do that. In that way, titled content can be grouped by subtitle, using the colon (:) which acts to mark a list as a tier without the need for leading spaces in subsequent lines, or without using multiple sets of triple space, one for each level of tier. A complex hierarchy may be form with multiple such cells as the examples below demonstrate, because every title and subtitle can have content and have further subtitles. The sequence: "Favorite book: Romeo and Juliet: To Be or Not to Be?" establishes a 3-tier book title reference.

Provisional vs. Sticky Tiers

Tiers established by leading space offer provisional tiers that must continue on each line to maintain the tier, one triple space for each tier maintained. Tiers established by a colon persist as "sticky tiers" until reduced space ends the tier. So, there are two different basic ways of specification of content hierarchy with those delimiters. Without any colon at all, leading spaces in groups of triple space ("  ") as one for each tier, define one tier per leading set of triple spaces.

Trailing or Closing triple Space  Like with this very line as an example, in additional to any leading space, a title can also contain a trailing "closing" triple space "  " to establish one further provisional titled content tier. So, there is a title, then a triple  space, then the titled content that corresponds with that title. Only one final subtitle tier (an edge tier) can further form after with subsequent triple spaces, as a series of content separated by triple spaces. So the first trailing (closing) triple space is like an English summary paragraph while any subsequent triple space would be subparagraphs. Finally, a newline character terminates the content cell. So viewed as the perspective of a "tree of text", the triple space only offers the "leaf nodes" and cannot offer any main tier title nodes. Any final subtitle layer in English form is to be a capitalized and end with a period.  This very text further extends as a one sentence subparagraph, so a second

subparagraph on the same tier as the previous one.

Empty Lines as Sticky Tier Markers

As with common language documents, empty lines may be used to start or end information segments as paragraphs or sections, which in this protocol means content cells and title tiers. Tiers may be "sticky" in that leading spaces are not needed to maintain tier deeper depth, whereas otherwise tier depth always resets to root without leading spaces. Empty space can: (1) optionally hint at future sticky tiers with beginning empty lines, (2) end sticky tiers with ending empty lines, also decreasing the tier, by decreased empty line counts, or (3) end cells of a tier while the next line reestablishes another cell of the same tier again. Sticky tiers are more useful for establishing more root or beginning level tiers, but weaker for establishing deep tiers. A titled tier may be established by a title, followed by one or more optional empty lines as a tier depth hint, followed by content. Then, a subsequent same corresponding number of empty lines ends that titled cell. A subsequent fewer number of empty beginning empty lines may offer a further beginning hint or otherwise end a cell and possibly a tier as well if it isn’t reestablished as continued on the following line. As with other tier definitions, only one tier level is in focus at any given point in the text space. There are three important rules. Firstly, any leading empty lines after a title mark as marked by a colon ":" are a beginning empty line as optional hints at the final spacing that will end the sticky tier and any corresponding cell(s) and could also highlight separation of cells in the same tier. Secondly, more number of lines is for more root (beginning) level tiers, while fewer lines corresponds with more branching as deeper tiers. This reflects expectations that many empty lines between sections reflects a more major grouping as beginning root tiers, while fewer empty line gaps reflects a minor grouping as deeper branch tiers. That is an inverse relationship such that a lower number of spaces corresponds with a higher tier number. If a document text shifts from one empty line to two as an increase in empty line count, that ends the previous cell, then returns to one more root level (-1 tier), and begins a cell at that more root level tier. So, after a three-empty-line-beginning document followed by some content, one empty line ends a cell and reduce the tier as -1 to root, two ending empty lines end a cell reduce tier as -2 to root, and three empty lines end a cell reduce the tier as -3 to root. This could be seen as more of a potential tier reduction than actual because if the following line is a title, then the tier remains the same among the two lines as the title effectively adds 1 back to the tier level.

Empty Lines Confusions  It is encouraged but optional to use empty line hinting at the beginning of the

document by beginning with the number of lines corresponding to the maximum sticky tier depth. These tiers cannot go to a more root level than where they started without resetting the tier depth entirely. So, if one goes from three empty lines at the document start to four empty lines, all but the root tier ends, but the three-line-based root tier really just converts into a four-line root tier. Suppose a starting a document starts off with "My Story:" followed by three empty lines, followed by content. The first tier titled "My Story" then ends with three additional lines after the required content. Meanwhile, any pairs of two empty lines would then indicate tier 2 section(s), while single empty lines would be best for tier 3 section(s), but could indicate any tier from 1 to 3 depending on how they increased or decreased as an empty line count. If one were then to create another title with four empty lines, then all previous title tiers would come to an end and the new title tier would be considered root level tier. That could be considered confusing, so it is encouraged that an initial set of empty lines at the beginning of the document effectively declares the maximum number of lines for the whole document with that optional set of empty lines. One wouldn't generally want a document where the root level is defined by a set of three empty lines at the beginning, but then switches entirely to a set of four empty lines later on. Another less discouraged but potentially confusing situation is that one could create tier 1 with three empty lines, tier 2 with a colon, and tier 3 with two empty lines, so the mixed tier creation methods could be potential points of confusion. Yet still there is a third major confusion, which is that when using this recommendation, initial reduction(s) in empty lines don't change the tier, as the optional sticky tier hint was used, because one cannot go "before" or "more root" than the root tier. So, if a document starts with two empty lines, then there is content followed by one empty line and additional content, both content blocks are operating on the same tier. A tier must first increase before it can be reduced back by a one or more empty lines.

Title Referencing

Titles enclosed in quotes "" or parenthesis () create a reference to a title in another location rather than helping define the title in the current location.

Title-Content Pair Series Double Colon

This enables content titles with empty or null content. A title beginning with a double colon (::) followed by a new line enables multiple following lines of titled content set by a colon (:) without causing a persistent subtier to form as would normally be expected. So content delimited by a double-colon (::) "unstickies" the following single colons (:) until reaching an empty line, a line with just ";", or "end" marker. This is useful for configuration value list.

Title Dependence
happens here with these words, where a title is bound to it’s context by definition and is not seen as practically independent. So, the title itself may be used as the beginning of a sentence which continues with the content. This might be most useful for short content. This is useful for titles acting as phrase definitions.

Reference Numbering
The tier number starts at one and increments by one for each additional subtier. If all tiers are titled, the "current tier" is defined by the most recently defined title.

Titled content with colon equals ":=" and ";"
There are two title end breaks that cause a title to be for the current line or line segment only. The one-line title end breaks are "  " triple space and ":=" colon equal. A title end break only changes the tier for the current line and reverts the to previous tier at the end of the line. So for example, "Color:=Green;" only establishes the title for the content "green". The semicolon ";" allows many titled content pairs to be on the same line, and is needed to terminate the content sequence.

Title Independence
Title Independence happens in this section, where information conveyed in the cell title is recommunicated in the cell content.

Title Dependence
happens in this section, where information conveyed in the cell titled is implied as a dependency in the cell content.

Title Set Inclusion
As summarized nearby, there are multiple acceptable methods of title set grouping. Adding an extra newline (newline character) after the last cell in the group marks the end of a group. The "Titled Content Examples" cell example in this document shows two labeled cell sets. Content cell sets may be separated by one additional newline character after the bottom cell. If no subtitle is assigned, an empty line before the first cell in the set defines the beginning of the set (as already described in Empty Line as Set Definition section).

Title Whitespace and Capitalization In Searches
Spacing in title is ignored for most purposes such as searching, except when used as a title break as described in that neighboring section. Titles are case insensitive when in common title case. Common title casing is either capitalized letters, all small letters, or the first letter capitalized in a word. Uncommon title casing is expected to be a searchable difference.

Title Grouping
When there is a comma (,) in a title, it will create multiple titles that share the same content. For

efficient searching, the first value will be referenced value, while the following values will be a search reference to the first value.

Tier Title Leading Indicators

Leading triple space or sets of them refer to a previously defined title. The leading spaces in this paragraph refer to the "Tier Title Leading Indicators" title. Any further triple spaces refer to the "supertitle" instead. So, a newline followed by a series of zero or more triple space (’ ’) or colon (:) delimiter marks establish the title tier for the focused line. So, the leading spaces indicate the tier level matching the number of triple spaces. Each change in leading marks from one line to the next defines the tier for each line. An increase of one mark compared to the previous line increases the starting title tier further by one, while a decrease of one mark decreases the tier closer by one. Normally triple spaces (’ ’) are expected to be used. So, tiers created with triple space are end by decreasing the triple space count to lower than the number created by it. So, for a tier 3 title created with three triple space, it can only end back to tier 2 with a line having two triple spaces. Using both a colon and a triple space creates one tier rather than two. This could be used to add "summary" content or "primary" content to a title compactly.

File Line One Implied Colon

When the first line of a text document file has content without any multi-space interleaved padding, it is considered containing the first tier 1 title even if it has no colon or triple space trailing mark. This is because line one of a document is traditionally expected to be the document title.

Mixing Additional Tier Indicators

Mixed additional leading indicators results in ignored leading spaces. So, creating a title with a colon followed with a triple space on the following line would not cause a total +2 tier change but instead would be a total tier change of +1. So, if a title is done with the colon then it should not use any leading spaces on subsequent lines for each list value. Conversely if a title is formed by leading spaces, it should only use leading spaces for each of its values or subtitles.

Branching Cell, Branching Title, Branching Tier

A branching cell has subcells. Any corresponding title (branching tier) has subtitles (subtiers).

Edge Cell, Edge Title, Edge Tier, Edge Node

An edge cell or node has no subcells. An edge title (leaf title) has no subtitles (subtiers).

Cell Set "(continued)" mark

When a subtitled cell set ends, but the higher-level group of the hierarchy continues, an optional "(continued)" note may be used to identify that a previous group is continuing with additional cells for the group. See "Display Formatting: (continued)" cell

for an example of such usage. In that example, the cell continues as another member of a set of the main title tier. This is done when a cell subgroup has ended but the previous group then continues.

Escape Sequences

One Character  Downslash (\) (aka "Backslash") indicates the following one character should be displayed or otherwise taken literally rather than used for cell structure information. This escape character is evaluated before any other escape characters or escape sequence. Arrow sets "==>" and "<==" allow a series of characters between the arrows to be escaped in the same way. The start arrow "==>" begins the sequence while "<==" ends the sequence to be likewise ignored for cell structure.

Multiple Character Escapes  Quotes ("") and parenthesis () pause a title tier between those character pairs, while beginning another title tier being used as a reference.

Delimiter Interference Note

The downslash/"backslash" (\) do interfere with some languages or protocols.

Nearby Content

A ’nearby’ content is in the same title tier (having a shared title) as the currently focused section.

Neighboring Section, Nearby Section

A neighbor section is in the previous or next title of the same tier (having a shared title) as the currently focused section. So, "Titled Content Examples" is the next higher tiered section, labeled neighboring to this section. It would not be considered "nearby" to the neighboring "files" section in the context of Reference Protocol.

Subtitled Title Reference

A section reference implies a starting reference point at the first matching title in the superset neighboring options.

Competing Reference Protocol

This reference protocol is considered an alternative to protocol "RFC 3986" which defines "URI", "URL", and "URN" entities. The standard includes references they divide into "scheme", "authority", "path", "query", and "fragment".

Title Path  The title path is the colon (:) separated title as defined by the Plain Text Protocol (PTEX) title definitions. This usage of "path" may conflict with the term’s usage in other protocols so it is encouraged to use the phrase "title path" rather than just "path".

Files:

Data stored on the Zeronet (ZNET) is expected to be stored in PTEX data files distributed across many geographic areas. Files stored in such a format are expected to be more trustworthy as they are human-comprehensible files.

Files: File Structure

Files generally include (1)addressing, (2)title, (3)content, (4)citations and extended metadata, (5)file display formatting, (6)layout, and (7)file attachments. Factors in that list rank include importance and readability. Any or all of those elements may be omitted from any given file.

Files: Types

File types include text, app, database, network graph, image, audio, multigraphic (multiple embedded files), and multimedia (audio + video). All file types are defined in the Information Graph (Iggy).

Files: Data Field

Text and/or numeric text data entry records.

Files: Stream

Temporally sampled (time periodic record) media recordings including video and audio where sample/record takes place at fixed time intervals.

Files: Pages

Files which contain File Layout data, are considered Pages. A media file can also be a page. A page contain media.

Files: Text

Files which contain Author/From addressing, Audience/To addressing, and Plain Text content are considered a Text or Text Message.

Files: Addressing (1 of 7)

Author/From - Line skipped for anonymous releases
Audience/To - Line skipped for general public release
Time sent/released - May be skipped if not considered relevant.

Files: Title (2 of 7)

Title/Subject - May be skipped if seems irrelevant.

Files: Content (3 of 7)

Content data expected to be encapsulated in cells. Data may include media streams.

Files: Citations and extended metadata (4 of 7)

Citations
Self-Citation Information - Unique hash of data segments of the file (unique at publication time) which may easily be used in a citation in other files.
Extended Metadata - Considered extended because addressing information is file metadata. Common metadata may include creation time, modification time(s) especially most recent, content data size, format-dependent metadata for file such as video, audio, etc, and many others.

Files: Display Formatting (5 of 7)

Formatting of cells is done after all cells are defined. Formatting would include cell positioning. Example follows this cell. A delimiter should mark the end of all cells such as twelve empty lines followed by a line that says "end".

Zeronet Protocol: Simple Text Control Protocol (STCP): Comprehensibility

Simple Text Control Protocol (STCP) is designed as a subset of Plain Text Protocol (PTEX) as a set of computer interface controls such as for navigation and database interactions. This is designed to offer a file human-readable file format for improved comprehension in replacement of HTML and CSS. It is easier to modify applications with human-readable file formats because no reverse engineering needs be done regardless of having source code, commentary, an API, or other instructions. So, Simple Text Control Protocol (STCP) is a Plain Text Protocol (PTEX) designed as a more comprehensible internet display protocol than alternatives.
Furthermore, all data structures are expected to be represented by nodal network graphs, so we wish to shift focus of fundamental data structures as network graphs that can then be defined further as high-level structures such as lists, grids, and geometric shapes that can be used for display formatting. By forming structures from their most basic forms, we hope to further increase comprehensibility. Comprehensibility is important to security because a larger number of people can be expected to be able to audit code when it is easier to learn and understand.

Display Features

HTML tables are replaced with STCP boxes that more properly function as purposed display formatting elements. A box is formed with much cleaner code in STCP than in HTML or CSS. CSS does have box models that have become dominant, but using a language designed for "style" for structure is a contradiction in terms making the concept less comprehensible. The formatting proposal in this section considered a rudimentary draft which will only be developed after HTML and CSS has a stable implementation to Zeronet (ZNET).

Text Controls

Hyperlink

Colon Referencing

Clicking within any of these three text options: "ref:Color:Fruit", or "reference Color:Fruit", or "ref Color:Fruit", but not other formats like "go to Color:Fruit" should result in being taken to that section in this document. If the section doesn’t exist, it is results in an internet directory link for that term using the participant’s Web of Trust. This would be like an "I’m feeling lucky internet search" where the first link is selected but without any luck involved because the most trusted person available who tags the reference will be selected.

Underlined Referencing

A light grey underlined text also indicates a reference or hyperlink. The underline changes color upon being highlighted, and for 12 seconds upon being clicked or tapped.

Button *[Press Me]* where "Press Me" may be replaced

with any other caption, resulting in the referenced computer code being executed as directed by the Web of Trust application without necessarily changing the current view location.

Check Button *[ ]* where selecting in the box results in "x" or check " ", being displayed in the box, or if already there, will clear the box.

Toggle Button *[ ]* ("Radio Button") set where selecting in a set of adjacent boxes sharing one caption label results in "o" or dot "•" to appear, while any other already existing marks in the set will be cleared.

Textbox *( )* (with three spaces between the parenthesis) Results in the text in the textbox being available to the textbox creator's referenced computer code as directed by the participants Web of Trust application. The two spaces will not be relayed when used to send data. Received data appears in the textbox after any text already there, with the size being limited in the document formatting, though participants may designate a maximum size. Pressing the enter key sends the text.

Textbox Label The sequence *(Label)* allows the Label text to be inside the textbox rather than to the left as is traditional. When the textbox is clicked the label moves to a status indicator leaving a blank space as *( )* to be set by the participant.

Control Instructions Control instructions may have an associated instruction text area that appears when the participant sets focus on the control.

Dropdown List *{=}* which may also be the 3 vertical dots character results in a plain text list the participant is then expected to select from by setting focus to the equal symbol. The equal symbol is then temporarily replaced with a selection list while it remains in focus. There may be an item already selected which causes the equal sign to instead be replaced by the selected option.

Combo Box *{=+}* is a dropdown list where a custom selection may be added.

Combo Box *<=>* is a dropdown list where selections are addable, subtractable, and customizable.

System Text *||* A pair of vertical lines establishes a system message space. Text between the vertical lines should display system messages. The text "This Space is for System Messages" will appear if the user clicks inside, which doesn't have to be editable. Standard system messages expected are example field data, field requirements, field acceptance status, form submission status, processing statuses (ready/processing/x% done/etc).

Machine-Readable Content

Titled Content Title Casing: Titles for comparison purposes are "titled cased". Title cased is expected for search matching. For titles, whitespacing is stripped

and all case is changed to lower case. If a space follows the last title colon (:) then that one space is removed as part of the title while any remaining spaces stay as content. So, Titled Content title searches are expected to be case and spacing insensitive.

Variables Lists

Beginning A variables list is expected to begin with a line beginning with any number of spaces followed by "Variables List:" or "Variables Tree:" for a data tree structured variable list. Or, the list begins with a line that says "begin" only without any spacing.

Middle Titled Content as described in with this protocol.

End The list ends with a line beginning with any number spaces followed by "End of Variables List", or "End of Variables Tree" (for that data type), followed finally by a newline character. Or, the line may end with a line that only says "end" without any spacing.

Escape sequences (see that neighboring section) apply to all of the mentioned characters in the variable lists information.

Related This concept is extended by Group Records Exchange (GREX) protocol. Reference that section for details.

Display Formatting: Format Syntax

Example Format Instructions For This Document:
Bold all "shadow-banned" in "MESSAGE"
Italics all "You" in "MESSAGE".

The above example simply makes all instances of "shadow-banned" in the cells titled "MESSAGE" in a thick font and also all instances of the phrase "You" in italics. That instruction is case sensitive so that "you" won’t be in italics but "You" will be in italics. That formatting only applies to the Titled Content labeled "Titled Contents". See "Display Formatting" section below for full explanation of the example format instructions.

Display Formatting: Formatting Instruction Order of Precedence

1. Style Option
2. "all" Option - Format applies to all text matching the following text.
3. Start Position - Either a number for the character position in the file where the formatting starts, or the full word to be formatted which is preferred for short text areas (less than 24 characters). Followed by a list of numbers 1 to the count of that word, where the format applies to those corresponding words.

4a. Cell to be formatted if start position is defined by words instead of numbers. Prefixed with "in".
4b. If number position used, then ending position for format. Prefixed with "to".

Display Formatting: Style Options:

Font Set

A reference to the shape set defining the text character appearance. Sometimes called "font family".

Baseline Size

mm The size of the largest letter in the font set in millimeters as it is to appear on screen.

Relative Size

Percentage positive for larger than baseline, or negative number for smaller than baseline.

Display Formatting: Style Options: Alacarte

Bold

Italics

Underline

Strikethrough

Display Formatting: (continued)

Cell Connections

Cells are connected together such as follows: "Cell 1" -> "Cell 2" such that "cell 2" links to the right of "cell 1". Multiple cells may link up to the same cell in the same direction. "Cell 1" -> "Cell 3" would then vertically split space to the right of cell 1 between both cells. To connect cells vertically rather than horizontally, the "v" character is used. "Cell 1" ->v "Cell 2" causes Cell 2 to display below Cell 1.

Cell Layout

Cell content is positioned such that spacing is equal between cells until available spacing is used by content. Cells will expand in size as their content expands in size unless specified otherwise. Cells will expand to a scrolling mode when content expands beyond a default maximum size for the cell to limit their screen space unless specified otherwise.

Cell border.

A repeating graphic that wraps around the border of the cell. There may also be different graphic provided just for the corners which will be rotated according to which corner it is placed unless otherwise specified. The starting corner position is expected to be the top-left.

Cell outer margin.

Cell will have space outside the cell border according to the border margin setting.

Cell inner margin

Space between cell content and cell border

Shaped Cell

By default cells are boxes (squares). Other shapes are also supported.

Files: Cellular Layout (6 of 7):

Box

Inner Margin, Outer Margin, Border, Content

Zone

Top, Bottom, Right, Left, Corner, TopRightop, TopLeft, BottomRight, BottomLeft, Interior

Alignment

All box "zone" options except corner. "Interior" is both vertical and horizontal.

Vertical, Horizontal

Data Structures

Cell

Information about a specific entity. See "Titled Content" for details.

List

A cell containing an array of related entities.

Cellnet

Titled contents with information that is associated to one or more other cells. There is not necessarily a hierarchal relationship among cells, but there may be. The first cell created is the hub cell and any connected cells to it are "hubbed cells".

Titled Content Content Types

Any piece of information can be the content of a cell. Examples include Title, List, Navigation Control, Display Control, Function, Field, Record, Semantic Entity, Message, Shape, Physical Definition, etc. Full category list can be found in the Information Graph (Iggy).

Cell Array

All cellnet cells are array members in a cell array which consists of the following data sets:
Cell Identifier
Title
Content
Cell Connection Set

Cell Connection

Any relationship can be represented with cell connections. Examples include Control/Logic, Causal, Temporal, Mathematic/Statistical, Orthogonal Position, etc. Connections are comparable to a preposition in grammar and a pair of pointers in computer programming.

Cell Connection Set

Connection Identifier
Title
Connection Type
Connection Detail

Focused Cell

The cell which is in current focus for a given purpose.

Hubbed Cell

A group of connected cells, where there is one central cell that connects to all other cells in a "cellnet" hierarchy from "center" to zero or more spoke or "branch" cells, and finally to the edge, "outside", or "surface" cells.

HUB CELL  A cell linking to additional cells. May be considered a "branching", "central/centering", or "center" cell. The first cell to be mentioned is the hub cell unless otherwise mentioned.

TITLE  A hubbed cell data structure shall optionally have a title.

ARRAY  A hubbed cell array consists of any (whole)

number of surface and hub cells. Surface cells have primary data and likely a link to one "hub" cell, while hub cells have both data and connection information to one or more other "surface" cells.

Title

Edge Cell

A cell for content only rather than additional cells. May be considered a "leaf", "edge", or "surface" cell.

ToHub Cell Number

The hub to link to.

ToHub Distance

Zero if the node is a hub node, then one for the first tier of cells.

FOCUSED CELL A reference to the currently focused node for a given purpose, of a hubbed cell data structure.

Cell Sequence

A sequence is a data structure forming ordered data point cells linked in order.

Title

The title assigned to a data sequence and its structure.

Sequence Boundaries

First Link, Last Link

Sequence Cell

Focus Cell

The sequenced

Next Cell

Reference to the next cell in the sequence data structure. When Next Cell data is present, the sequence is a forward linked sequence.

Previous Cell

Reference to previous link in the sequence data structure. When Previous Cell data is present, the sequence is a double linked sequence. If previous cell data exists, next cell data is expected to also exist.

Unlinked Sequence

Link references are omitted. The order data is written defines order of the sequence for the data structure.

Display Projection

Metrification

When Netportal first begins, participants are expected to define the pixel size of standard symbols to appear on their screen as they set the size. The number of pixels per character is a frame of reference, as is the number of pixels on the display. This information is used by Netportal to render data to the device display screen.

Font

Users may vary width to length ratio of standard symbols on their screen. Other font modifications may be supported as well.

Display Dimensions
Display dimension is defined in terms of standard symbols which may fit by width and length.
Files: File Attachments (7 of 7)
A list of references to other files to be included as part of the file (if not yet already included).
Files:end

Plain Text Protocol (PTEX): (continued)

Group Records Exchange Protocol (GREX):

Summary
Group Records Exchange Protocol (GREX) is a comprehensible standardized plain text record table format and filing system for organizing, storing, and sharing information in such a way it can be searched and analyzed effectively. This system is expected to work for many or most Zeronet (ZNET) database records, ERP(Enterprise Resource Planning), CRM (Customer Relations Management), API(Advanced Programming Interface), and other organizational information system data exchanges. Support for tiered/hierarchical relationships such as records in Plain Text Protocol (PTEX) format is expected. All Group Records and Exchange Protocol (GREX) data is stored as human-readable text.
Plain Text Protocol vs. Group Records Exchange Protocol
Group Records Exchange is a restricted as simplified subset of Plain Text Protocol (PTEX) so that all records can be expected to be stored and associated in an identical format. Furthermore, it includes formatting for efficient (or less inefficient) searching of records which could be considered outside the scope of a goal set for "plain text".
Competing Protocol
MyISAM (developed for MySQL) is the primary competing protocol. The main focus of Group Records Exchange Protocol (GREX) is comprehensibility. The focus of MyISAM seems to be other factors including speed.
Delimiters
In addition to Plain Text Protocol delimiters, Group Records Exchange Protocol also uses Vertical Pipe "(|)" and braces [].
Essential Table groups
Essential table groups include tables needed to establish Zeronet (ZNET) connections and Cog connectivity.
Standard Table Groups
Standard table groups include any information expected to be shared by organizations including data regarding geolocation, logistics, contact, financial transaction, inventory, statistical study reporting, offerings, messaging, public trust reporting, and private messages.
Database Answers Website:Data Models and schema.org may

be valuable sources in establishing this protocol.

Table Metaclass

Essential: Expected to be needed for any use by all participants or organizations.

Common: Expected to be used by most participants or organizations.

Extended: Expected to be considered for use by specific types of participants or organizations.

Note: Zeronet Service Cogs (COG) (see associated section for details) also have this metaclass structure.

Style Restriction for Titles

While Plain Text Protocol (PTEX) allows more than one title on one line, Group Records Exchange Records (GREX) fixed width data is expected to have only one title per line to encourage an identical record format across all organizations. Furthermore, only edge tiers (tiers without any sub-tiers) should use the titled-content assignment delimiter of Colon and Equal (:= ) followed by one space, and that is the expected method when a sub-tier has one value only rather than a value array.

Identifier Tagging

This tagging method is expected to generate a unique identifier as a "GREX tag" for PTEX database records. In variable-width format, individual GREX records may be formatted as PTEX formatted titled-content pairs. These pairs are then written back in the fixed width GREX record format. The double-colon title-content pairing system is the encouraged method, though the leading space tier system should also be supported. To the end of that generated record, a new line followed by the number of characters in the record will be added. Each record will have a SHA-512 hash calculated including the appended followed by an equal sign ("="). The SHA-512 algorithm will then be done on that record, and the first 42 characters of the hash code will be added after the equal sign. That last line will then be the "GREX tag" for the record.

Metacodes

Records are universally "tagged" (identified) by first structuring the record according to the Group Records Exchange style of Plain Text Protocol (PTEX) as described nearby. When groups of tags are them selves given a tag, the tag is then considered a type of "metacode" that applies to database records.

Table Layout

Each table is a text file or text file set expected to have at least two columns including one unique identifier to be called the "tag". Rows in the table all have the same number of fields. Columns are separated with a vertical line (|). A semicolon may end a field early unless lead by a downslash (\) ("backslash") Composite keys are not directly supported as they are less comprehensible. The table should begin with its most recent modification timestamp. Additional columns

are considered "minor" columns are put in another file with the same structure but different data (except tags) and are expected to be restricted to metadata such as record modification timestamps, edit count, deletion flagging, and row display information.

Table File Spacing

Files are filled with "empty space" for faster row writing times. Files begin as "empty space" filled with whitespace characters (" "). Each file is expected to start at a number of bytes based on the Fibonacci sequence, and when being expanded is expected to expand into the next Fibonacci number of bytes. Tables are expected to start at a size such as 20,736 bytes. Tables also are expected to have an upper limit on size based on the device being used.

Tag vs. Key

A tag is unique value to one column only. So a tag is never a "composite key" and only a "simple key". A tag will also act as a "primary key".

Table Sorting

Tables are expected to be kept in two versions. One version is sorted by tag column and the other by major column in ascending order. This enables fast searches. The file is to begin with a timestamp of the most recent sorting time. The table sorted by key takes precedence over the table sorted by value in case of a mismatch for repairs.

Table Index

Sorted tables are expected to begin with an index table. The index record rows are sorted in ascending order. The "key" are the first bits of a given indexed field while the "value" is the character position in the file. The file is to begin with a timestamp of the most recent index time.

Auditing Table

Table(s) that track another table that may record record modifications, deletions, and searches of an "audited" table.

Table Viewing and Editing

Netportal is expected to have a portal for developing and viewing tables.

Derived Columns

The major column in a table may be computed by a provided calculation.

File Directory Structure

The file system layout is used to indicate database information. The folder name should be the same as the table name. This allows metadata

Signature Code, Crosslink Code

Signature codes are expected to be appended to the beginning of metacodes (see associated section) on the following line as identification codes (as hashes) before signed as follows.

ACK:= Acknowledged; AGR:= Agreed; TRS:=Trust; HNR:= Honoring; DNR:= Dishonoring; DST:= Dissent;

Group Records Exchange (GREX): Data Tables:

Major Sections  The major sections expected in bold are the table metadata which may be untitled, the table rows as titled, any variable table rows, and the index as titled. One empty line should separate each of those parts. The metadata heading line as the first line should consist of the protocol used followed by all "leading titles" in the file meaning the first titles in titled rows.

Major Section Heading Line Example:

TABLE: METADATA, DATA ROWS, VARIABLE RECORD SIZE ROWS, INDEX

Each element of the heading line corresponds with a section of the table which should titled in PTEX title format and also separated by a newline character ( ). The file ends with six to twelve newlines followed by the word "end" followed by another newline.

File Pointer Syntax

"file:byte number as integer" refers to a specific byte position in the current file. Also supported is common file structure notation with an integer in the "fragment" position. So, "file://myFile.txt#12485 would refer to byte location 12485 in the myFile.txt text file.

Metadata

Table Title  If the metadata is subtitled, the subtitle is expected to be the table title. The table name should as specifically as possible describe the contents of the table. The table name should be singular if a tag represents one entity or plural if a tag represents multiple entities. Table names may be subtitled using the PTEX colon (:) delimiter (title:subtitle).

Style

Grid  A series of fixed-width columns separated by a vertical line (using the vertical line ("|") character) between each column.

Tiered Grid Rows  Some rows without any vertical lines, which will be padded to be the same size as the other lines, will act to title the following rows and also use the title as a (nonunique) shared grid value to the beginning of each row.

Tiered Expanded Rows  Rather than a grid, data is defined only by tiers and established only leading whitespace, so there are no implied tiers or abbreviated tiers with leading colons (":").

Table Count  The number of tables in which the same rows may be arranged in a different order.

Fixed Data Location  Start and End of fixed data.

Variable Data Location Start and End of variable data.

File  The number of files the table is distributed to. Files may be limited to a size such as 4GB.

Characters  The character set protocol used for the file such as UTF-8 or ASCII.

Row

Size  The character count size of the table row data.

Count  The row count of the table.
Filled  The number of nonempty rows in the table.

Form

Table column structure information are fixed size records beginning as one row for each column description. This table is for describing the table structure for the data, and does not contain the GREX data itself. Each table column is listed along with information describing each column. Then there is to be one fixed size line for each calculation used in any rows.

Columns  The number of data fields in the table.

Form Row Size  The character count size of the table rows that describe the table data.

Column Names  Column names are expected to be up to 60 characters long.

Tag Flag

Tag  Each table may have one column which uniquely identifies each record row in the table. The name of the table is also considered another name of the "tag" column. So, if the table is named "Contact" each "Tag" represents the identifying mark for one "contact".

Unique  A table column may be required to have a unique value for each row.

Tag Reference  "Foreign Key" A table column may contain data that is only a reference to a value in another table.

Size  The size of each column is expected to be limited to a specific number of characters. Columns marked "Varies" could be any length. Note that the actual fixed size may be shorter than the maximum length up until data of the maximum size is entered.

Data Type  Description of the data structure. Expected options include tag, text, numeric, and integer.

Controller  The person granted enough trust to modify the records.

Calculated Column  Tables might be generated dynamically based on a functional calculation. Functions are considered "basic", "common", or "extended". Basic calculations include all the singe-key mathematic operators on current keyboards. (!,%,^,&,*,}{|;-+/*})

Calculations  If no calculations are used, the line "(none)" should be added after the "Calculation:" title expected to be at the end of the table columns information table. One full fixed size row is expected per calculation column.

Basic Functions  Addition (+), Subtraction (-), Multiplication (*), Division (/), Modulus(%) , Factorial(!), String Concatenation (&), Exponent (^), Expressional Grouping Parenthesis "()", Conditional/Equality Operations (==,<,>,>=,>=)

Common Functions  Common functions are those

functions supported by most spreadsheet applications or most of the common coding languages.

Extended Functions  Extended functions are column calculations neither basic nor common.

Grid Heading

Heading rows are used for grid column captions, sorting information, and could be used for other column metadata. The heading row is expected to define any title tiers and mark where the vertical line delimiters (|) belong which separate data field columns. This can also be used to establish column character size if not previously stated. The tier number corresponds with the heading line number from the bottom line. The last line is the highest tier, which each previous line as one lower tier. So, tier 2 data would be on the 2nd to last line. The position of the heading vertical lines is expected to exactly match with the position of vertical lines in all column rows. Any missing vertical lines would be considered corrupted data.

Captions  Caption rows are expected to title the data.

Caption Abbreviations

If a caption cannot fit in the space between vertical lines, an abbreviation is used and then the corresponding title is listed in the table form metadata as a "caption" column.

Control Domain

The controller of the tag column is also considered the controller of the table in general. The table controller or anyone with a higher trust rating assigned to the control domain may edit those areas. Each table column may be created with a different controller. That controller or a more trusted person may edit those areas. This trust is within the context of the control domain. The control domain will be for a specific purpose such as a contact list in the Web of Trust. So, only people who are trusted for that purpose may edit those records. For Web of Trust, mostly just the "SELF" is expected to be the person to edit those records because they can be used to control many other Zeronet (ZNET) GREX record sets. "SELF" is a reserved tag that begins as the full controller of all control domains (or trust domains).

Editor

When editing is taking place, editors are expected to reserve the file to be edited by only that one editor until editing is complete. The creator of the table may edit the table. Anyone trusted more than the creator under the same control domain may also edit the table. Editors are expected to be able to modify records at a specific performance level such as in terms of row edits per second. If that performance

goes below a specific value based on the expected device performance, the reservation is nullified and another editor may take the reservation. A Zeronet (ZNET) cog is expected to manage reservations.

Data Rows

The data rows consist first of the fixed size data rows and then the variable size record rows. Each fixed size row contains columns of the same size separated by the vertical pipe (|) character. Expected information in the first row includes the row byte size, row count information, the count of tables in the row, "Sort Order Row;" if the table is sorted, and finally the text "Dynamic Rows" if there are dynamic rows in the table. The table rows are listed once for each column sorted. If a column is expected to not be specifically searched then it should remain unsorted. The entire table is repeated for each sorted item. The table heading is restated for each table, which first has a row listing all column names corresponding to their position below. After that there may be a sort order information row with the sort status of each column. Sort statuses are expected to include "(ascending)", "(descending)", or "(unsorted)". This column may also have unindexed columns marked ", unindexed" added to the column sort information such as "(unsorted, unindexed)". Columns are otherwise expected to be indexed.

end footer After the last data row, a line is expected beginning "end"

Filler Space

Rows using fixed size data begin filled with filler whitespace. The filler space allows records to be added without creating a new file. Both leading and trailing spaces in each column before and after the vertical line delimiter (|) is added are not considered part of the field content, but rather are empty space.

Variable Record Size Rows

Variable Record Rows are to be referenced with "file pointers" (see nearby section) from fixed size rows. Each variable size record row begins with the fixed size tag field. Then there is a vertical line (|), then there is the table column, ending with another vertical pipe (|) followed by a newline character ( ). Variable size records are discouraged from being searched through. Instead, the variable data itself could be parsed into individual fixed with records which can be more easily searched. At least one empty line is expected to follow the section, but two empty lines may follow the section when one of the newlines is acting as a filler character, and there is not space for any further spaces on that filler line.

Index of Fixed Data Rows

The index lists starting characters of a row tag, and

the character position of that record within the file. There is expected to be one index entry for every specific number of rows such as 24 rows. When the index itself reaches 144 records, the index itself is expected to be sub-indexed the number of times needed for entries to be less than 144 index records. The index records, as with the table records they reference, are fixed size rows. Each index is expected to be subtitled as "Start Positions Sorted by (column name)" where "column name" is the name of the column sorted in the table.

Index of Dynamic Size Data Rows

Dynamic data isn't expected to be searched through because it would be inefficient. Instead, each dynamic record should itself be fragmented into parts for distribution to a fixed size database.

Meta Table

Records of processing a table are considered "secondary records" and "table metadata". Each GREX file may have another file with "_meta" added to the end of the filename and having the same file extension. The meta file is expected to be a table that leaves an "audit trail" of a specific file which includes records of creating, modification, and accessing of the "primary record" along with the person or process name causing the table activity.

Column Referencing

For table processes including column calculations, tables are expected to be referenced in "dot notation" (similar to SQL).

Sytax: tableTitle.columnName

Tables may be titled using PTEX title hierarchy with colons to mark subtitles.

Expansion Method

A percentage of expansion space is shared between fixed and variable. The expansion space will fill at the same ratio as the current file is filled. So if the current file is 50% variable size data, the expansion space will be filled with 50% of filler space for variable size data.

Record Spacing and Expansion

Records are initially spaced according to the first character in the key. Using base 64 records as an example, characters expected record writing are a to A to Z, then 0 to 9, then "+" and finally "=" for a total of 38 character options. So, the number 0 would be expected to be first placed in the 26/36 position, which would be  When the records expand, the spacing is based on existing data statistics for that table. Variable records are filled sequentially in order to the end and then the record expands. For fixed size records, the record set is expected to expand when available space is less than a certain percentage like 40% available.

Example

Reference the GREX attachment for an example Group Records Exchange (Grex) file.

Group Records Synchronization

Metacodes (see associated section) can be used to synchronize Group Records Exchange (Grex) records.

Group Records Exchange Record Metacode Construction

Metacodes are based on a record being constructed in PTEX "tree" format (see associated section) using leading spaces to define the tier level of each record field. A metacode record could itself consist of other metacodes in a hierarchy. Basic metacodes are in simple chronological order of publication for record sets that may not be edited.

Variables List

is a simplified form of GREX for defining settings and variables as text for an app. The list begins with a line beginning with any number of spaces followed by "Variables:", case insensitive. Following lines are title-content pairs. The beginning of the line is a variable title followed by a colon (:) then one space and then the variable content as one string which lasts until the end of the line. This is simple to parse but has no escape sequences and so is limited in capabilities. Arrays will need further parsing. The order of the title-value pairs should be unimportant. The variables list ends with a line beginning with any number of spaces followed by "End of Variables".

GREX Tables:end

INFORMATION GRAPH (IGGY):

Primary Purpose

The primary purpose of the Zeronet (ZNET) Information Graph (Iggy) is to organize content into categories in creation of easy to discover topics and channels.

Information Graphs

An information graph represents information in the form of nodal patterns as network graphs (see associated section). A network graph is expected to consist of one or more sets of edges and/or vertices connected together. This is typically portrayed as lines that connect dots together on a network chart. Lists and sets are the most common expected data type, but all data types are supportable. A network graph is used because it is able to accommodate or integrate a wide range of other data structures. Such a data structure is used by Zeronet (ZNET) for several reasons. Zeronet (ZNET) can be searched using an information graph based on directional search paths as further explained in Information Graph Cogs:Database and Search Cogs. This structure can be used to implement the Focus Portal (FP) system of information queries. Visualization of information in this structure is possible using a

network visualization Service Cog (COG). Text and audio can be loosely translated across multiple languages using an information graph.

Use Cases

The Zeronet (ZNET) Information Graph (Iggy) is expected to be formed cooperatively across a number of various public databases which may be both pay to read and pay to write, although different databases may have different incentive structures or may be charitable or otherwise sponsored. This data structure style is particularly useful as a Topic Map (ref Public Content Network:Topics:Topic Map) database table for the Information Graph (Iggy). Metastream Providers (Public Content Network:Key Features:Metastream) are expected to form contracts with an Information Graph (Iggy) Database Cogs (ref Database and Search Cogs:Public Information Database Cog) to stream recent content reference additions from content creators to evaluate newly created content. The actual content isn't stored in the Topic Map Database table, but references to the content are stored in the Topic Map Database table. Search services such as the Topic Search Cog (ref Information Graph Cogs:Database and Search Cogs:Topic Search Cog) will also want that same data for their search databases so that participants will have up-to-date search databases for their Public Information Database searches.

Graph Domain

There are multiple possible structures which attempt to represent knowledge in the form of patterns represented by network graphs. Each Zeronet (ZNET) component should be considered a domain of the Information Graph (Iggy). Valid Information Graph (Iggy) service providers are expected to update information to the Information Graph (Iggy) in "real time" as new content is added. Creators and Public Information Databases (ref Database and Search Cogs:Public Information Database Cog) of sufficiently similar graph domains may attempt to merge their record sets where doing so increases efficiency.

Hidden SubGraph

is a node cluster which the name has been hashed or both hashed and salted. Such nodes are expected to have no substantial connections to the primary graph.  most often zero or one connections regardless of how large the subgraph becomes. This number of connections is designed for added privacy. The one "connection" to the primary Information Graph (Iggy) could also be a connection to the 'Null Node' or 'Zero Point Node' which is also designed to establish the graph as a private information service which is only indirectly rather directly connected to the Information Graph (Iggy).

Information Graph (IGGY): Structure:

Graph

Space laid out to show a set of numbers.

Network Graph

Space laid out to show a set of numbers which may link together.

Semantic Identifier

A symbolic representation of anything at all.

Nodes, Topic Nodes

Each Information Graph (Iggy) Node represents a semantic entity. Each semantic entity may have various relationships with other semantic entities. There may be multiple records for each language lexicon. Each semantic entity is expected to be assigned a topic title so it can be "mapped" on the Public Content Network (PCN) network "topic map".

Node Identifier, Topic Identifier

Each node is assigned an identification tag as a digital hash for faster node data retrieval. The node identifier is encouraged to be created by a formal and consistent process according to Group Records Exchange Protocol (GREX) Identifier Tagging record format set by (Democratic Communication:Plain Text Protocol:Group Records Exchange:Common Table: Information Graph (Iggy) Tables:Topic). So, the Public Content Network (PCN) network graph corresponds to the Information Graph (Iggy).

Semantic Entity Network Graph

Content is graphed according to one network node per semantic identifier. Each semantic identifier is expected to have one or more "topic titles". Each network node may connect to one or more other network nodes, and each connection has a strength or weight representing how strong the connection is in comparison to other nodes. Connection strength depends mostly on push and pull volume (uploads and downloads) which references the node.

Multilingual Nodes

Multilingual nodes are words that translate well to multiple different languages with few resulting conflicts. Multilingual nodes make it easier for SigilX Service Providers (ref Democratic Communication:Sigil X Protocol) to offer simplified text translation services.

Node Cluster

Semantic Entity Network Map nodes may be grouped in clusters when there exists between them a type of association or relation. These clusters are most often likely to be sets, lists, sets of sets, and lists of lists. Node cluster will have a title and classification. May be used for lexicons and sigil sets. For example. Sets may be referred to as clusters on the Information Graph (Iggy).

Node Connection

Each node connection represents a relationship between two Information Graph (Iggy) nodes. Relationship types reflect common propositions. The basic relation is an association. However, more complex detail can be found in relations. Relationships may include is-has, has quality, has quantity, cause-effect as previous/next,

ranged/quantity prev/next, ranged quality prev/next, inside-outside, noun-verb word version, etc as determined by consensus and negotiations. So while simple types such as lists are most common, more advanced relational data is supported with compatible software components may be designed with broadening node connection type support.

Node Cluster Development

The energy required to create a node cluster association is expected to be compared to the benefit of its usage. Statistics analysis is done to calculate the value of a given node cluster to determine whether each given node meets a minimum benefit for inclusion in a node cluster. For example, how often would the node be used as part of the cluster, and how much resource is required to incorporate the node to the cluster. Metastream Providers (ref Public Content Network:Key Features:Metastream) are the people with primary responsibility of bounding node clusters because they deliver information streams based on topic node clusters.

Connection Layers

Node Clusters may be organized in a hierarchy or multidimensional structure. Examples that may be represented by organized clusters include such concepts as information grids, a spider web, a warehouse with shelves and those shelves having boxes, a combination lock, a circuit of any kind, a transportation system, and a multi-line comma separated list. A connection layer is comparable to a dimension in mathematics. The cluster may then be "navigated" from one cell to another by focusing on the connections among cells. Connection layers are expected to be formed where simplicity is increased by another layer.

Lexicon Graph

A node set within the Information Graph (Iggy) which matches symbols to meanings. Contains text-based symbology and also phonetic symbology. Each language is a semantic subset on the Lexicon Graph.

Topic Referencing

Topic Profile

In the context of the Information Graph (Iggy) a profile includes a definitions, associations, and descriptive information regarding a topic so includes dictionary entries, encyclopedia entries, and other information about a topic as accepted by a shared perspective. This topic profile is expected to be accessed with a referencing system.

Topic Tree Format

The Group Records Exchange protocol is expected to list topics and and how they are associated together. Topics are expected to be organized as a data tree. A tree begins with a trunk at the trunk root and splits into branches. Each branch can split to a number of smaller branches until. The end of branches are

expected to contain leaves. A data tree uses that concept as a metaphor. Each titled topic may be referenced as a Title Path (ref Democratic Communication:Plain Text Protocol:Title Path:References). So, each title is a branch while the leaves are the values associated with the title.

Topic Tree Connection Layer, Topic Tree References
Informational text is expected to branch from general to specific topics, and commonly referenced to less commonly referenced topics. Participants can select an information service such as by a Topic Cog (ref Service Cog:Public Content Network Cogs:Topic Cog) to define the divisions between topics which determine what content matches with which topics. A reference tree is a complete Information Graph (IGGY) connection layer which is formed as a data tree. Data tree references are expressed as a Title Path (ref Democratic Communication:Plain Text Protocol:Title Path:References).

Incomplete Section Mark
Sections beginning with a triple asterisk ("***") are so marked as incomplete. This differs from common written language which uses such a mark at the end of a word or sentence to reference another section of a document.

Ref, Reference
To reference a given topic, it is expected to be referenced as a set of topics in parenthesis () using a Title Path (ref Democratic Communication:Plain Text Protocol:Title Path:Reference) starting with a reference root name and then going from most general to most specific, and when generality isn’t known then most commonly accessed to most rarely accessed topics. The most general topic begins on the left and is more and more specific to the right. An example of a reference is "(ref Human:Resources:Foods:Bananas)". The topic service selected by a participant would determine whether "(Resources:Human:Foods:Bananas)" are the full path to bananas or "(Human:Resources:Foods:Bananas)" are the correct path. The topic service could also automatically convert a reference from one version to another so that either one would be functionally the same, but that may not always work because order is important for some topics. Reference (Service Cog:Public Content Network:Topic) Cog for additional details.

Technical Language
When a section of text information does not contain a full description and definition of a given topic, it is expected to be marked as technical language with a reference to to full description and definition in each final branch of a descriptive topic tree. For example "(Technical Language: Computer Programming)".

Topics linked to on the information graph are encouraged to be organized similarly to an encyclopedia, though with a branched titling system compatible with the Information Graph (Iggy). Each paragraph is encouraged to be titled. To keep topics easily accessible using the Information Graph (Iggy) paragraphs as sections are generally encouraged to be only a few sentences long (less than 2,000 letters or characters) though are discouraged from having a specific limit.

SERVICE COG (COG):

Feature Summary

A Zeronet (ZNET) Cog is a automated information service in a set of related information services designed to be easily replaceable with alternatives. Client-side means a process on a participants local device while "remotely managed" means outsourced to another participant or additional devices in another location(s). Reference "client-server dichotomy" to learn more about those terms. Cogs could be considered as having two types of components, "front-end" client-side components as "cog portals" and "back-end" or remotely managed components as the cogs them self. Cogs having any remotely managed components will be considered remote cogs even if most processing is client-side. Cogs are expected to work on a broad range of computers. The Cog is generally expected to be controlled through a Cog Portal (ref Netportal:Portals). This section contains a partial list of important cogs, but is incomplete as new cogs are expected to be constantly created.

Service Latch

When a participant uses a Service Cog (COG), they "latch" the service. When multiple services are latched that offer the same functionality, the participants Web of Trust select service manually or automatically according to their preferences. The Netportal service console is expected to have multiple factors in selecting the service provider. Factors are expected to include trust level, speed, price, and quality of each service.

Information Service vs. Cog

A Cog is an automated information service applied to Zeronet (ZNET). All cogs are information services. A information service may or may not have a service portal. A cog is expected to have a related Portal (Ref Netportal:Portals to Replace Websites) which manages use and activation of an information service. So, Cogs are expected to work like current "browser extensions". Many information services are described in other sections and then reference specific details in the Service Cog section, while some information services are described exclusively in this section although they may be also strongly associated with other sections.

Cog Default Distribution

All Zeronet (ZNET) participants run common Information Technology services and sell unused system resources to the highest bidder automatically unless settings are changed to the contrary.

Resource Availability

Participants are encouraged to provide their expected future device availability information for the cogs they share across Zeronet (ZNET) as service provider participants. Their history of availability is expected reported by their service reviewers. By forming teams across distant time zones with a mostly automated process, people can collectively form higher service Cog availability. Some service cogs such as the Token Pack Cog need to be available constantly.

Common Cogset

Each participant is expected to form a contract for Zeronet (ZNET) cogs with enough services to access the Zeronet (ZNET) platform according to their individual demands.

Cog vs. Consultant Interface

A cog only performs services in an automatic way according to rules that all service providers are expected to list in their contract. Any service that requires manual performance is not a cog. However, a Cog that performs some performance manually is a cog if most of the performance could be determined as being automatic by such a measure. Otherwise it is some other type of software or application acting as a consultant interface.

Cog Portals

Cogs should have an associated service portal to interact with that service or at least provide status information. Service cogs are expected to provide a user interface for their service via a service portal. Reference Netportal:Portals to Replace Websites for details.

Cog vs. Cog Portal

A Cog is the back-end features computer programming code for a portal (in a programming language such as Python or C++), whereas a portal is the front-end graphical participant interface for controls expected to be formatted by Plain Text Format (ref Democratic Communication:Plain Text Protocol) or HTML. A typical portal will generally be expected to pull data from the internet while a cog portal may or may not need the internet depending on the features. Some portals might be able to be used for any user interface system which could be a system outside of Zeronet (ZNET) entirely, especially when coded as HTML files. When ’latching’ onto a Cog, the service portal would fail if the service requires a connection to another computer (as a cog service provider) that cannot be found. The service portal may or may not work if one portal is used to connect with multiple service providers, though we hope

to design the network such that portals for identical purposes and features are practically identical and the same portal could work with multiple Cogs of the same type. Current browsers already have a comparable system where the search box on their internet browser app can work with multiple different search engines. So, the search box as as a portal while the search engines act as the "cog". For website developers: Unlike current websites where it is often considered unethical to copy an HTML file and use it for another website, it is encouraged behavior to copy a portal file to use it for your service or database when possible. It is encouraged to develop standards in a public forum such as using the Open Collaboration Protocol (ref Democratic Communication:Cooperative Development:Open Collaboration Protocol). The reason for this change is the initiative of portals is on information sources who want their information to spread in as many ways as possible, in a shift away from website creators who have incentive to monopolize provided information. So, portals are more re-usable than HTML websites. By coding a portal, donation requests are encouraged while requiring payment is strongly discouraged. Because novice participants are expected to only notice their Cogs through Cog Portals, there could be confusion on cogs vs. cog portals.

Cooperative Computing Service Integration

Service Cog (COG) may be further developed to offer a platform for "software as a service (SaaS)", "application service provider (ASP)", and "platform as a service (PaaS)" style computing services.

Cog Distribution

Cog are encouraged to have at least one back-up service location in case the first location fails.

Cogs As a Full Organizational Platform Potential

Because Zeronet (ZNET) can include all aspects of organization including Open Exchange (OX) (ref associated section) in one protocol as Plain Text Protocol (ref Democratic Communication:Plain Text Protocol), Zeronet (ZNET) cogs offer an opportunity to both develop and market any information service for an organization seeking to sell computer software or computing services by linking with an IDE that supports plugins. So, a Zeronet (ZNET) plugin could be developed for IDEs which support plug-ins or have an API. This would be similar to having an IDE with a Google Play or Apple Store plugin. However, because Cogs are easier to develop than complete apps, it would be the easiest way to sell software functionality as a "cloud app" and so be a very powerful feature. And it would be easy to develop after Zeronet (ZNET) is complete because Cogs are encouraged to be simple single files.

Cog File

Current computer operating systems provide a "home directory" for each user. The home directory is expect to have a "Netportal" folder. The Netportal folder is

expected to have a "Portals" and a "Cogs" folder. The cogs and portals folder are both expected to contain one folder for each cog name, so that each cog has a corresponding portal. Each cog portal folder is expected to have a portal file for each cog portal version available named the same as the cog version. Likewise, each cog folder is expected to have a cog file for each cog version available sharing the same cog name.

HTML Cog Portal Files

HTML Default Values

(Technical Language:HTML)

Each cog portal is expected to default values such as for settings, controls, and calculations. Cog portals are expected to be linked to a specific cog version. A folder should be created in the directory "[home directory]/Netportal/Portal/[portal name]/[portal version] Data". Each HTML element with an id tag (such <input type="text" id="myFieldValue" value="seeking default...">) may be provided with a default value. In the data folder, a file may exist for each default value named according to the id, so myFieldValue may have an associated "myFieldValue.txt" file in the folder. A javascript script will, upon loading of the page, set the value of each field according to the provided default values through a Netportal data request.

Embedded Javascript

(Technical Language:Javascript)

A non-cog portal may also function as if they were a cog to some degree when having linked Javascript files. This is generally discouraged because Cogs can easily interact with each other under many languages while Javascript cannot easily interact with non-Javascript files. To use Javascript as a cog, special support would be needed to be added to Netportal such as JSDB. Or, JS2PY could be used to convert all Javascript files to python files.

Service Cog: Cog Development

Cog Programming

(Technical Language:Computer Programming, Computer Networking)

Most computer programming languages are able to create a cog, but security precautions are expected to heavily restrict programming options with a permission system each participant has control over. Netportal (see associated section) provides a "universal API" system. The universal API provides a shared memory, one part of which is persistent on disk and the other part is temporary, for each operating system sessions, in system RAM. The API also provides communication channels using TCP/IP sockets both remotely and locally for

communications between applications. This is done partly so that it is easier to have cogs that can work locally on a machine or remotely, as TCP/IP is used regardless. Each cog is assigned a folder within the persistent memory and is assigned a maximum persistent and shared memory usage. The folder is expected to include the cog application executable scripts, compilable code, or binary executables depending on restrictions and trust levels set by the participant. Cogs have access to other shared memory areas based on trust levels and permissions set by the participant. Each cog is encouraged to expansive access to its operations by registering variables and functions with the API. Functions are called using provided Netportal API TCP/IP socket commands. Variables are likewise manipulated though the Netportal API TCP/IP socket command set. All data stored on disk is expected to be stored in PTEX formats including Group Records Exchange (GREX) format (ref Democratic Communication:Plain Text Protocol). Netportal API provides a set of PTEX functions including Group Records Exchange (GREX) functions. This functionality also encourages each GREX database created by the Cog to be registered as available to other local cogs using a Netportal API TCP/IP socket command.

Naming

Cogs are suggested to be named briefly and plainly and with few if any acronyms, in a way that describes what they do. The version is suggested to be named according to the main author followed by the time of release. The time of release is suggested to be the most broad time in which a further release is unlikely. So if the author is Henry and releases are expected to be once per season, then the version can be named "Henry 2022Q1", "Henry 2022Q2", and so on. The portal file is expected to be named the same as the version. A release during the winter would instead use the 3-letter month abbreviation (Dec, Jan, Feb). Season names are discouraged because a "winter" north of Earth’s equator is "summer" south of Earth’s equator. Furthermore, "winter" includes both the beginning and end of any given year. If another release happens in the same time period, the time can become more specific like "Henry 2022Jul4".

Service Cog (COG): Public Content Network Cogs:

Metastream Cog

Lists content a Zeronet (ZNET) participant is likely to find most valuable. Common content types displayed on the metastream may include news stories, personal messages, media streams, and (any wanted) commercial offer information. Information Graph (Iggy) nodes are subscribed to based on the interest level of each topic. The Web of Trust is a part of the Information Graph (Iggy) section where each node represents a person, and the subscription level is based in part on the trust

level of the person. The primary concern is the Information Graph (Iggy) topic value map showing which nodes have content that results in donations. Another concern is nodes having content that is formally reviewed. Another distribution factor is time spent per topic, with more subscription to topics of more attention of time. All of these factors are weighted by how strongly referenced content is to a given node and metastream. After content has been loaded, it will generally not reappear on the recommendation list. Each time recommended content isn't loaded, it will be less likely to appear on the recommendation list in future recommendations.

Private and Public Metastream

A public metastream has a different process for predicting which messages will be valued than private (as in private messaging and other private data) metastreams because the mode of payment is entirely different from public to private. So, it is expected that a Private Metastream provider will be a different service provider than a participant's Public Metastream provider. Furthermore, it is better to compartmentalize the two so as to avoid leaking excessive information to any one provider. All private messages (ref Democratic Communication:General Concepts:Private Messaging) are encouraged to be encrypted for better security. Any unencrypted private messages are expected to be routed though a Data Negotiation Service (ref Web of Trust:Data Negotiations Service) if one is set up for a participant.

Content Value Prediction Cog

Calculates likelihood of a user pulling (downloading) content when displayed with specific metadata such as a specific title and lead-in image. This data is used by other Cogs (COG), particularly a metastream cog, to assemble metastreams for a participant.

Topic Cog (Topcog)

provide a topic information to participants by classifying content as belonging to specific topics. The topic Cog (COG) may also determine which topic is the "main topic" for given content. A main factor for such a determination is expected to be how much honor a topic receives when designated to the candidate topic. A provider may be tasked with the job of allocating content to a specific topic according to each participants Web of Trust so that when the participant queries a specific topic, the most associated content is listed as expected by the participant. Creators and Cogs (COG) may match specific portions of the content with one or more specific topics. Any participant may start their own Topic Cog (COG) so it is up to each participant to use their Web of Trust to select the best fitting one, as with all Cogs (COG). The Topic Cog (COG) also has the task to cluster topics into Topic Cloud

Clusters (ref Public Content Network:Topics:Topic Cloud Clustering section) with the goal of having topics with roughly equal levels of participant activity.

Topic Map Cog

is an information service that maps available topic nodes for Zeronet (ZNET) participants. This service is for searching, querying, filtering, and discovering information nodes that may be useful to participants. This Cog (COG) may also group topics into Topic Cloud Clusters (ref Public Content Network:Topics:Topic Cloud Clustering section). Topics are linked together on the Information Graph (Iggy). Each connection has a weight which may be determined by the Topic Map Cog (COG) which evaluates multiple factors to determine the level of connection. Factors include the likelihood a person who subscribes to one topic will subscribe to a connection candidate topic, the likelihood they will value content in one topic based on valuing content in a connection candidate topic, the likelihood they will interact with a candidate topic because they also interacted with another topic, and other similar interaction factors. Also included in this consideration is the expressed content interests of participants. The likelihood of one interest being paired with a candidate topic is calculated to determine the strength of the connection between two given topics. Zeronet (ZNET) clients using this cog are expected to include metastream providers, topic search providers, and the Netportal browser. Service providers are encouraged to set up their financial incentive structure such that each class of client provides a roughly equal share of revenues so that the Topic Map (ref Public Content Network:Topics:Topic Map) is displayed with equal influence from each client class as a sort of negotiated consensus.

Topic Cloud Cluster Cog

is an information service used by Topic Map Cogs to form topic clusters. Topic clusters are a group of the most strongly related topic that collectively amount to a certain amount of views, subscriptions or a weighted combination of both. If a topic isn’t listed on the Topic Map (ref Public Content Network:Topics:Topic Map), this service is expected to create and cluster the topic. So, the service uses data mostly compiled from Traffic Cogs to divide and merge topics to maintain roughly equal amounts of traffic for each topic.

Topic Map Search Cog vs. Topic Search Cog

The Topic Map Search Cog can return a set of topics that match a specific search term. The Topic Search returns a list of content for given topic. When just the phrase "Topic Search" is used, it implies a Topic Search rather than a Topic Map Search without context indicating otherwise.

Topic Hint Cog

Topic Hint service is like topic identification service,

but also estimates the likelihood given content will be found valuable to a specific topic's audience. The topic subscriber base where the audience most highly values content is the 'main topic' for the content. (ref Public Content Network:Topics:Topic Map).

Content Title Cog

Content title service providers may help content creators to create titles for content, where the title used may depend on a certain avatar's preferences and information such as Web of Trust data for the purpose of content queries. This service is essentially paying people to formally title content according to an "expert system". Any participant can create and broadcast any content with any title at any time. So, the content search query leading to the display of specific content may vary by participant. While content may have multiple titles, it will often occur that a reason a title is changed for a participant is because it conflicts with an existing identical title matching with other content. In such a case, the competing content may be displayed instead when the user searches for the term matching the competing title, in such a way that the participant may or may not notice the competing content of the same title as it may involve the user specifically looking for the different content of the same title. A participants Content Title Cog (COG) is expected to match titles to content for each specific participant given their topic interests. If their Content Title Cog (COG) is not being paid by that participant, the title may be either the title chosen by the content creator or a "clickbait" title chosen by the Content Title Cog (COG), whereas a paid Content Title Cog (COG) will be incentivized to replace "clickbait" titles automatically for participants and better match titles to content both indirectly such as by outsourcing to a Content Title Cog (COG) and directly such as by reviewing content as part of the paid service and editing titles as they are relayed to participants for satisfying accuracy and fit according to the participant. This would be different from for example a currently used Torrent peer-to-peer system where the content distributor titles content and that title generally never changes even when titled with poor grammar and accuracy.

Broadcaster Map Cog

lists available broadcasters by topic on the Topic Network Map. This is may be considered part of Contact Discovery Service (Ddisc) (ref Information Graph:Information Graph Cogs:Database and Search Cogs:Contact Discovery Cog).

Content Compression Cog

Zeronet (ZNET) content may be compressed for reduced bandwidth usage and faster loading times. See neighboring Service Cogs and Cogs for Cogs:Data Compression Cog for details.

Title List

A list of cell or cell set references contained in Zeronet (ZNET) files.

Collaborative Portal Cog

This cog provides a default portal for common Zeronet (ZNET) services. It is important to select a trustworthy participant to set collaborative portal service because this service could be used to misdirect personal information to malicious people. This service provides portals that are a user interface to information systems including Cogs and website data when that Cog does not provide its own portal file for more specialized types of information services. Most portals are expected to be developed by open collaboration so they are not necessary to developed repeatedly by every similar service provider. Large organizations are expected to develop their own specialized portals for their information systems, but that is generally not supported by this service, though they are welcome to develop their information systems under public collaboration. If a proprietary system does develop with superior service, it is expected to be incorporated into the Collaborative Portal Cog using the Open Collaboration Protocol by development of the underlying systems which is expected to include the Group Records Exchange (GREX) protocol (ref attachment) since that system allows all other information to easily share searchable records.

Public Information Database Cog

This service provides access to an expansive range of public domain data sets and streams for any purpose which is expected to often be public records, public recordings, public posts, public forum announcements, verification, validation, and statistics. Sets of the data important for Zeronet (ZNET) purposes include internet traffic and commercial transaction data for verification and statistics. Such Zeronet (ZNET) data is expected to be formatted according to the Group Records Exchange Protocol (GREX) (ref Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol). This is useful for when an original data source releases information to the public domain without expectation of value in return, such content is expected to be considered for inclusion to the database. The Data Exchange (Datex) (ref Open Exchange:Data Exchange) is expected to be the primary way to buy and sell Public Information Database Service data. Although the information itself is public, it costs money to store and send. Price factors include bandwidth usage and the specific data sets to which access is wanted. Service can be purchased both to read from the database and add records to the database. Records will generally expire if remaining unaccessed for a period of time such as seven years, depending on the service contract. Different data sets require different amounts of file storage space. Data collators and distributors write information to any number of Public Information

Databases where they expect a demand for their content or data.

Public Information Database Cog: Data Trustworthiness and Credit

Data written will always record the participant who wrote the data to the database so that data being read can be filtered to include only trusted information sources. The data sources and due credits and citations for all records is always expected to be included for all records. The Public Information Database Cog offers no guarantees of information accuracy, only guarantees of the direct source for the records written to the database. A Public Information Database Cog is expected to all but guarantee many records to be entirely inaccurate, harmful in various indirect ways, and completely wrong because it is generally unfiltered and sometimes unanalyzed data. A database may hold a listing of participants considered insufficiently trusted to add data to the database, and may also hold records of participants considered sufficiently trusted to submit data to the database. The Public Information Database Service provider may also publicize its level of trust for each participant who submits data. The provider generally starts with one specific data set of information and expands to additional sets over time without a specific limit of set types or ranges expected. See Public Content Network:Topics:Topic Map for details regarding topics. Data set inclusion is largely expected to be directed by client base requests. Many Zeronet (ZNET) data sets including the Information Graph (Iggy) are expected to be stored using this Public Information Database Cog.

Compensated Information Database Cog

This information service is nearly identical to the Public Information Database Cog except the data sources expect financial compensation for data pulls (downloads). Compensation may be a requested donation instructions or specific fee request by the creator. The Compensated Information Database Cog is expected to process these transactions and so they decide what kind of submissions to accept. A Public Information Database Cog provider is likely to also be a Broadcast Service provider by adding that similar service. Data collection, especially original data collection, costs resources to collect. So, we encourage rewarding those who took the effort to collect data, and reward them for doing so, while dishonoring those who avoid doing so.

Web of Trust Cogs:

Data Discovery and Synchronization (Disco) Cog

(ref Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization)

Tracks the information submitted to Zeronet (ZNET) which is summarized into "metacodes" representing a hash of all available Zeronet (ZNET) information. This service

connects people who seek data with data providers. Reference Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization Service for details. Helps participants develop, recognize, and negotiate consensus agreement. This service helps form "trust paths" (ref Web of Trust: Relational Trust Expectation) with a chain of trust to given a Web of Trust record of a network participant. This trust path is used to determine what consensus has been reached by which people, and which are recommended to be accepted by the participant. This trust path is also used to determine summaries of "the internet" for a specific point of time so as to be able to have unification of record sets with trusted peers. This service uses the Data Discovery and Synchronization Cog (Disco) to form the recommended trust paths.

Crosslinking Cog

Determines consensus according to client-side rules. This is a very important cog for security because it automates the delegation of trust to some degree. For example, this cog can help determine consensus on which content is malicious and which is trustworthy.

Trust Garden Cog

Based on Web of Trust Trust Garden, helps a user select a cogset for their Zeronet (ZNET) experience. A participant selects the sort of experience wanted based on such factors as their budget and targeted uses. This service may use questions and instructions to determine the level of previous Zeronet (ZNET) experience, level of Zeronet (ZNET) technical awareness, and domain of services the participant wants to latch.

Trust Chain Analysis Cog

This service analyses a trust chain to help determine the best fitting Trust Domain for a participant. Selecting an honorable and virtuous Trust Chain Analysis Cog service is essential to system security. While trust chain analysis is expected to be done on each participant’s local devices, some processing may be outsourced to others.

Group Trust and Synchronization Cog (GTS)

Given a participant’s Web of Trust and selected trust chains, group names and contact points are verified, and Data Discovery and Synchronization (Disco) cog settings are tuned in with recommended metacodes. Whereas Data Discovery and Synchronization (Disco) service wants a maximum range of metacode offerings, a Group Trust and Synchronization service recommends specific metacodes according to specific trust domains and broad trust domains. (ref Perspective Development:Network Synchronization:Crosslinking:Trust Group)

Trust Evaluation Cog

This service is used in conjunction with a Trust Chain Analysis Cog to distribute honor points automatically for various activities by a participant and re-rank the Trust List accordingly.

Contract Performance Review Cog
This service provides suggestions, interfaces, and advice for submitting contract reviews. This is process is important for building trust, especially on the Web of Trust. Every time a contract is formed, there should be a high chance that the contracting participants will review each other's contract performance. Such performance reviews are expected to be posted to the Public Settlement Network (PSN).
Negotiations Cog
Provides automated negotiations. Perspective analysis. Value-matching, virtue matching, and ethics code comparisons. Offers compromise suggestions. Used by Web of Trust trust garden and other Zeronet (ZNET) components.
Data Negotiations Cog
Controls regarding topic searches, shopping decisions, content pulls (downloads), content pushes (uploads), and so on.
Information Systems Conflict Resolution Cog
All Zeronet (ZNET) censorship is entirely voluntary, so requests for censorship or halt of information services is done with negotiations expected to involve dispute resolution services including mediation and arbitration. See the Information Systems Governance section nearby for details.
Information Service Voluntary Governance
See Rainbow Rock:Rainbow Civics for information related to this section.
Bonded Behaviors and Service
Cogs (COG) are all expected to list all the types of bonded guarantees they offer to participants, and expected to clearly list any bonded guarantees they require of participants.
Mediation and Arbitration Service
Cogs (COG) are all expected to list all accepted mediation and arbitration networks and participants.
Civility Bond Cog
A civility bond is a secured guarantee of civil behaviors in for any and all meaning of that phrase as the guarantee is contracted. This could guarantee of avoidance from anything from the most minor infraction of name-calling to serious violations of physical violence, depending on the specific contract formed. The Civility Bond Service collects money as bond which is guaranteed accessible by a specified network of arbitrators pending release given any judgments by those arbitrators. Any cancellation of bond service by the bond poster is generally only refunded after there is no money pending in mediation or arbitration. A network of mediators is also able to lock bonds into judgment status upon initiation of any mediation. Deposits may be fully tracked and claimed as digital money. So, a deposit is made in a digital transfer. That transferred money may be

expected to remain untouched unless a judgment is made against the bond amount by an arbitrator. Systems involving high risks to deposits is at a higher risk of dishonor. To help prevent fraud, specific amounts of time for any and all mediation and arbitration activity is expected each transfer of funds is enabled. The contract is expired if the bond security is depleted by judgment against the bond poster, or by defect including lost or stolen deposits.

Creative Origin Dispute Cog

This service is for content creators who believe they are not being properly credited or compensated by Zeronet (ZNET) participants to petition for corrective actions to be taken. For example, if a donation-requested content created by a participant is mislabeled as public domain by another participant and released to a public domain database (such as by plagiarism), a mediation service accepted by the public domain database may be authorized by that public domain database to remove violating content. There may also be appeals to an arbitration service. Any rule enforcement costs not covered by civility bonds are expected to be paid for by creators except at the grace of any service provider. So, a careful and thoughtful negotiations processes is encouraged between content creators and developers, and content distributors to develop consensus on civility bonds by content pushers (uploaders). Lack of consensus on this topic may result in network fragmentation, increased hostilities, and system reputation damage.

Content Feature Dispute Cog

enables formal content tagging (ref Democratic Communication:Sigil X Protocol:Tagging Service) provided by content creators, distributors, and reviewers is expected to make claims about topics, ethics, and morals of specific content. If such claims are both falsifiable and false, those negatively affected are expected to dispute these claims through a mediation and/or arbitration service.

Creative Credit Cog

is a service which helps acknowledge creative credit to content developers.

Plagiarism Detection Cog

is a Service which scans the internet for content that is inappropriately credited.

Democratic Communication Cogs:

Data Translation Cog

Reads information in one data format and then translates to another format.

Common Service Classes: Proprietary Format, Open Format

Common Format Classes: Application File, Service File

SigilX Replacement Cog

A service that offers automated text replacement for a

wide range of purposes. See Democratic Communication:Sigil X Protocol.

Content Translation Provider Cog

A service provider that converts content to a semantically as nearly identical as possible, but more preferred language/protocol.

Text Analysis Cog

is a service that offers spell checking, grammar checking, word count, or other related text analysis services.

Dispute Resolution Cogs

These cogs are expected to be created by Dispute Resolution Organizations (DRO) to help resolve disputes automatically among participants, especially where there is good faith efforts by the participants involved. A mediation cog may direct participants to consider the evidence available on each side of the dispute. An arbitration cog may analyze the evidence and suggest what the outcome is likely to be based on the contract and available evidence. A content removal cog may analyze content to determine if a word is on a list of words agreed to be censorable by the content host.

Private Message Filtering Cog

A client-side application which resorts private messages (ref Democratic Communication:General Concepts:Private Messaging) in their metastream according to prioritization rules which may analyze the content of the message for specific topics or keywords. Messages may be sorted according to multiple weighted factors including the level of trust for the sender, and the urgency level expected when information is sent by a specific sender. For commercial organizations, advanced filters may track the amount of pending financial transactions being done or in process with specific participants, and prioritize on those terms as well.

Contact Discovery Cog (Cdisc)

A contact directory matches names or other data to contact points of Zeronet (ZNET) participants and their encryption instructions. Each participant is encouraged to list their contact point set, otherwise they may be unable to be contacted by participants in their contact list. A contact point will only be an IP address for their most trusted peers (generally immediate family only). For most peers, a contact point will be a selected rendezvous point as a rendezvous server. Each avatar is encouraged to use three rendezvous servers that are rotated every eleven days. Contact points are generally private until listed.

Because people may choose an avatar name that is already being used, differentiating factors determine which avatar name best matches with which contact point according to a participants preferences. The participant may manually select which avatar is selected from multiple options. Furthermore, the participant may send contact inquiry messages to several of the avatars to

help discover which one is correct. An avatar profile picture is one example of a factor that can help people determine the difference of otherwise identical avatar identities.

DB Service Distribution Cog

This service is used by a database to determine the optimal data distribution given factors including available BYTE service budget, likelihood of a given record being accessed over time, and minimum performance settings by geographic region. Each database query may determine whether multiple paths are available for the specific query, and if not whether multiple paths should be made available. So, statistical analysis is performed on data access to determine whether a record set or file should be distributed over additional nodes for faster access times according to the thresholds set by the client. Distribution may be architecture-dependent, so this distribution service may be specialized. Automation of this service may be limited.

Grexcog

This service communicates between participants to send and receive Group Records Exchange (Grex) data. All Zeronet (ZNET) participants are expected to list what data they have available or otherwise collect. They match each Grex classified table (see associated section) of interest with available (or collected) table data, summarized as a metacode. This service may append data to any Zeronet (ZNET) database formatted according to Group Records Exchange Protocol (Grex) such as an Information Graph (Iggy) database or Public Content Network (PCN) database. Client-side activity includes development of systems to automatically delete data after it is no longer wanted by the participant for factors that include being unaccessed for a sufficiently long period of time.

Private Information Database Cog

This service is used to store records formatted according to participant's formatting guidelines, or according to Group Records Exchange Protocol (Grex) (ref Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol) when possible. The Private Information Database Cog is used by Zeronet (ZNET) Private Messaging (ref Democratic Communication:General Concepts:Private Messaging) to hold private messages until the participant is ready to delete them, which is encouraged to be after being pulled (downloaded). Participants are expected to list their Private Information Database Cog contact information with their Contact Discovery Cog (CDisc) (ref section nearby) record.

Database Architecture Cog

This information organization service develops recordset organization, formatting, and indexing. This service has varying levels of automation. Based on expected or

historical database search patterns, a search indexing system is developed for a data set and data structure may be optimized. Automation of this service may be limited.

Focus Point Cog

The Focus Point (FP) system serves as a method of registering contacts with a Contact Directory which is expected to appear for people who pay the Contact Discovery Service (Cdisc) to list all available contacts. Contact Discovery Services (Cdisc) are expected to be aware of Focus Points (FP) contributions. The directory service is then expected to list each contact when the minimum listing criteria is met. More detail available in Focus Points (FP) section. This is a differentiating factor when determining best match for avatar name to contact point. While listings may be by name, a direct hash-based avatar identifier is preferred for contact matching.

Web of Trust Honor Points (HP) are used to help differentiate contacts by the likelihood of the person matching the person they are looking for. The earliest registered avatar name is expected to be granted honor points for a given name. So, both honor points and focus points may be joint weighted factors for contact information discovery.

Democratic Communication Cogs: Security Cogs:

Routing Cog

This service is for traffic routing. Creates rendezvous point servers, VPN routers, LogLo routing, TOR service, proxy service points.

Security Reporting Cog

A service that categorizes participants when believed to be participating in malicious activity such as inadvertent participation in a DoS (Denial of Service) attack.

Security Cog

An anti-virus application that includes Zeronet (ZNET) components and also may include their entire computing environment. Regularly randomize MAC addresses.

Social Security Tester Cog

Emulates automated social engineering attacks on a participant to ensure they behave in secure ways. Prompts with advice if the participant engages in risky behaviors. This is expected to be a paid service as to offer more optimal incentives.

Whitehat Security Tester Cog

A white hat hacker group attempt to hack into your system using automated methods. The group will offer advice on securing your system if a hack is successful. This is expected to be a paid service as to offer more optimal incentives.

Encryption Cog

Replaces unencrypted text with encrypted text before being pushed (uploaded). Replaces encrypted text with

plain text as it is pulled (downloaded).

Device Trackdown Cog

This feature enables participants to recover a Zeronet (ZNET) device better if someone takes it without permission. Zeronet (ZNET) devices are expected to have settings for trackdown capability for the ability to recover a lost or stolen device. Tracking information from usage of the device occurs after a participant activates this trackdown feature after losing the device. That could occur simply by not entering in a security password for an amount of time such as 24 hours. Or, a remote trackdown command may be sent by any internet-connected computer with the appropriate software. Then, the device sends tracking data as it becomes available to the alternate device. A lost trackdown password will lead to your computer hardware being useless, so the trackdown password should be carefully hidden in at least two different locations. Some devices have a feature to be entirely unusable without a password, but these devices can be entirely reset if stolen in most cases and reused as if new. That is why the trackdown feature may be better for many participants.

Security Cogs: end

Information Graph Cogs:

Information Graph Database and Search Cogs

Information Graph Cogs include database cogs and search cogs.

Topic Database

See Information Graph (Iggy) Database Cogs nearby. Content creators and distributors (including Metastream Providers) are expected to associate their content to the Topic Map (ref Public Content Network:Topics:Topic Map).

Parameterized Search Cog

This data service pulls (downloads) many data sets from a set of supported databases and provides parameterized searches to those data sets such as the Public Settlement (PSN) and Open Exchange (OX) messages for specific ranged criteria. Expected usages include shopping, map searching, and public database searches.

Compensated Information Database Search Cog

This cog is like the Parameterized Search Cog (ref nearby section) but this service cooperates with a Compensated Information Database Cog to compensate information sources.

Topic Search Cog (Topcog)

Topic Search Cog (Topcog) is a topic channel search service for Zeronet (ZNET). See Democratic Communication:Zeronet Protocol:Topic Search Protocol for some details on topic searching. This service lists available content by topic to Zeronet (ZNET) participants related to a specific search topic. It is

used for searching, querying, filtering, and discovering content listed with topic nodes that may be valued by participants. See the Topic Search attachment for one possible solution regarding this process. Zeronet (ZNET) may support predefined Unordered Search Queries (PREQUE) as described in the attachment. However, other search systems are encouraged to form as more complete alternatives with advanced search options. This provider may also group topics into Topic Cloud

Search Result Filter and Order Cog

This search component is designed to reorder a search result set according a participants Web of Trust and append Competing Perspective Consideration (ref Netportal:Competing Perspective Consideration) results for controversial issues. Because millions of people can very easily add content to any search such that there may be a large number of search results for any one search, so the search results are be sorted. So, rather than being sorted by the number of backlinks or according to the corporate political bias of tech oligopoly employees, the links are sorted according to a participants own Web of Trust ranking. This service is likely to be done client-side for privacy purposes.

Search Query Auto-Complete Cog

After beginning to type a search query, an auto-complete service attempts to predict what the remaining search string will be. Predictions are expected to be made based on data shared on the Data Exchange (Datex) (ref Open Exchange:Data Exchange).

Similarity Search Cog

Supports data set searches without an exact match.

Image Search Cog

The client provides an image. The server identifies the most similar images and their internet location(s).

Audio Search Cog

The client provides an audio clip. The server identifies the most similar audio files and their internet location(s).

Video Search Cog

The client provides a video clip. The server identifies the most similar videos and their internet location(s).

Focus Query Cog

Network Query Cogs are paid by individuals wishing to have query results according to the Focus Point (FP) system to assign points based on the rules defined by the Focus Portal (FP) system, or by a generalized Search Query Cog who wants to receive a list of focus points by search node as a factor in their own search rank. These providers are expected to provide proof of work showing that they have not biased their results based on advertising revenues. So, their ranking is based on openly shared formulas rather than proprietary, bias by censorship and propaganda search results.

Netportal Cogs:

Content Feedback Cog

Content award information, evaluations, reviews, ratings, and comments are sent to participants by content review services related to any content being "pulled". Pulling participants are paid to submit their reviews by other participants who wish the data (as content or records) to be evaluated. Zeronet (ZNET) participants may pay a Content Feedback Cog to enable access the reviews for the purpose of predicting which content a participant will find most valuable. A service provider may pay another service provider for the same purpose. So for example, a Content Title Cog may use a content review service as a factor in establishing their title matching. Review scores are expected to be adjusted by a harshness factor of reviewers in circumstance where different reviewers seem to be more harsh than others. So, if one reviewer only seems to rate at the maximum possible rating, while the other always rates the minimum possible rating, both of them are encouraged to be ignored entirely. Only when multiple reviewers can rate the same content with a range of different ratings does a reviewer's ratings become meaningful. With enough ratings by a reviewer, their rating can be adjusted automatically according to the relative harshness of their reviews, though this adjustment is expected to be made clear to the participants involved.

Public Data Reporting Cog

This service organizes, analyzes, and summarizes public data and statistics regarding any topic for redistribution, so that participants can learn statistical information about each other or specific topics without necessarily revealing personal details. Data Negotiation Service (ref Web of Trust:Data Negotiation Service) reports summary information to the public domain according to the Group Records Exchange Protocol (GREX) format (Democratic Communication:Plain Text Protocol:Group Records Exchange Protocol). As part of a Data Negotiation Service contract, personal data provided to any organization is encouraged to be relayed through their Data Negotiation Service to Public Data Reporting Service providers for helping participants learn about each other but with some privacy. Public Data Reporting Service provide data to broadcasters, who then list available data on the Data Exchange (Datex) (Ref Open Exchange:Data Exchange). Public Information Database providers are encouraged and pressured to (by selection as a partner by participants who favor this behavior) to contribute a specific portion of their revenues to the appropriate Public Data Reporting Cogs when using them to filter their data. They are also expected to cite the Public Data Reporting services used as their sources.

Public Data Reporting Traffic Cog

This is a type of Public Data Reporting Service specializing in data traffic. A traffic report service provider is expected to prioritize independent objectivity in reporting claims of traffic from a broad range of traffic push (upload) and traffic pull (download) sources. The primary source for accurate information is firstly donation-only (and donations-rejected) metastream providers (Public Content Network:Metastream), secondly content pullers, and lastly all other participants who have the ability to directly gain that information including advertisers and content distributors. The sources with the closest knowledge of this information in order of most to least accuracy incentive are donation-only metastream providers, donating content pullers, people who advertise their offerings, metastream providers who advertise, advertising cogs, and content distributors. After pushing, pulling, or relaying Public Content Network (PCN) content, a participant is expected to report that activity to trusted Traffic Report Cogs, preferably though a Data Negotiation Service (ref Web of Trust:Data Negotiation Service), both of which are expected to protect access to personal identity information. As mentioned in the Data Negotiation Service explanation, after a content push source receives value for content either directly or indirectly when an advertiser gets a sale, that activity is also expected to be reported to Traffic Report Cogs by all participants involved including the buyer, seller, and all middlemen and advertisers involved. Any Data Negotiation Service is expected to relay such data. So, an accurate traffic estimate is expected by having all participants report either privately or publicly, and check with multiple Traffic Report Cogs which are paid to post this information by incentivized participants, less any personal details, to the public domain. Using the Public Data Traffic Reporting Cog is encouraged to be done through a Data Negotiation Service to avoid large organizations being able to monopolize personal data.

Advertising Cog

A service which connects marketing advertiser push content to creators, content distributors (including metastream providers) and to pulling (downloading) evaluator participants and any Data Negotiation Service (ref Web of Trust:Data Negotiation Service) they may be part of.

Fusion Cog

Service which bonds or bridges together multiple similar services into one service. Zeronet (ZNET) Portals are easier to bond together because most of the portals have no hidden back-end like websites.

Message Fusion Cog

Service which bonds together messaging services.

Legacy Direct Messaging
Translates services such as XMPP, ICQ, and AIM to Zeronet (ZNET) service. Translates services like Element.io and Signal to Zeronet (ZNET) service.
Legacy Group Messaging Fusion Cog
Service which bonds together internet social media services such as Twitter and translates them to Zeronet (Znet) service.
Legacy Video Publication Cog
Service which bonds together classical internet media publication

Service Cogs and Cogs for Cogs:
Uptime Reporting
Uptime of cogs is expected to be automatically reviewed and reported to the public using such systems as Contract Performance Review Cog (ref neighboring Web of Trust Cogs:Contract Performance Review Cog nearby). Such reports from metastream service providers (ref Metastream in the Public Content Network section) and other cogs can also be automatically cross-referenced against other public resource usage claims of IT resource cogs to help validate usage claims by resource cogs. Content distributors pay the most for these services with expectation that participants will provide more than the storage service costs by donations, awards, rewards, purchases, and any other revenue streams.
Common Cogs:
File Storage Cog (BYTE)
is a paid file storage service. Service-specific contract provisions are to include provisions for upload bandwidth and download bandwidth. IOPS, latency, and other specifications may also be applicable depending on the usage.
SCRIPT
is a paid scripting service including for generation of interactive Zeronet (ZNET) and website content. Scripts are expected to frequently connect with remote servers for various other Cog services. This service is expected to be included as part of COMP service. Possible scripting language support include ECMA/Javascript, Python, and Javascript.
COMP
is a remote computing package as a Computing Domain (ref Democratic Communications:Zeronet Protocol:Computing Distribution:Computing Domain) expected to include at least CPU, RAM, BAND, BYTE, and SCRIPT service. Service-specific contract provisions are expected to include performance expectations for such services.
CALC Cog
Service-specific contract provisions are expected to include specific function executions per second by function classification given a specific range of function parameters.

DB Cog
is a paid records database with search capabilities. Service-specific contract provisions are expected to include database server application, and a set of associated services including BYTE, BAND, and DB scripting.

CPU Cog
Service-specific contract provisions are expected to include CPU model specifications, core usage count, percentage of cores, instruction set, burst capacity. CPU is used in the form of Python, ECMA, or other scripts that use system resources as paid for. The scripting service is expected to be able to monitor what these Python scripts are doing so that any processes deemed harmful may be halted.

RAM Cog
Service-specific contract provisions are expected to include RAM model specifications, latencies, bandwidth, burst capacity, byte size. This is expected to be packaged with CPU, GPU, or other Cogs.

BAND Cog
Service-specific contract provisions are expected to include maximum latency by geographic location and burst capacity.

HTTP Fetch Cog
Given an HTTP URL, return the data provided from that URL.

Extended Cogs:

VM Cog
Virtual machine service is a operating system level access computing domain including a number of other IT Cogs integrated to one computing system.
Service-specific contract provisions are expected to include operating system and the set of associated Cogs like CPU and RAM.

GPU Cog
Service-specific contract provisions are expected to include GPU model specifications and percent utilization.

FPGA Cog
Service-specific contract provisions are expected to include FPGA model specifications and instruction set.

Screenscraper Cog
Given screen, return all text from the screen. Given video, return text and identified objects from the screen.

HTML Disassembly Cog
Given an HTML page, return the page structure.

Service Distribution Cog
This service is used by other services to determine if enough resources such as CPU or BYTE are available for the needs of a service. If not, the service is modified according to the clients needs such as adding more service resources locations, throttling resources to serve a limited number of service requests, or changing the price of the service. This service may apply to all

other services, as can be seen with the DB Service Distribution Cog section nearby.

Bandwidth and Connectivity Cogs:

Network Connectivity Cog

Manages connections according to the Zeronet (ZNET) protocol including connection establishment, keep-alive data, time-out determination and optimization, and automated encryption. Maintains internet connection according to participant preferences. Helps ensures security protocols are followed regarding connections. For example, it may be ensured when a participant sets up VPN that the VPN is always used when appropriate to do so, and may furthermore attempt to connect to an available VPN service. Expected to maintain a history of the available connections used to help determine which connection to use for the best performance. Connection data more than five minutes old is encrypted by default.

Network Connection Bundling Cog

When a participant has more than one method of gaining bandwidth, multiple paths may be used simultaneously using this cog.

Connection Diagnostics Cog

A service that helps maintain a participant's internet connection and Zeronet (ZNET) connections. This service is also expected to have a generally full listing of Search Cogs because a Search Cog (COG) is expected to be able to list any and all Cogs (COG) a participant may want to discover and use. A directory contact table for common simple data services including time reporting is provided. The service provider is expected to have a generally unchanging service location and static IP.

Network Topology Development Cog

Develop a network for distributed computing services. Allocate network nodes to specific tasks. Determine optimal paths given available resources of each node. Add or remove a node from the set of available nodes.

Website Keepalive Cog

A convenience feature offered for website connections that keeps connections to organizations with time-outs active. If your device is in a secure location with little to no risk of problems by being logged in unattended, making websites with auto-logout a pointless inconvenience. This cog may need a database of different activity requirements needed for different websites. Without specific instructions, a simple refresh command may be issued at regular intervals of four minutes if no other activity is detected.

Website Login Cog

A cog which holds an encrypted list of usernames and passwords for a participant to access traditional websites. The cog automatically detects when a username and password is being submitted, then prompts the user to ensure the username/password combination is being saved appropriately. The cog then automatically enters these in the appropriate fields the next time the user

expects to log in. A checkbox indicates whether to display usernames and/or passwords. This is expected to be a client-side cog, though an encrypted password file may be stored remotely.

Pull Cog

Manages and processes inbound data transfers including cache data handling, intermittent connection handling, traffic bottleneck handling, automated compression, processes inbound data filters (such as via whitelist/blacklist) and limits, and pulled content database.

Push Cog

Manages and processes outbound data transfers including cache data handling, intermittent connection handling, traffic bottleneck handling, automated compression, processes outbound filters (such as via whitelist/blacklist) and limits, and push content database.

Bandwidth Distribution Cog

Enables processes to use specific amounts of bandwidth.

Whitelist Cog

Manages list of trusted peers and participants.

Blacklist Cog

Manages list of untrusted peers and participants.

Greylist Cog

Manages proxy connection distribution to limit usage of restricted services such as traditional website database queries. For example, proxy access to Reddit.com may be limited to four participants per year and two website usernames for each participant. Services running BAND Cog and especially Connection Proxy Relay Cog also run this cog by default to protect residential IPs from being blacklisted or inconvenienced. Access may be charged on a per-website basis to greylist destinations, or a "popular destinations" package that includes access to many popular websites. Currently these limits can be seen by attempting to access many popular websites by Tor, which either is slowed or stopped entirely by servers who wish to restrict service on a per-IP basis and often also a per-day basis. Typically service is also limited on a per-username basis for proxy access to traditional websites. Per-username restrictions take additional steps to implement such as keyword scanning. Zeronet (ZNET) portals are discouraged from greylist involvement because Zeronet (ZNET) portals and data streams are generally directly paid for and so no amount of traffic from one IP is expected to be considered problematic. All services are encouraged to be structured to be able to scale up for large global demands for any purpose a client wishes, even on a short-term basis.

Connection Bridge Relay Cog

A connection service provider connects clients to others through a connection relay service. Because a participant’s physical connection to the internet may

constantly change, this service manages those changes of location or contact points to continue network connections over time. Furthermore, this service used both for increased connectivity and for privacy since an ISP (internet service provider) will not have access to the final destination points and instead only see that a connection is formed to the connection relay device. The connection server is also expected to avoid storing records of specific connections to dramatically improve privacy. Traffic volume records by each client may be stored. Unless a more specific type of relay is used, this relay simply forwards all data to generally any IP of the client's choice without any processing involved except for decryption since all connections are expected to be encrypted. The service may be limited to a whitelist or blacklist of the service's choice, though such a listing is expected to be provided in full to each client upon request.

Connection Directory Relay Cog

A client informs the Connection Relay Cog of their connection availability to any or all other locations. The client uses specific Connection Bridge Relay Cogs as their preferred bridge connections. If the Connection Relay Cog is contacted by someone wishing to contact the client, all their data may be relayed to that client. The client may offer a whitelist and blacklist to the Connection Directory Relay Cog to filter out unwanted traffic. For Tor Service, a similar directory service is named "introductory point" service. As a Zeronet (ZNET) service, this a "directory relay", though when specifically offering Tor service is a "introduction point relay".

Connection Proxy Relay Cog

This service offers a domain of proxy data requests such as HTTP fetch on behalf of a client. Such proxy requests generally establish a final relay point before the client's contact destination point. In Tor this service establishes the Connection Relay Cog as an "exit node". A Proxy Relay Cog may use a Greylist Cog to help maintain good peer relations.

Connection Privacy Cog

This service offers complete Zeronet (ZNET) connection services including as VPN, Tor, Loglo (ref Democratic Communication:Secrets Protocol:Security in Numbers:Local-Global Wheel) or any other connection privatization service.

Data Compression Cog

Pullers (downloaders) of specific data types may have advantage for their data being compressed according to a function designed by an algorithm that compresses data based on the type of data being downloaded. That participant may be either another service provider or the endpoint loading participant. The Compression Cog may have compressed versions for popular content so they

do not have to redownload the content before restreaming it depending on their usage statistics. Content providers are encouraged to contemplate several versions of their content with different compression levels.

Remote Data Compression Cog

If a content provider does not offer compression service, requested content may be streamed to the compression service, who then restreams content in a compressed form to the Zeronet (ZNET) participant.

Information System Resource Cogs:

Randomization Cog

Given optional random seed and optional random number generation algorithm, provide psudo-random numbers as requested.

Game Scrambler Cog

Collective randomization is a process by which a group of people can rely on bits being proven to be randomized, which is useful for processes which are meant to be provably (psudo)random including multiplayer games. First, all participants including the host provide a retrocast message with a predetermined number of input bits used for randomization provided by predetermined participant(s). The order of the participants to provide their bits is also predetermined. Each participant provides a specific number of input bits which may then be hashed according to a predetermined hashing function. The hash may involve all input bits provided. The data is randomized according to a collection of the collectively provided bits, as provided by each participant involved. Data receipt is provided with timestamp. The number of output bits provided is then provided as randomized, and the same number of bits outputted as the randomized bits to each participant as requested. By using a sufficient number of randomization bits by each participant, any one participant generating a predetermined outcome is seemingly impossible. For games in which the host is fully trusted, all the bits can be provided before the game begins. Otherwise, the bits can be provided at regular intervals such as each turn in a turn-based game. if someone’s connection is temporarily lost, that can be handled in various ways depending on the importance assigned to the game, but the most common way (without large sums of money involved) would be expected to be a forfeit of the right to randomize the part of the game when their connection was lost. All input and output data is typically expected to be timestamped and rendered public.

Data Scraping Cog

Reads information from one source and dumps it’s information in a format wanted by the service user.

Dynamic Content Cog

is an API for the SCRIPT resource designed to connect specific interactive content with one or more service providers.

Generalized Prediction Cog
Given a set of data, predict the next item in the set.
Code Security Audit Cog
Performs automated code analysis helping to identify insecure computer programming code.

Public Settlement Network Cogs:
Claim Evaluation Cog Determines if a claim of a specific claim class as defined by a Democratic Communication (DCOM) protocol (or any other claim evaluation process) consensus is valid. This applies to any claim that can be verified according to axiomatic rules, or automation will be unlikely.
Claim Publication Cog: Creates a digital claim using client-side methods.
Retrocast Claim Cog Creates retrocast messages using client-side methods.
Broadcast Cog Distributes claims using a broadcaster agreement.
Claim Confirmation Cog Determines how confident the participant can be that a claim is confirmed based mostly on their own definitions, though default settings will be in place if not changed.

Digital Money Cogs:
Transaction Validation Cog
This service validates any transaction claim according to a protocol referenced by the client. See Public Settlement Network:Claim and Transaction Validation for an example of such a protocol.
Token Pack Cog
Token Pack Service can be a public offering by any always-on internet-connected Zeronet (ZNET) device. Zeronet (ZNET) devices are expected to run this service by default because they generate tokens that are presented to them to use their computing resources as specified by their contracts. A psudo-random process generates a large list of strings of randomized letters and numbers. Each item in this list functions as a password to receive a specific offering. Each item in this list is expected to be paid for and then redeemed for a set price. For small transactions, a Token Pack Cog can generate many tokens that can then be redeemed for a small amount of digital money. Tokens are typically expected to be transferred one time only after being issued. The recipient of tokens is expected to redeem them within a specific time period such as 18 months. Participants should be periodically notified of this situation upon token purchases. So, if for example a digital money is not efficient to trade below an amount of $USD 1, then a Token Cog provider can sell 100,000 tokens for USD$ 1.03 that can be redeemed for USD$ 1.00 per 100,000 tokens if redeemed by a set time period such as 18 months. The difference USD$ 0.03 is the service charge of the Token Pack Service provider.

So, tokens allow people to pay for bandwidth costs of a single video. For example, one 100MB video pull (download) may cost 100 tokens to pull (download), which would be roughly USD$ 0.001. The file storage service (ref Service Cogs and Cogs for Cogs:File Storage Cog) charges a set number of tokens for a given pull (download). The pulling (downloading) participant sends their tokens to the File Storage Service provider by telling the token pack Cog provider to dedicate the tokens (which they previously purchased) to that specific push service. Alternatively, the token passwords can be relayed to the File Storage Service provider who then relays those token passwords to the token pack service with instructions of who they want the recipient to be. So, the file service provider verifies with the token service that the tokens have been relayed to the appropriate name or account.

Direct Service Tokens  A token pack cog provider may be the same or different person as the associated service provider for those tokens. If two different people, they determine the token set in advance, sharing the token passwords together. So, direct service tokens are purchased to be used with a specific service. The token service is in accounting for these small funds over time and then converting to larger money unit sizes chunks when they get to an appropriate size that enables small transaction fees to receive the service funds. If the service and provider are the same person, the funds are received as the larger size up front but the service is then in debt to deliver the underlying service over the following 18 months or other number as agreed. If a trustworthy 3rd party service is available, that is considered a more suggested method because the accounting system assures services are only paid for upon delivery and tokens are expected to be refunded if the service provider goes out of business. If the tokens are claimed by the provider without any service being delivered, the bank is not to be involved in any resolutions because that would instead be considered to be a commodity service token rather than a direct service token.

Commodity Service Tokens  Nonexpiring tokens can be purchased via a banking service that enable multiple service providers to be used. Direct tokens are then purchased by the bank upon usage of the service as appropriate for the situation. Banks must publish their proven reserves, which would be expected to be above a number set by a consumers purchasing union. These tokens are expected to have an arbitrator and mediator. The mediator’s primary duty is to release the funds at the end of the service period and associated resolution time allowing a complaint to be filed. The arbitrator’s primary duty is to determine a final sending of funds to the most appropriate

people. Each mediation or arbitration event is expected to itself cost money to both parties in equal amounts, which makes disputes over sufficiently small token amounts infeasible. So, mediation and arbitration are only expected for larger value service tokens and may be unavailable for smaller denomination tokens or token packs.

IT Resource Token Cog

IT Resource Token Packs are for Zeronet (ZNET) Service Cogs. One token can also be specified to have a specific number of uses before being depleted entirely. Tokens may also be time-limited according to the specifications of the Token Pack buyer and as agreed by the IT Resource Token Cog (COG).

IT Token Distribution Cog

This automated service generates and manages IT Resource Token Packs for an IT Resource Token COG if needed. So, IT Resource Token Cog (COG) is generally always used by any Service Cog, however, a Service Cog which does not want to internally manage tokens then outsources this service using the IT Token Distribution Cog. Participants may trust the distribution organization more than a more unknown service provider, so this service cog acts may reduce token related contract disputes. This service is similar to the Beenz coupon system. It may be preferable to have a third party token distributor because the tokens may be used for many different purposes and traded on exchanges more easily.

Token Pack Service

Token Packs are methods of payment where the amount transacted is less than what would be efficient for a digital money such as transactions of less than USD$ 0.03. Token Packs are designed as methods of paying for Zeronet (ZNET) automated services where each token is redeemed for (typically) one unit of service. High transaction volumes are easily supported with this system. Most Service Cogs (COG) are expected to operate by token service. When the service provider collects a specific minimum number of tokens, the tokens are redeemed for a medium of exchange designed for higher values.

Token Pack Service

Tokens are generated to be sold in sets that are later redeemed for an offering or money.

Token Pack Cog

See Service Cog: Digital Money Cogs:Token Pack Cog.

IT Resource Token Service

IT Resource Token Packs are sets of randomly generated passwords which allow assignment of the token to a specific client or service provider. These token packs are paid for, typically to pay for a specific offering, but also purchasable without any specific offering in mind, and then used to access Zeronet (ZNET) services. An expected primary purpose of token packs is to reduce unwanted messages

including some forms of Denial of Service (DoS) data, but they can be used for many reasons. Tokens can be used for distributing content that is pay-per-download. For example, when someone buys a proprietary software, they might also be given three download tokens that can be used within on year of receipt to download their purchase. Or, they could be given one token that is usable three times. Token packs are expected to replace Captcha service of current internet sites to save substantial amounts of time. The price for each token will be different for each purpose. Expected usage includes Captcha, priority download access, and service vouchers. Service providers may trust other parties for this service, though as with any service they may directly run their own Token Pack Cog (COG). Tokens may be intended for various number of uses. They may be single use, usable a set number of times, limited unpredictably, and unlimited usage, as negotiated with the token pack requester, issuer, and users.

IT Resource Token COG

An automated IT Resource Token Service. See Service Cog:Digital Money Cogs:IT Resource Token Cog.

IT Token Distribution Service

IT Token Distribution service manages token packs for content distributors. The most frequent expected usage of the Public Content Network (PCN) is distribution in exchange for donations or advertising acceptance. However, hostile entities may attempt to purposely drain such resources by using up a distributor’s bandwidth with the intention to waste it which is considered a form of Denial of Service (DoS) attack. When an IT Cog contract is formed, the service buyer may request service tokens of varying priority levels that act as passwords for the service, and may be able to request more automatically on demand from that service provider. When a problematic resource drain is automatically detected, the priority token system activates until the drain attempts halt.

Open Exchange Cogs:

Budgeting Cog

A budgeting service to help install or use a Zeronet (ZNET) service package. Personal consultations are also expected to be available.

Purchasing Cog

A purchasing service to help with shopping decisions and transactions. Full transparency including relationship biases is expected with recommendations based extensively on measurable offering metrics and various types of offering reviews.

Purchasing Statistics Cog

Shows important shopping data statistics regarding specific offerings such as what offering viewers

actually purchased after viewing an offering and what similar items are available.

Listing Cog
: A market listing cog to publish offerings. This is currently comparable to the Ebay automated listing software on the market.

Contracting Cog
: A contract development cog helping people form, edit, and analyze contracts according to a given contract protocol and system of governance. Also helps troubleshoot contracts when something goes wrong. May link with Web of Trust Cogs for such purposes. Helps form and communicate expectations and suggestions for evaluation (including reviews and ratings) agreement participation.

Offering Performance Cog
: Links with a Web of Trust Cog to integrate offering reviews and contract performance reviews of Open Exchange participants into open exchange listings.

PUBLIC SETTLEMENT NETWORK (PSN):

Settlement Claims
: (Ref Zeronet:Summary section for summary of this system.)

Settlement
: The facilitation of transactions, development of consensus, formal evaluation of pledges, formal conflict resolution. Any situation which could end like "So, its settled then." followed by "Yes, its settled.".

Public Settlement Announcement (PSA)
: is a Public Post regarding a settlement topic. See Democratic Communication:General Concepts:Public Messaging.

Retrocast Message
: is a message designed by a creator who wants to prove they published a specific message, but without it being understandable until after it is acknowledged as being published in to the satisfaction of others. Message timing information may also be used as evidence for the source of the message. The message may be "sealed" with a "seal code" and "unsealed" when the full message is sent. See Democratic Communication:Retrocast Messaging for details.

Original Creativity Claim (Ocla)
: A Homestead Claim on being the first person to create information, a design, a process, or other intangible creation.

Public Settlement Network (PSN) Contracts
: offer methods of forming formal agreements. Participants are should select contract protocol(s) using a Public Settlement Network (PSN) protocol selection process.

Transfer of Property Claim
: Person claims to transfer their property right to

another person. Expected to include a reference to the trusted claim broadcaster.

Property Abandonment Claim
If reaffirmation of a property claim is past due, the property claimed might be considered abandoned.

Homesteading Principle
The homesteading principle is where a person is granted control over something because that person was the first one to exercise control over it. This principle is the basis of many property claims, especially land claims. An initial investment of energy into the item may be expected for honor of such claims.

Homestead Claim
is a claim declared in accordance with the homestead principle. For Zeronet (ZNET) the claim is expected to be automated according to mathematic or axiomatic rules, especially property for claims. Broadcasters may also be evaluators and conduct a review according to the given claim rules as to the nature and accuracy of the claim. Property claims may be recorded as an Information Graph (IGGY) "has a" connection between a participant identifier (as owner) and the property claim document for the Public Settlement Network (PSN). Generally the homestead claim will be a text document with public references. Public Settlement Network (PSN) Claim broadcasters are expected to list which claim categories they support upon request. After a certain claim is first received by a broadcaster, it is assigned a chronologically sequential number and marked as original if no earlier identical or excessively similar claims (as defined by their automated metrics) have been submitted, while any further contradictory announcements are marked as disputed by evaluators. The conflicts may only be resolved by further claims by the parties involved in the conflict. The time the claim was authored is irrelevant to the settlement, while the time the announcement is received by each broadcaster is relevant in terms of which announcements will be marked honorable and which ones would be ignored.

Public Settlement Network (PSN): Broadcasting:

Wide Broadcast Incentive
Property claims are expected to be advertised before being honored. This rule is an incentive that encourages claim beneficiaries to broadcast their claim broadly in a way that prevents conflicting claims. This incentive is expected to be applied with homestead claims. This incentive enables decentralization of account ledger authority.

Public Forum Announcement
is plain text format information for release to the public regarding any topic. Each announcement is assigned a unique identifier and may be distributed using a Public Post (ref Democratic Communication:Public Messaging:Public Post).

Public Announcement

The Public Settlement Network (PSN) focuses on public interaction for settlements. So, Public Posts are expected to be used (ref Democratic Communication:Public Messaging:Public Post) for the Public Settlement Network (PSN) claim settlement.

Public Announcement Category

Public Settlement Network (PSN) categories (topics) of announcement as listed in the Information Graph (Iggy). Announcements could regard topics such as event invitations, social contracts, commercial contracts, property transfer, trade offer availability, performance reviews, voting, formal news, press releases, warranties, insurance or assurance announcements, or others. So, of course a public announcement may be related to more than just settlements. See Democratic Communication:General Concepts:Public Messaging for public announcement topics with a Group Records Exchange (GREX) (ref attachment) metaclass.

Broadcast Service

(As copied from Public Content Network:Content Distribution:Broadcast Service:) A service to ensure plain text messages are available for pull (download) according to contracted terms to a broad range of participants. Other Database Cog can provide Broadcast Service by adding these service features. Also see Service Cog:Public Settlement Network Cogs:Broadcast Cog.

Trusted Broadcast Source

A broadcast source trusted by a participant to have an up-to-date record of Public Settlement Announcements (PSA), which may include dates and summary information. These records should be organized in a way where specific records are easy to find. Record blocks for fixed time intervals are expected to be available. Broadcasters may be open to various audits and reviews on a continuing basis by both dedicated evaluators and the general public to help determine trustworthiness.

Syndicate List

Broadcaster affiliates of a broadcast source which shall receive and rebroadcast announcements from a broadcaster. The more an affiliate is valued as trusted, the more an announcer may expect a source to be successful in broadcasting their announcement. So, a broadcast source affiliate with numerous trusted affiliates is a more valuable source in general. If the sources are mutually syndicated, that would be better.

Broadcast Syndication Agreement

Broadcasters may form agreements with other broadcasters to broadcast each other’s content. Because different participants trust different broadcasters, it may be beneficial to have an alliance between broadcasters with different target audiences.

Broadcaster Syndication Negotiation

The Open Exchange (OX) is used to facilitate a syndication contract. The contract is a publicly

viewable agreement expected to be reviewed by both professional evaluators and the general public.

Broadcast Announcement Agreement

Trusted broadcast source may pay or be paid for broadcasting messages. Any party including either sender or receiver may pay or be paid depending on the contract. The amount of time the announcement is available is expected to be limited, and upon the ending time, an extension is expected for as long as the announcement is valued such as for property claims. Public claims are expected to be done using the Open Exchange (OX) system. A broadcast announcement agreement is expected to involve the Public Settlement Network (PSN).

Accepted Broadcaster List

Zeronet (ZNET) evaluators delegate specific trusted broadcast sources to distribute their public claims broadly. So, they maintain a list of accepted broadcast sources associated with their public identity. The time the list was created is stated in the list. For property transfers, the parties should maintain the list on an ongoing basis in association with their public identity.

Announcement Receipt

Trusted broadcast source dates and numbers the record according to the order it was received, creating a hash with the message.

Claimchain Transactions:

Accounting Ledger

A ledger is a list of who owns what.

Claimchain Transaction Summary

A claimchain ledger is an ordered list of who owned what and in what order, so that you can notice when property is transferred from one person to another. The passing from on person to another can be seen as a sequential link in a chain. A blockchain ledger groups these transactions into ranges of time.

Claimchain Transaction Security

Claimchain may be secured with a system of duties to participants carefully incentivized to arrive at a broad consensus of ownership.

Claimchain Integrity

The quantity and quality of cooperation in agreement with precise language determine the strength of a claimchain. The degree to which claim evaluators agree on the exact application of a claim protocol determines claimchain integrity. For example, if all known participants agree that for a claimchain involving a transfer time limit, "UTC time" is related to a clock in the town of Greenwich, then the property transfer can be done with more claimchain integrity then if half of participants insist UTC time was merely an opinion based on activity by a groundhog in Northeastern America. A claimchain is generally better to enable bitwise completion (see definition) such that protocols provide

(mathematically discrete) exact answers to claimchain questions. The degree to which participants share information especially as it relates to the claimchain also determines the integrity of the claimchain. The fraction of participants acting in good faith cooperation determines claimchain integrity. For a claimchain where most participants act in good faith, most participants have agreements to share information with most other participants, and most participants agree on the validity of most of the claimchain transactions (weighted by their value), the claimchain is expected to have the integrity needed to achieve acceptance.

Claim Push and Pull Claim Cooperation Duties

The main duty of cooperation of claimants for honor of claims is to expend efforts to widely broadcast their claim to many trusted publishers which is considered "pushing". The main duty of claim evaluators is expending effort to discover such claims through a wide range of sources which is considered "pulling". So, the first claimant duty is to broadcast their claim widely to the extent agreed by consensus, which is considered pushing a claim. However, this is not enough to ensure their claim will have priority over potentially conflicting claims which have a weaker broadcast strength but greater validity. Therefore their second "push" duty is to notify a broad range of honorable claim evaluators and compensate them for the cost of evaluating timing the claim, which determines claim honorability. Claimants should ensure their claim noticed and respected by many trusted claim evaluators. Evaluators pull the claim because evaluators are expected to receive claim information from multiple broadcasters to confirm that the broadcaster contract(s) are successful in advertising the claim. Evaluators are expected to publish an expansive list of accepted broadcast sources for claimchain data. The more trusted sources that appear on their list, the more potential trust the evaluator should be assigned by participants, but also the more searching that is needed by the evaluators to notice any conflicting information. So, evaluators also have a pull duty of awareness to a broad range of claims broadcasted according to the minimum broadcasting effort rules as set by consensus agreement. So the push duties are for claimants to broadcast and validate their claims widely. The pull duty is for claim evaluators to receive claims from a broad range of sources.

Participant Inclusivity

Inclusivity is an inherently cooperative quality that improves the integrity of a claimchain. Participants are expected to prioritize discrete as clear rules that everyone can see and follow without any doubts as to compliance. Behaviors that result in noncooperation with any participant are expected to be known and judged

fairly with due process. So, claimchain data markets are expected to be inclusive to all participants who are abiding by a clear and concise set of rules. Participants therefore have a duty to prefer inclusive participants with open invitations based on free and open markets for participation. Exclusive participants who favor specific people for reasons unrelated to claimchain integrity are encouraged to be less preferred.

Claim Timing

The claimant is expected to pay a number of claim evaluators, all of whom are tasked with timing and validating the claim record promptly. Evaluators are expected to summarize (such as by metacode) a claimchain database of each accepted broadcaster who includes the claimant’s claim along with their own timestamp, both of which are digitally signed together by the evaluator as a record of the claimchain as a "snapshot metacode"(ref Information Graph:Network Synchronization:Crosslink Metacode). The Service Cog (COG) section describes that "crosslink" process. The summary (by hash) of that snapshot record is considered a "metacode" or "hash". Claimants are expected to repeat this process for a list of trusted evaluators each of which signs the broadcast record that includes their claim. If a claim record is first evaluated at a significantly later time than the claim was first made, then the timing of claim records may be less provable, which weakens the claim as evaluators would have to factor trustworthiness of each broadcaster’s timestamps. So, there is time pressure to have the claim validated soon after the claim is made.

Claim Identifier

A claim identifier includes the item being claimed. Also expected to be included would be any seal which can be later matched to an unsealing code to release the claim.

Claim Pull Incentive Summary

Claim evaluators have a duty to pull all claims that are broadcasted with specific minimum effort as defined by consensus. Without cooperatively pulling properly broadcasted records from any and all broadcasters who are operating under good faith and effort, an evaluator is behaving dishonorably and is discouraged as to be avoided by participants in favor of honorable evaluators.

Claim Evaluation

Evaluators are incentivized to maintain an up-to-date list of the current state of the claimchain as snapshot information (generally expected to be summarized as a snapshot metacode (ref Information Graph:Network Synchronization:Crosslink Metacode) ) about accepted broadcasters and the available claims that they have on record. The expectations of an evaluator are to evaluate any claim created according to a specific claim protocol, record any claim according to the protocols as meeting consensus standards to a public database along with timing information of that claim, and to evaluate each claim objectively by using mathematically specific

and mathematically consistent methodology. Costs for these services are generally encouraged to be consistent and equal for all participants. Evaluation consideration factors discouraged include honor or dishonorable behaviors, personal characteristics, or personal associations. Long-term service cost agreements are encourage to be formed to offer claim evaluation stability over time. This agreement could be formed in any way that results in more stability, whether set by Open Exchange market forces of supply and demand, whether set by estimating what costs would result in a targeted profit margin, a combination of those concepts, or any other method for achieving stability and system confidence.

Accepted Evaluator List

Zeronet (ZNET) participants delegate specific trusted Claimchain evaluators to help determine the validity of a Claimchain transaction. The transaction recipient establishes a list of trusted evaluators. Each participant determines exactly how much evaluation honor is required to consider a claim honored. A Web of Trust application (ref associated section) will offer an initial honor scoring recommendation which can easily be changed. The initial recommendation may be to honor a claim when their most trusted evaluator and a majority of other trusted evaluators who evaluated the claim have accepted the claim. Different types of claims can be handled differently, so this establishes default rules for generic claims. It should be noted that Competing Perspective Consideration content (see associated section) may specifically display claims which are dishonored or less honored during conflicts such as a "forking conflict".

Evaluator’s Broadcaster List

Zeronet (ZNET) evaluators (ref Web of Trust:Evaluator Participant) delegate an expansive range of broadcasters to be aware of all claimchain claims made by all Zeronet (ZNET) participants. The quality of the Evaluator Broadcaster List is expected and encouraged to be one of several factors in selecting a claim evaluator (see associated section). The higher the number of accepted broadcasters which meet minimum standards, the more an evaluator is expected to perform good quality honorable validations. However, each additional broadcaster does add additional search effort, so the number of broadcasters listed may be limited. A broadcaster not appearing on the list does not necessarily limit the evaluator to search only through the designated list unless they claim a limit.

Express Confirmation

One accepted broadcaster and one accepted evaluator are selected as "express" for a transaction that may take less than one second to secure. A broadcast source from which a single broadcast will be considered sufficient evidence of a claim to take action. For rapid

transaction or settlement speed, an express source would typically be selected. Under such a system, the property recipient forms a broadcast agreement for the broadcasting of their claim with one broadcaster and one evaluator. Additional broadcasters are expected to be part of the broadcast, but it is not necessary for the transaction to be considered temporarily secured for the claimant when the broadcaster is sufficiently widely accepted by evaluators. As the transaction propagates through broadcast and evaluation networks, it is considered extensively and permanently secured.

Expedited Confirmation

This is like an Express Transaction Pair but two or more broadcast sources and evaluators are used for temporary security of transaction. The recipient of the broadcast considers a broadcast receipts from each of the expedited evaluators as sufficient evidence of claim from a buyer to provide value to that buyer. All broadcasters on the list are planned to be used for advertisement, but only the expedited broadcasters and evaluators are necessary.

Basic Confirmation

Three or more trusted broadcasters are listed as claim broadcasters on the Evaluator’s Broadcaster List and the corresponding evaluators have confirmed a given claim. Confirmation is done by logically objectively confirming a transaction to be compliant with transaction requirements.

Extensive Confirmation

Twenty four or more broadcasters and evaluators on both the Accepted Evaluator List and Evaluator’s Broadcaster Lists have confirmed (or advertised for broadcasters) a transaction. Furthermore, most of the evaluators and broadcasters are considered trusted participants by the claimant’s Web of Trust.

Transaction Schedule Confirmation

A claim evaluator may acknowledge a claim by issuing a statement about how many pending claims there are for a given claim. This is beneficial for high-value claims where there is fraud incentive for other methods such as releasing the secretive code without any retrocast messaging (ref nearby section). Evaluators may check with each other to ensure which pending claims have precedence over one another and the corresponding timing for each pending claim. They may develop consensus on considering a claim original and irreversible.

Transaction Subjectivity

It is considered opinion whether a transaction is sufficiently confirmed or not. It is considered opinion what level of confirmation and validation is high enough for a transaction to be honored. Evaluators who validate a transaction that should have been invalid are expected to be dishonored by other evaluators. Information from a sufficiently dishonored evaluator is not expected to be considered for transaction claims.

Double Sending

Transferring exclusive property rights on a given property to multiple people while multiple recipients are told that they are exclusively and collectively more than 100% owners of the property, which is contradictory and generally fraudulent and dishonored. This occurs for example when someone has transferred property to another person, but that other person has not sufficiently advertised the fact that the property is now theirs. The earlier owning person could take advantage of this by also transferring the property to a different other person in exchange for additional value in a way. The transaction won't be honored because the pledged property is already gone.

Transaction Decree

A statement where someone transfers their claim of property to another person, and the publication of such a statement in accordance with consensus methods of advertising establishes the transfer as a fact.

Public Settlement Network (PSN) Transactions

are transfer of property ownership where a claim is validated by evaluators and then the transfer is made public. Publication is expected after confidence of confirmation and validation by the receiver(s). A receiver decides upon one or more mutually trusted claims evaluators and also claims broadcasters. More specifically, trust is mutual with the property recipients and prospective future trading partners of the recipient, not necessarily mutual with the sender and receiver. Property recipient(s) select one or more trusted broadcasters to broadly and sufficiently advertise their property claims and reduce the associated risk of double sending by the sender. Property senders are otherwise incentivized because of a potential double-send perspective against a claim being broadcast. So, property recipients have the duty to ensure transfer claims are broadcasted. So, recipients are generally considered to be the payers of the transaction fee, though this cost could be passed on to the property senders by means such as using a contract.

Transaction Broadcasting

Factors for Public Settlement Network (PSN) broadcast selection may include speed, propagation quality, and price. Recipients are expected to form a broadcast agreement with trusted broadcasters to achieve expansive broadcasting for a satisfying price. Recipients also form evaluation agreements with the trusted evaluators in the same way and for the purpose of expansive validation and honor of claim, which also works to propagate the claim. These advertising, evaluation, and recording costs are considered a transaction fee and may be the full transaction cost. The recipient establishes an Accepted Broadcaster List and Accepted Evaluator List for the purpose of the transaction. These

broadcasters and evaluators are listed as part of a public transaction contract. A transaction decree should include a declaration of a source and destination for a property transfer. The sender is expected to cryptosign the transaction decree to the recipient using any and all signing keys required.

Retrocast Transaction Decree

The transaction decree may be a Retrocast Message as described in that nearby section. The recipient sends this transaction decree or a summary thereof to the listed broadcasters and evaluators who a contract is formed with. The sender then sends the unsealing codes as defined by the Zeronet (ZNET) Secrets Protocol (Sproc) section to the recipient(s) and their proper signature, if required, of the broadcast agreement. The recipient uses that information to publish the transaction decree. The recipient is expected to acknowledge the transaction as complete upon receipt of sufficient confirmation from evaluators which is expected to include confirming broadcaster capabilities. The recipient then posts any and all unsealing codes of the claim to all the broadcasters as proof the transaction is complete. The transaction is expected to be marked complete by all parties upon the referenced seal codes being released to the public, and the public identities or related ownership entity designated in the transaction decree are considered the new asset owner(s) as agreed.

Claim Identifier

A claim identifier is a code that corresponds with information regarding a claim which would typically include the item being claimed, and a seal code or other code that enables the claim to be released to another person.

Retrocast Transaction

A retrocast transaction sends a digital asset in a way that is exceptionally irreversible, by releasing a message hash first and then the full message including a secretive code later. The sender tells the receiver the specific assets to be sent. The receiver creates a claim identifier code to identify the new claim of ownership. This identifier is expected to be created by combining the asset identifier code with a secret code. The sender then tells them the identifier code but keeps the secret code a secret. The sender then schedules the transaction using a transaction schedule message. A "schedule message" is first created as a plain text statement and then hashed. The retrocast schedule message is a message which predicts the timing of when a specific message will be unsealed, what unpredicted text will be revealed, and intentions for the unsealing. The prediction statement is expected to consist of text such as "Protocol ZR0: Claim ID XYZ was created with a seal code of ABC123 and unseals at UTC 2022 06 27 23:45:18.

The new claim identifier is 456 in protocol ZR0." ZR0 is the hypothetic name of a claim protocol. "ABC123" is the unpredicted text chosen such as a randomized set of numbers and letters as the secretive seal code for a claim transfer. That entire schedule message is hashed, and the hash is the schedule message identifier. And more specifically, it is also the "transaction identifier" ("TxID"). The schedule message is designed to prevent a message from being "hijacked" by a malicious participant. This schedule message identifier is then publicly broadcasted and recorded by trusted evaluating participants. At this point, the portion of the message text without the secret code can be (not does not necessarily have to) be relayed to the trusted evaluators but not the broadcasters. An evaluator can then release information regarding how many scheduled transactions claims exist for a specific claim ID. Multiple transactions scheduled would indicate a conflict, and such conflict information would be provided to the transaction participants. Conflict is resolved by ensuring the first message to reveal the secret code according to most of the agreed upon evaluators has priority of all others. If different evaluators get different schedules first unsealed, the scheduled claims (for both sender and receiver) are damaged or destroyed to a degree determined by the specific transaction protocol. Good faith cooperation between sender and receiver will avoid such claim damage. After the schedule is sufficiently distributed according to the trust of the transaction’s recipient, the secret code is released by the sender to trusted evaluators by those evaluators relaying the full message such as "Transaction [TxID]: [schedule message as defined nearby]" to all participants involved, at the designated transaction time. The transaction is then honored if satisfactory to the involved evaluators. A certain level of honor set by the transaction recipient satisfies their definition of transaction completeness as the transaction contract is expected to detail. After that level of confidence is achieved, the transaction is then complete as detailed in the transaction contract.

Splitting Transaction

The nature of Zeronet (ZNET) cryptography is to release seal codes upon completion. This creates security risks that must be addressed. One such risk is that if upon sharing an unsealing code (also named unlocking code), all related assets are released. When one sends one asset, all assets of that claim identifier are released. So, to send partial contents to another person, first one sends different parts of their asset into two different claims, one they intend to keep and the other they intend to transfer to the other person after the splitting transaction is done. So, money transfers are expected to often involve two or more separate transaction. The first establishes a claim with the

"change"(only part of property is sent rather than the entire property) of the transaction and another claim with the "sending asset" being transferred to the recipient. The second transaction sends the sending money to the recipient. This is unrelated to "forking".

Combined Trust Retrocast Transaction (cTx)

In transactions where there is ’transaction change’ (only part of property is sent rather than the entire property), this can require a splitting transaction. However The sender and recipient may mutually agree on trusted broadcasters and evaluators to avoid the need for that. In this case, the transaction is managed by the property sender in agreement with instructions of the property recipient. This is generally done by the property sender adding their trusted transaction partners to the list provided by the recipient. The recipient directs which claim identifiers should be used. The sender then takes the steps needed to complete the transaction according to the agreed protocols and details. So, Combined Trust retrocast Transactions (cTx) are done by the property sender in close cooperation with the property recipient. This is generally accomplished by simply agreeing to the Accepted Broadcast List and Accepted Evaluator List for all participants involved in the transaction. So, most digital money transactions are expected to be completed by the property sender on behalf of the property recipient with a formally agreed contract.

Faith in Sender Transaction

Like a transaction, but done entirely by sending the unlocking code(s) to a trusted party, rather than achieving pending status first. The risk would be that the sender could send to multiple parties simultaneously, and there could then be conflicting claims about which new claim contains the asset. The sender normally first changes the status of the asset to pending transfer. For such a conflict, each evaluator is expected to form an opinion on transaction validity based on their Web of Trust ranking, and when an evaluation decision is complete it may never be changed honorably. When Broadcast Agreements and/or Evaluation Agreements are ineffective, the transaction is effectively the same as a Faith in Sender transaction. So, each transaction requires a certain amount of faith. However, without any broadcast agreement the faith of the transaction is at a maximum. A transaction that was not placed into pending status could be claimed to have never been received even though it was, and there would be no witnesses to know what happened except for the parties of the transaction.

Forward Faith Transaction

This is done by transactions that both have full faith in each other. The sender secretly relays the unlocking code(s) and then deletes their copy of the unlocking code(s). The recipient risks a double send by the

sender. No broadcasting is involved. Benefits include the lowest possible transaction cost and maximum possible privacy. The drawback is risk of the unlocking code being insufficiently deleted or not deleted at all as reported, allowing another person full access to the funds.

Claim and Transaction Validation:

Claim Evaluator

Any participant who is trusted to determine the legitimacy of a claim is an evaluator. The less value the claim is associated with, the higher level of speed and automation of validation is expected, and the lower level of broadcasting is expected. Larger value claims are expected to be processed with more scrutiny. Validators are expected to use a set of satisfyingly objective and precise methods of determination of claim accuracy. Personality characteristics are expected to be avoided as a factor in transaction evaluation. All evaluators are expected to have a database of transactions that is not necessarily shared with others and is used for transaction evaluation purposes. When an evaluator is paid to record a transaction, they are expected to evaluate a claim at only one point in time without any reevaluations. Evaluators are generally expected to evaluate a limited range of claims in accordance with their area of expertise and amount of resources.

Evaluator Selection

Evaluator selection is the most important factor for honor of claims. Participants are encouraged to use External Review service (see associated section) to help select multiple Claim Evaluator participants who can be trusted to account for claims according to the agreed upon consensus. Many evaluation services are encouraged, at least 12 evaluators for smaller claims are encouraged and at least 24 for larger claims are encouraged. This process allows a consensus to be achieved more easily on the validity of claims. Factors for good evaluator review are expected to include conformity to the agreed consensus of rules for claim validity, connection to a large number of claim broadcasters, and high availability to perform evaluation service over time.

Honor of Protocol Claim

Affirmation of acceptance of a protocol. If multiple protocols are honored, the order of honoring resolves any conflicts. If not ordered on a single document, the chronological order of submission may be considered as the order from most to least priority.

Honor of Property Transfer Claim

Acknowledgment that property rights have been transferred. This may include a reaffirmation of rights claim by a property owner to maintain their claim.

Cross Audit Claim

A participant such as a Trusted Broadcast Source (TBS)

has evaluated a group of announcements in a specified time range from another source and states how they compare to their own records, summarizing any conflicts in records.

Ledger Leaf Node

The most recent valid property transfer for given property. After property has been transferred away from a specific participant, their ownership is represented as a branch node rather than a leaf node.

Ledger Leaf Node Confirmation

Ledger leaf nodes will not be confirmed beneath a certain size deemed to small.

Database Metacodes and Synchronization

Database state-time summary codes named "metacodes" and cycle sync processes (ref Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization section for description) are used to identify and discover the different databases used for Public Settlement Network (PSN). These metacodes are points for consensus for Zeronet (ZNET) participants. (ref Web of Trust:Perspective Development:Network Synchronization:Metacode).

Public Claims Consensus

All public claims of any kind are encouraged to be listed on the Public Settlement Network (PSN). These claims are expected collated as a database of public claims which may consists of a database for each claims protocol. Most claim records will be assigned a level of honor by claim evaluators with Topic Knowledge Trust in the topic the claim is made. The less topic knowledge trust the evaluators have, the more claim validations will be needed before participants can be expected to honor the claim. Where multiple participants agree on honorability of claims, a consensus begins to form. Depending on the claim, consensus may form in different ways. The broadest consensus expected to be achieved regarding public claims is where encryption public keys match to cryptosigned statements, as this is generally a mathematic proof. Financial transactions are one of the most important points of consensus, which are also centered on mathematic proofs and so can be automated and acceptable to a broad audience. Organizations involved in this activity are expected to be part of topic interest groups that publish assessments on the accuracy of transaction information. These topic interest groups create publications that are analyzed by various Service Cogs (COG) for validity according to mathematical proofs such as currency transaction ledgers. Bitcoin Core is an example of a Topic Knowledge Trust evaluator considered to be topic interest group which helps form consensus on which Bitcoin claims are accurate. These topic interest groups may publish their collective affirmations as a summary record. This summary record is expected to be analyzed and accepted by participants most trusted Group Trust Synchronization

and Consensus Service (GTS) (ref Web of Trust:Trust Information Sharing:Group Trust Synchronization and Consensus Service). All participants are capable of honoring or dishonoring any claim, so it ultimately the responsibility of each participant to determine which claims are accurate, and how much agreement is needed before a consensus has formed, or how much disagreement has formed before consensus is lost.

Public Claims Consensus: Crosslinking

Data Discovery and Synchronization Service (Disco) (ref Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization) provides participants with new public claims meeting conditions they define, which for a Trust Synchronization and Consensus Services (GTS) (ref Web of Trust:Trust Information Sharing:Group Trust Synchronization and Consensus Service) or other Trust Cohesor, such conditions would be claims within their topic of interest pending consensus validation. The topic could be anything, such as encyclopedia entries for example. Service providers collate accepted records of many kinds and relay a summary of records. These summary records are identified by a Metacode identifier. Snapshot Metacodes are collected by Public Claims Databases (ref Service Cog:Information Graph Cogs:Database and Search Cogs:Public Information Database Cog) having records honored or dishonored at specific points in time. A specific claim evaluator evaluates such claims, which is often done with a Claim Evaluation Cog (ref Public Settlement Network:Claim and Transaction Validation:Claim Evaluation Cog). Multiple claims databases (expected to be Public Information Databases) merge and reorganize records with a specific order of most to least trusted record sets such that there are multiple different transaction databases, but with a priority of which database is most correct. This would be expected to be validated by a Group Trust Synchronization and Consensus Service (GTS). The evaluation and validation processes identify any conflicting records, and view that conflicting record where there are two trusted databases but with conflicting data. The participant is expected to automatically accept the record of highest ranked database trust in their Web of Trust, but can see that there is a conflict and a less trusted analyst has a different perspective of a record in question. These Metacodes are grouped in with other Metacodes such as protocol Metacodes when there may be an agreement across multiple databases. These Metacodes are then shared using the Web of Trust to exchange the codes and negotiate with other participants to achieve as broad a consensus as possible regarding the most accurate and current database information using the crosslink consensus process.

Database Consensus Building by Crosslinking

Each shared metacode agreement is a crosslink (ref Information Graph:Network Synchronization:Crosslink Metacode). A consensus of which Public Settlement Network (PSN) databases are accepted and used by participants is developed in a decentralized way in part by crosslinking of databases. The general idea is that participants summarize and track each other's record modifications. See Information Graph:Network Synchronization:Crosslink Metacode section for "crosslinking" definition. Broadcasters and evaluators are expected to summarize (by hash) their records with metacodes where records are sorted at least by category, original publication time, and advertisement spending level. Hashes are explained at ref:Democratic Communication:Identity Information:Hash. Each broadcaster and evaluator is expected to publish their most recent version of their databases by releasing a database summary (by hash) as each record is added. In this way, people can help to prove whether a record has been added to a database and which time the record was added. Alterations would be difficult as multiple network participants access and record this snapshot information. See Web of Trust:Perspective Development:Web of Trust Garden for consensus-building information.

Settled Ledger

Rather than validating the full claimchain, it is expected that transaction evaluators will work from a starting point of settled transactions. After an amount of time such as two years, older claims can be deleted. Also, the previous ledger hash is calculated and noted. The previous ledger hash along with a list of all current honored claims form the settled ledger for a specific date. This settled ledger is then used for evaluations when considered sufficiently reliable. This enables the need for unlimited data retention which would otherwise be excessively large.

Focus Portal Feature:

Focus Points

See the Public Content Network:Focus Points for information about how Focus Points work. This information is needed to understand the Focus Portal references in this section.

Focus Portal Honor

Focus Portals may be set up for different monies. Assigned honor may be adjusted based on how favored or disfavored that money is by a participant. Generally +25% honor for favored money and -25% honor for disfavored money. Web of Trust settings can however be set to any extreme. So, certain money may be entirely ignored for the purpose of search queries, contact registrations, or whatever else the Focus Points were intended for.

Focus Portal Equivalent Support

Cryptocurrency stakeholders of money may notate their monetary structure for a certain recipient address to be considered the address of a Focus Portal. Or they may modify their monetary structure in some other way to support the Focus Portal monetary system. Next, they are expected to have a trustworthy record of money conversion from their money to the dominant cryptocurrency meeting minimum Zeronet (ZNET) criteria in support of Zeronet (ZNET). Finally, there is expected to be a maintained real-time database of Focus Portal (FP) equivalent records for a minimum amount of time.

Digital Money Systems:

Bank

Below a specific transaction value or time delay, it is considered uneconomic to process a Claimchain Ledger transaction but still economical to process transactions on a private ledger that is not listed publicly. This is accomplished through a bank account ledger where a person sends money to a ledger banking service. The ledger banking service then keeps track of who owns what with the ledger service and then participants may expect to be able to receive their money using the Claimchain Ledger upon demand to receive a title on the Claimchain Ledger. This dramatically lowers the threshold of transaction value and speed. Current cryptocurrency participants offer such services such as Coinbase but these participants often are given excessive levels of unearned trust, leaving the bank failed resulting in financial losses for excessively trusting participants.

Token Pack

Token packs require more risk than with bank service because you send value in a way that is difficult to prove that the value was sent. But, Token Packs can provide lower costs than a bank for many services. See "Token Pack" section for more details.

Trusted Peer Ledger Transaction

Below a specific transaction value, any kind of banking or ledger service is considered uneconomic. However, it may still be economic for one trusted participant to track smaller amounts delegated to a trading partner that may accrue to larger amounts that are economic, to then exchange the ledger balance for another medium of exchange such as a Bank deposit, Claimchain Transactions digital money, or Token Pack token. These trusted peer accounts are considered a Peer Ledger account. Transaction value limits are expected to be the highest for a Claimchain Ledger, followed in descending order by Bank Transactions, Token Pack Transactions, and finally Trust Peer Ledger Transactions which could be so small as to transact a purchase for example 50 milliseconds of a processor in an automated system with a participant who is trusted to a small degree. So, this account is expected to be direct with trading partners rather than through other mutually participants such as banks or

digital money systems.

Blockchain Transaction

A group of people form a consensus on a system of puzzle-solving that determine who may process a set of transactions. This set of transactions is called a transaction block. The participant who solves the puzzle first then adds their transaction block to a chain of transaction blocks, and the ledger of who owns how much of the associated money is adjusted based on the transaction block. Consensus forms on which blocks are valid as to following the consensus agreed transaction rules. A new puzzle is generated based on unpredicted (and allegedly practically unpredictable) aspects of the block which is most recently added. So, this cycle repeats to add new sets of transactions.

Token Pack Service:

Token Packs

Token Packs are methods of payment where the amount transacted is less than what would be efficient for a digital money such as transactions of less than USD$ 0.03. Token Packs are designed as methods of paying for Zeronet (ZNET) automated services where each token is redeemed for (typically) one unit of service. High transaction volumes are easily supported with this system. Most Service Cogs (COG) are expected to operate by token service. When the service provider collects a specific minimum number of tokens, the tokens are redeemed for a medium of exchange designed for higher values.

Token Pack Service

Tokens are generated to be sold in sets that are later redeemed for an offering or money.

Token Pack Cog

See Service Cog:Digital Money Cogs:Token Pack Cog.

IT Resource Token Service

IT Resource Token Packs are sets of randomly generated passwords which allow assignment of the token to a specific client or service provider. These token packs are paid for, typically to pay for a specific offering, but also purchasable without any specific offering in mind, and then used to access Zeronet (ZNET) services. An expected primary purpose of token packs is to reduce unwanted messages including some forms of Denial of Service (DoS) data, but they can be used for many reasons. Tokens can be used for distributing content that is pay-per-download. For example, when someone buys a proprietary software, they might also be given three download tokens that can be used within on year of receipt to download their purchase. Or, they could be given one token that is usable three times. Token packs are expected to replace Captcha service of current internet sites to save substantial amounts of time. The price for each token will be different for each purpose. Expected usage includes Captcha, priority download

access, and service vouchers. Service providers may trust other parties for this service, though as with any service they may directly run their own Token Pack Cog (COG). Tokens may be intended for various number of uses. They may be single use, usable a set number of times, limited unpredictably, and unlimited usage, as negotiated with the token pack requester, issuer, and users.

IT Resource Token COG

An automated IT Resource Token Service. See Service Cog:Digital Money Cogs:IT Resource Token Cog.

IT Token Distribution Service

IT Token Distribution service manages token packs for content distributors. The most frequent expected usage of the Public Content Network (PCN) is distribution in exchange for donations or advertising acceptance. However, hostile entities may attempt to purposely drain such resources by using up a distributor's bandwidth with the intention to waste it which is considered a form of Denial of Service (DoS) attack. When an IT Cog contract is formed, the service buyer may request service tokens of varying priority levels that act as passwords for the service, and may be able to request more automatically on demand from that service provider. When a problematic resource drain is automatically detected, the priority token system activates until the drain attempts halt.

OPEN EXCHANGE (OX):

Open Exchange Summary

See Zeronet Component Summary:Open Exchange section for summary.

Financial Exchange

Transaction types expected to be supported for Open Exchange include digital money, digital Bank Transactions, and Token Pack Transactions in order of most to least expensive and most to least secure.

Open Exchange (OX): Contract Class:

Contract Governance Classification

Participants agree on a complete governance model for contract performance including mediator options, arbitrator options, enforcer options, Contract Code of Conduct, Governing Civil Contract, Declaration of Force Initiation, and Protocol Foundation. See Democratic Communications:Contract Foundation for details.

Contract Governance Identities

Mediator, arbitrator, and enforcement identities are expected to be points of agreement stated on contracts. Each of these Contract Governance Identities is expected to be listed on the Information Graph (Iggy).

Contract Class

Participants may agree on a set of contract topics.

Templates are expected to include topics of negotiation for each type of offering. For example, a contract for a haircut may include provisions on price, date and time, cancellation limitations, cancellation procedures, paid review agreement, quality assurance, and performance escrow bond.

Value Exchange Contract

A contract where the dominant purpose is an exchange items, goods, or services of similar market value. Contract length may be expected to be in accordance with the total value being exchanged.

Open Exchange Post

To post is to publish a classified offering as a Public Post (ref Democratic Communication:Public Messaging:Public Post). Types of post include Contract Bindings, List, Bid, Ask, Accept, Close, and Cancel.

Bid

Contractually make an offer to pay for an offering.

Ask

Contractually make an offer to sell an offering.

Accept

Contractually sign to agree to the term of a contract, such as accepting a bid or ask price for a contract.

Close

All terms to a contract are agreed to, and the terms have been fulfilled, or the contract has otherwise ended.

Cancel

Cancel a bid, ask, or other contract term.

List

List an offering on the exchange. Uses the Information Graph (Iggy) to identify the classification category of the item.

Complain

Post a public complaint regarding the status of a contract. Mediation and arbitration may be private or public depending on the agreements and behaviors of the participants involved.

Offering:

Offering Metrics

Expected offering metric fields include Item, Title, Description, Contact Key, Preferred Money.

Indexed Metrics

Any entity for exchange may have a list of indexed metrics and associated measurement or quality. For example, a vehicle for sale could list a car as having an indexed metric of "color" with the measurement of "blue".

Offering Qualities

Any product features that are not indexed metrics can be explained with this offering text. The item identity and item title are expected to be qualities of all offerings.

Offering Conditions

Common Conditions: Performance Time, Performance Location, Minimum Bid or Price, Contract Governing Body,

Mediator, Arbitrator. Offering agreements are encouraged to acknowledge liberties including civic freedoms and rights, and discourage monopolistic leverage to extend control over unrelated basic needs to or complete control over basic needs.

Quantity Offering and Unique Offering

A Quantity Offering is a participant who makes a public announcement about a product or service that will be repeatedly made available to multiple parties. A unique offering is a good or service that will be made available to a single person and may not be the same such as in terms of features and benefits as any other offering of the participant. A Quantity Offering may be expected to be reviewed by the public. Something like a parcel of land would likely be considered a unique offering, while something like a bag of rice would likely be considered a quantity offering.

Price vs. Cost Context

Cost is focused on the resources to create an offering. Price is focused on the resources to exchange an offering.

Money vs. Currency Context

Currency is focused on value as an energy of exchange, such as for describing prices or costs. Money is focused on a preferred medium of exchange for an offering. A product may be priced in USD$ while only being able to be purchased in BCH$. In that case USD$ is the currency, while BCH$ is the money.

Standardized Exchanges:

Standard Exchange

By operating under a consensus agreement involving Grex (Group Records Exchange) format (ref attachment) of offerings, standardized exchanges may be developed.

Dataset Exchange

Offerings of data such as database records and topic streams of a specific topic, which are restricted to a specific range or form. Data is generally fixed to an identification tag or topic, determined in advance, without being created for a specific participant request. Data may be provided in Group Records Exchange (GREX) format (see Democratic Communications:Group Records Exchange) or another format as specified. A complete list is expected to appear on the Information Graph (Iggy). When data is sold or even provided at no direct cost, it a bond may be posted guaranteeing the accuracy of such information by the data exchange or the sources, which are expected to be cited. This way, if a source of information abuses the system, there is a way for the cost of information review required to remove the information to be compensated. There are expected to be content distributors that claim to be the creators of the content giving it away for free, when it is actually sponsored or malicious data.

Information Service Exchange

The Information Exchange includes such services as cog provision, customized information stream services, Research assistance, Q&A, expertise offerings, medical advice, financial advice, and social contract advise and handling. Information exchange offers uniquely and/or dynamically generated information according to a custom request. The request is based on a variable range of information provided by a participant. The Data Exchange (Datex) (see nearby section) is for "bitwise complete" offerings which are not tailored to a specific participant request upon demand. So, static database records are for the Dataset Exchange while dynamic information generation is for the Information Exchange. Also included are privacy masking services such as VPN. An ISP is an information service as well. Governance services not directly involving physical resource management are including such as mediation, civil negotiation, civic negotiations, and arbitration.

Goods Market Exchange

Items having or including "physical matter" for sale. Terms are expected to include delivery locations and delivery dates.

Claims Market Exchange (Claymex)

Items having energy form ("virtual", "intangible", "tokenized") form, including land.

Derivatives Exchange

Contracts for financial exchange including stocks, loans (including bonds), insurance, (conditional) grants (like a "GoFundMe"), and derivative options.

Labor Market Exchange

For offering labor services.

Civic Exchange (Govex)

Social Contracts directly involving tangible (physical) objects or life forms. Services include escrow, civic enforcement, and cohesor service (ref Rainco:RCG:Highlights:Cohesor Roles) when physical interaction is related to such services as wanted in a specific physical location.

Private Information Technology Resource Exchange (Pitrex)

Lease unused system resources over the internet automatically to the highest bidder. The system satisfies the privacy of network participants for the purpose of maximizing the freedom of speech for participants. This component is used in a demonstration hardware implementation of all other components.

Logistics Open Exchange

Sells logistics services over the internet generally automatically to the highest bidder or other purchasers.

Cab Exchange

This is a part of Logistics Open Exchange. When someone is going on an unscheduled trip, generally for a primary purpose other than mail delivery or taxi service, but has extra space for such a purpose, they may offer to transport additional people or things along their designated route, and they may

furthermore offer extensions if they are willing to extend their route for the dropoff. They may post their itinerary to the Logistics Open Exchange. Cab Exchange service is expected to be often less formal than other Logistics Open Exchange services.

Advertising Exchange (Adex)

An automatable advertising system. Those with influence over advertisers including metastream providers are hoped to encourage advertisers to have no set minimum purchase or quantity discounts as a way of helping smaller businesses start up by using automated display systems. Advertising Exchange advertising participants are expected to cooperatively syndicate to a generously expansive range of Data Negotiation Service (ref Web of Trust:Data Negotiations Service) providers just as Data Negotiation Service is expected to syndicate to a generously expansive range of advertisers. Any censorship is entirely set by each participant's announced preferences so that advertisers to not monitor content of any advertisers. Monitoring is entirely the responsibility of the advertising recipient who sets their advertisement content filters according to their preferences and social contracts. Advertising is expected to have advertising medium, a number of demographics, and declared censorship filter allowances, as indexed metrics.

Standardized Exchanges: Private Information Technology Resource Exchange (Pitrex):

Common Services Offered:

BYTE Data Storage by the Byte

SCRIPT Scripting and Interactive Content

COMP Computing Package

CALC Calculation

DB Database

CPU Central Processing Unit

RAM Random Access Memory

BAND Bandwidth

HTTP Fetch Hypertext Transfer Protocol Fetch Service

See Service Cog:Service Cogs and Cogs for Cogs for more details about these services.

Partial List of Extended Services Offered:

VM Service

GPU Graphics Processing Unit

FPGA Field Programmable Gate Array

See more extended services at Service Cog:Service Cogs and Cogs for Cogs.

Private Information Technology Resource Exchange (Pitrex) (ctd):

IT Public-Usage Token Packs

See Service Cog:Digital Money Cogs:IT Resource Token Cog) for a description of IT token packs. Public-Usage Token Packs may be distributed and used for many services and content, especially content available at no direct cost to the general public. Distribution is

designed to allow a broad range of people to access information or an information service without congestion. Participants may otherwise wish to use more of a resource than what is available on a per-participant basis or on a few cases maliciously waste the resource. In this case of general public access to an information service, congestion could be more likely to be an issue. To help avoid congestion, priority service tokens are granted to people with the higher Web of Trust ratings on the distributors Web of Trust. Generally the first token requested from a known (signing key) source gets top priority, the second request results in second priority, and so on.

Congestion Avoidance

Outbound Avoidance

is a limit for outbound IP traffic volume to certain places by destinations already considered congested. This could occur because of service congestion, a DoS attack, or greylisting. Greylisting involves traditional website access using proxy access. See Service Cog:Service Cogs and Cogs for Cogs:Greylist Cog for details.

Inbound Restrictions (hostile IPs).

Either manually or by 3rd party service, IPs that are alleged to do harmful behavior such as DDoS attacks are expected to be blocked from usage of system resources. This is expected to be done with a Blacklist Cog (COG) (ref Service Cogs:Service Cogs and Cogs for Cogs:Blacklist).

Port Restrictions

Should be done through the participant’s Firewall Service Cog (COG). The firewall should in turn have a way of sharing a report of which ports are whitelisted and blacklisted to other information systems on the device. Any statistical data reported to the firewall provider is expected to be relayed through a Data Negotiation Service (ref Web of Trust:Data Negotiations Service).

Banned Content

Governing or authority organizations may claim a contact address such as a web page or other data to be banned. Participants can choose to cooperate with governments to censor their content. When participants set up Zeronet (ZNET) on their device, they may already know which contact address and other contact information is the appropriate contact for their government body. If not, the most popularly used addresses are expected to be available by Zeronet (ZNET) information service providers such as the Content Discovery Service (Cdisc). A UN website may have a website that lists the official website of each member country, so the UN would be an information service provider listing contact points for various governing bodies. Each member country may then share a list of banned content. Participants

select the governing body in which their computer currently is domiciled, and that information is used to report and share information regarding banned content according to their preferences. That selection also determines which information will be ignored (with voluntary participation) instead of displayed on their browser such as Netportal. Each governing body may develop Service Cogs (COG) for this purpose. SigilX settings (ref Democratic Communication:Protocol Resolution:Sigil X Protocol) can also be used to automatically ignore or replace unwanted data.

Contraband Detection

A participant's information filtering associates may send a list of banned content hashes to systems subscribing to that filtering participant. Any files matching these hashes may be deleted automatically with the cooperation of the participant. This list may take up substantial device memory space depending on the quantity of banned content.

Battery Depletion Avoidance

Processing power should generally only be distributed while the system is plugged in and charging or fully charged. If system battery information isn't available, then a trial and error system may be able determine whether the host computer is plugged in on most systems. Any power related shutdowns will be a noticed annoyance by participants and carry a high opportunity cost due to user uninstallations. Temperature data may be available to help determine this because the battery will generate heat when being used, causing an increase in system temperature, then providing a clue that the system isn't plugged in. If the user has available funds, predictive scheduling service is expected to be available such as by Service Cog:Service Cogs and Cogs for Cogs:Generalized Prediction Cog to determine when the participant is and isn't plugged in based on all available factors. This should be a rare problem because a strong majority of systems have such information available.

Standardized Exchanges: end

NETPORTAL:

See Zeronet Component Summary.

Netportal is a Zeronet (ZNET) internet browser. See Zeronet Component Summary:Netportal for a more complete summary.

Mission

Netportal is the internet browsing and cloud computing software that will offer access to Zeronet (ZNET). Initially Netportal will use a participants default browser for browsing, but offer special software for cloud computing. Applications for publicly accountable

and open computing through the Web of Trust for the Public Settlement Network, Open Exchange, and digital money are important capabilities of the initial version of Netportal in support of public reviews, economic exchanges, and social contract interactions. Netportal will be initially designed to display Public Content Network content including articles, audio, and video, portals for the mentioned major components of Zeronet. Computer code that is easily reviewed and audited is important, so coding standards will be developed to such an end. The Information Graph and Service Cogs will offer comprehensible back-end architecture for easy coding. This will lead to code that is easy to review. Development standards, software, and learning resources will also be suggested for that end.

## Portals to Replace Websites

Portals are designed to replace traditional websites. A portal is an interface created to access various Zeronet (ZNET) databases for any and all internet interactions such as discussion, reviews, and maps. Portals are also designed to control a participant's internet experience and resource distribution, so Zeronet (ZNET) system settings are controlled by designated portals. One key difference between a website and a portal is that a portal doesn't necessarily control their own databases. A portal is primarily a graphical user interface (GUI). This is done so that participants and content creators can retain better control over their content. Rather than submitting content to a website, participants store their own content and send a reference. The reference could then be copied by the portal service provider to their own database, but more likely it is kept as only a reference. Because portals generally don't use their own databases, it is expected to be much easier to copy a portal and edit it into a similar portal than it is to copy a website and create a similar one. Portals are encouraged to be created as Open Collaboration Content using the Open Collaboration Protocol (ref Democratic Communication:Cooperative Development:Open Collaboration Protocol). Websites are essentially replaced by open database interface systems, to access systems such as the Open Exchange (OX) database and any number of other Zeronet (ZNET) Group Records Exchange (GREX) (ref attachment) format database.

## Netportal Downstream

The Netportal Downstream is the Zeronet (ZNET) data as it is pulled (downloaded) as part of Zeronet (ZNET) and also data as it as it is pulled (downloaded) by the operating system. This data can be checked for malicious activity because this data stream should reflect the entire data exchanged by the operating system to the device. If there is hacker activity, it is hoped to be recorded by these data logs. We expect internet activity to be able to be 'played back' later in ways that precisely repeat internet activity.

Netportal Upstream

The Netportal data Upstream is the data pushed (uploaded) for Zeronet (ZNET) activity or any other activity of the device. This data is logged in synch with the downstream data. So, this is played back along with the datastream to ensure that exactly the same internet activity can be played back in precisely the same way as it happened previously. In some cases exact replay may involve additional steps like activating a feature that also records keystrokes, mouse clicks, voice command activation, and so on. Such history may be able to be encrypted and then saved as the participant determines best.

Netportal Datastream Database

The Netportal Datastream Database is an internet activity log database file containing a combination of Netportal upstream and downstream data in the Plain Text Protocol (PTEX) format that can be used to detect hacker activity. It can also be used for tracking, so it should be heavily guarded data that should be deleted on a regular basis. This system can be used for restarting incomplete and interrupted pulls (downloads). Archived data may be encrypted and then saved according to participant preferences.

Relative Information Graph Display

The Information Graph (Iggy) is displayed according to a specific Avatar Perspective (ref Web of Trust:Perspective Development:Service Cogs by Crosslink Metacode:Web of Trust Avatar Perspective for details). Titles may be hierarchal, and the default syntax for that (as set by the Democratic Communication section) is Title:Subtitle, where the colon is an example of any delimiter that may mark the end of a title and the beginning of a subtitle. Generally the full topic text will be treated as one topic, and the subtitle will be treated as one subtopic for various purposes like topic searches. By titling content with an existing title having different underlying content, one competes with the other content for ownership of that title in a sort of conflict of words. Those with higher Web of Trust ranking are the ones to have their content displayed as the content that match with a given title. Competition may not be hostile as for example long periods of time will tend to fade preference for older content in favor of newer content.

Zeronet Settings

Settings controls selected and customized by each individual determine how information will be displayed, interpreted, and shared or otherwise kept private.

Competing Perspective Consideration

As a participants Web of Trust is built, the chance of more unbiased and balanced information should increase, but the incentive for trusted others to take advantage of misplaced trust grows. So, information with possible reasons to reduce trust for trusted others will be

visible by more untrusted parties. The Web of Trust can cause a "yes bubble" in which their web of trust all tends to believe wrong information, and because their perspective is reinforced by trusted others and repeated often, they become overconfident in bad information. So, any time the Web of Trust is used to display information, contradictory information by lesser trusted, most untrusted people, and people in competing or opposing groups may also display while being marked as such. Competing Perspective Consideration helps protect people against "thought bubbles" and "group think" by ensuring multiple perspectives are available on any given content having multiple interpretations or comment. This feature is not unlike the current internet service Dissenter. So, when someone specifically tags content as "dissenting" from a specific content, this provides the beginning point for Competing Perspective Consideration content interjections.

Competing Perspective Display

A portion of the screen as determined by the participant prioritizes Competing Perspective Consideration when content is dissented against. Competing Perspective Consideration service is expected to paid by dissenters to post dissenting content also by the Competing Perspective Consideration service client. This service provider operates like the Metastream service provider, but posts various alternative perspectives including popular alternatives, paid dissent, dissent from lower trust level sources than would usually be displayed, randomized dissent in reply to specific other content, and dissent receiving high donation levels to their creators. The paid dissent is sent to specific Competing Perspective Consideration service providers, expected to be weighted by trust level, under contract with those providers. A certain amount of the display is for each type of dissent. For paid dissent, the most highly paid dissent appears more often based on the amount paid for the particular dissented content such as twice as often for dissent that is paid two times more than other dissent. Dissent (as with any misleading content) that is reviewed as off-topic is expected to be filtered out through the participants Web of Trust.

Directly Competing Content

Content titled the same as a previous title (with both titles and subtitles) becomes competing content. Indirectly competing content is by being marked Competing Perspective Consideration (ref that section nearby) which may have an associated reference to the replacement content of any title. Depending on the preferences of participants, a version screen may be displayed so that a participant can select different versions of the content. The list by default is expected to be sorted by trust level, displaying the alleged content author for each competing option. The first known publication date is also expected to be displayed.

Content targeted to one specific person as a private communication is not considered competing content unless the same title is applied twice consecutively. A participant's Web of Trust determines what content dominates the competition and is displayed.

Accidental Title Repetition

Someone may accidentally write the same title twice for two different messages. The author should be prompted as to whether they mean to revise previous content, or add detail, in which case the author is encouraged to add a subtitle or otherwise modify the title slightly such as by adding a sequence number to the end like "Meeting Summary" being changed to "Meeting Summary: 2".

Navigation

Search Query Window

The default portal query window is a small circle that becomes a partial oval when text is being entered. When the query is being done, the oval changes to indicate an active query. This default is representative of the simplifying nature of Zeronet (ZNET).

Search Query Result Set

The search result set is delivered by the selected search service cog using the same format as a metastream provider provides content suggestions.

Website

Websites are expected to have digitally signed components that are considered more valid when signed by the person who created the website entry password (or website signing key if there is no entry password). The signer is also expected to be known by signing the public key used to create the website. This information may be part of the Information Graph (IGGY) and other Zeronet (ZNET) components by using encryption and a shared password that unscrambles the content on the Information Graph (Iggy). It can also be developed as an entirely separate information graph, separate content network other than the Public Content Network (PCN), and none of the Zeronet (ZNET) components except for the Netportal browser.

Websites Design Compared to Portal Design

A traditional website needs a "backend" to function. A portal instead is expected to define a specific open-source interface (which could be HTML) and declare open-source Group Records Exchange (GREX) databases to connect to, and is expected to suggest sources for the data rather than connecting to a proprietary system. When a specific delegated authority is wanted for systems involving such concepts as rating, scoring, or specific evaluation, the authority public keys and connection addresses are referenced. The delegated authority then may use the crosslink metacode system to confirm the validity of such information (ref Information Graph:Network Synchronization:Crosslink Metacode for crosslinking explanation).

Portal Collaboration

It is encouraged behavior on Zeronet (ZNET) to develop portals using the Open Collaboration Protocol. See Democratic Communication:Cooperative Development:Open Collaboration Protocol for details on how such collaboration works. Website developers currently created websites with HTML files which are discouraged from being copied. Portal developers are encouraged to create designs that can be shared, reused, and modified. Rather than monopolizing data that people want to openly share like every major website, we as information providers collaborate together so our information is shared in a decentralized way with any profits being directed in more moral and ethical ways. So, we wish to shift initiative of content distribution from information power brokers to information providers and content creators.

Cog Service Provider Profile

(Copied from Democratic Communications:Zeronet Protocol): Service Cogs (COG) and content service providers are expected to post a profile to a contact database such as Service Cog:Information Graph Cogs:Contact Discovery Cog summarizing their services offered to participants. The list should include records of services provided and their associated prices.

Content Tagging

Options for tagging content on Zeronet (ZNET) include commenting, commenting as dissent, content evaluation review. Content may be editing as either collaborative content or competing content but that is not considered tagging. See Democratic Communication:Sigil X Protocol:Tagging Service for details.

Content Storage, Content Editing

All Zeronet (ZNET) content is expected to be stored on an the participant's local device automatically unless settings are to do otherwise. By default, the content is kept for as long as storage allows or up to seven years. Participants are expected to designate a certain amount of their local device data storage space to Zeronet (ZNET) Netportal content records. Content can be edited as either collaborative content or competing content. With collaborative content, the editor credits the previous content composers with a certain percentage of the work, while they request a certain percentage of credit to them self. This begins the credit negotiations process which is only able to be somewhat automated.

Content Tagging and Commentary Privacy by Avatar Compartmentalization

When a topic is being tagged, commented on, or otherwise participated in, an Avatar dedicated to the specific topic may be automatically activated to compartmentalize a participant's information for privacy purposes. It becomes too easy to identify a user based on the likelihood of one avatar having a specific mix of interests, and cross-referencing that information.

File Handling

HMTL files are generally automatically placed a dedicated folder by operating systems, and portal files should likewise be expected to be in a dedicated folder. Content files will frequently have an associated metafile. When they do, that metafile should be in a folder as well.

Netportal Security

Netporal security relies on all information being filtered and checked with a Web of Trust. See that section for details.

Sending Stream Privacy Delays

Data is not sent instantaneously for privacy. Data may be sent every so many seconds such as 0.33 which is more than most people's reaction time. There should be a consensus minimum randomized delay such as 0.1 to 0.2 plus a constant randomized delay such as 0.03 to 0.09 which would be different for each participant avatar.

Netportal Development:

Component Interactions

Netportal primary interface is the content browsing window. Also included to interact with other Zeronet (ZNET) components such as the Web of Trust, Service Cog (COG), and Democratic Communication (DCOM). These components are all described in detail in their respective sections.

Application

As described in Zeronet:Democratic Communication:Zeronet Protocol, an aggressive plan to replace internet interface languages including HTML and CSS is part of Zeronet (ZNET) is formed, but for practical purposes existing protocols will be used to a expansive extent to be operational quickly.

VPN System Modification

Video and voice calling often have insufficient quality using most VPN connections. A VPN application layer interface is expected to be designed that may directly connect to the peer rather than using the VPN interface when connecting to immediate family members because while there is a small risk of a network spy noticing such connections, they are expected to be publicly known connections any way. This may involve VPN organizations incorporating Zeronet (ZNET) codes into their VPN client software for compatibility.

Graceful Latency Conferencing

Software may be developed that estimates latencies and makes such a latency constant though a time delay to the 2nd worst of 12 ping tests. This provides clear video and voice quality but with a consistent delay. The software may also account for expected packet loss and send redundant information over the connection.

Initial Coding

Minimally modified versions of Tor for peer-to-peer connectivity, qBitTorrent for direct file transfers, and

Komodo for banking are expected to be used for the Zeronet (ZNET) software. So, the initial application will incorporate some or all of those applications. While this results in a somewhat "scattered" internet platform, it may be better unified over time. Protocol usage is described in more detail in the Democratic Communication (DCOM) section.

Weaknesses

The initial version of Zeronet will be inefficient for real-time gaming because of higher network latency. Image editing and 3D modeling may also have high overheads to overcome. Plain Text Protocol math operations are slower in back-end computing than machine codecs, but hardware could be developed that makes it less slow. Cogs that use direct peer connections and machine formatting rather than Plain Text Protocol are possible that overcome these hurdles, but are encouraged only to be used where strictly necessary. Cogs that involve direct peer connections and binary formatting and any associated codecs are expected to result in security advisory notifications.

Netportal: Features:

Query Bubble

For searching Zeronet (ZNET) or other purposes as the participant adds.

History

It expected to see browsing history as settings allow for up to seven years or longer as specified. Selecting a history item loads the item in the browser.

Sort Options

By Time, By Creator

Search

Search history for keyword.

Title: Searches title of content only.

Full: Searches entire content for the keyword(s).

Forget Time Range

Forgets any data from specific start and end times.

Delete Item

Portals

It is expected to have portals or other command shortcuts listed.

Default Portals:

Democratic Communication (DCOM) Portal

Netportal Internet Connection Portal

Connection Check  Will check to see if the internet is connected and if so, what is the global IP address of the connected device.

Ping  Will time the connection to another internet device using the Ping protocol.

Zeronet (ZNET) Socket Check  Will query another internet device to ensure a socket connection is available.

Netportal Avatar Contact and Postage Portal

Settings by Avatar: Crypto Key Set, Protocols

Preferred and Accepted
Contacts by Avatar: Contact ID as initial sharing "public" key hash, Declared Current Status, Sharing "public" Key, Current Postage, Protocols Preferred and Accepted, Public Profile, Notes
Netportal Postage Settings
Tokens by Avatar
Token Purse: Token, Token Cog Contact ID, Redemption Status
Token Redemption Stack: Token, Token Source Contact ID, Token Cog Contact ID, Redemption Status
Link to Messaging Portal
Netportal Messaging Portal
Communication Lines by Avatar: Communication Line ID, Contact ID, Contact Address, Protocol, Current Status, Scrambler ("symmetric") Key, Start Time, End Time
Messages by Avatar: Communication Line ID, Contact ID, Contact Address, Protocol, Status
Messages by Communication Line: Line ID, Message, Bytesize Claim, Received, Requested Timestamp, Received Timestamp
Message Parts by Message: Message ID, Part ID, Bytesize Claim, Timestamp Received.
Sigil Portal. For each Sigil Namespace:
Namespace Rank An integer beginning at zero then counting up. Lower ranking Sigil Namespace is considered before higher ranking Sigil Namespaces unless ceded otherwise.
Rank ID A hash of the namespace definition.
Sigil Namespace Table Matches a namespace symbol or symbol set to its value as in a dictionary, encyclopedia, or protocol syntax.
Zeronet Resource Control (Zerco) Portal
Public Content Network (PCN) Portal
Metastream Portal
Topic Search Portal
Service Cog (COG) Portal
Web of Trust Portal
Trust Garden Portal
Open Exchange (OX) Portal
Information Graph (Iggy) Portal
Network Graph Portal
Datagrid Portal
Database Portal
Public Settlement Network (PSN) Portal
Digital Money Portal
Content Editor Default Portals
Text Editor, Image Editor, Video Editor, Audio Editor, Olfactory Smelloscope Editor for Gas Experiences
Additional editors of any and all sorts are encouraged.

Tabs

As with most browsers, multiple information displays can be available simultaneously by having multiple tabs.

Menu Options

New Browsing Window

New Browsing Window: Forgetful Mode

Forgetful Mode

Pulled (downloaded) content won't be recorded and cannot be replayed at a later time. A prompt pops up to ask if the currently displayed content should be forgotten as well.

Cut, Copy, Paste

Creator Mode

Changes the Portal to Development Mode where the GUI can be redesigned and text or content can be edited.

Inspection Mode

Provides selection options and analysis of the portal structure elements.

Blank Page

Opens a blank page where content can be created as with a Word Processor app.

Find

Finds specified text on the display either in one tab or in all open tabs.

Print

Custom

Edited menu options.

Zoom Level

It should be possible to proportionally size content on the participant's display according to a specific multiple from a low number such as 1% which shows a broad range of content in low detail, to a number such as 900% where a small range of content is shown in high detail so it is easier to see on the display.

Portals:

Summary

Portals are graphic user interfaces to a Zeronet (ZNET) information system. Default portals are files that can be easily edited. When someone edits and then publishes an portal, they are expected to credit the portal appropriately such as by using the Collaborative Development (ref Collaborative Development:Open Collaboration Protocol) system.

Zeronet Distribution Portal: Summary

A Zeronet (ZNET) participant with a computing device under their control can transfer their system resources to Zeronet (ZNET). The default setting is to transfer control of a fraction such as two thirds of all available resources to Zeronet (ZNET) in exchange for market rate prices. Zeronet Distribution Portal provides a Zeronet (ZNET) service cog management system to help determine what computing resources are available for redistribution. This resource distribution control originates with the Zeronet Distribution Portal. This control enables Zeronet (ZNET) participants to create

and earn resources as distributors and enablers of Zeronet (ZNET). See nearby and neighboring sections for details.

Zeronet Resource Control (Zerco)

This control allows participants to modify their Netportal browser. Participants dedicate an explicit amount of system resources to Zeronet (ZNET) using the Zeronet Distribution Portal. These resources are managed with the Zeronet Resource Control (ZERCO) process. The process involves filtering resources through the Web of Trust delegating control over computing resources and associated information flows to trusted parties who manage the resources. Furthermore, Netportal manages resources for the participants Zeronet (ZNET) browsing experience. Processes like displaying metastream data such as a newsfeed on their screen for example are authored by a specific person, and that person is considered the controller of that process. After someone reads and understands a process, they can adopt the process as their own, and be equally considered the controller of the process. So for example if someone wishes to adjust information to sort it differently on the screen, they might analyze the computer code for the process, then edit that code. Upon doing so, they become the controller for the process on their computer. If this code is shared and adopted by others, the controller changes to that editing participant.

Zerco Portal

Zerco provides a Zeronet (ZNET) service management portal for Zeronet (ZNET) participants. This interface uses a Netportal portal.

Zeronet Resource Control (Zerco) vs Zeronet Distribution Portal

Zeronet Resource Control (Zerco) manages resources that have been distributed by the Zeronet Distribution Portal with permissions set by the Web of Trust. Zeronet Distribution Portal determines what amount of device resources to dedicate for different purposes. Zeronet Resource Control (Zerco) determines how put those dedicated resource to use.

Avatar Portal

In replacement networking websites like Facebook will be the Avatar Portal. The Avatar Portal is the channel for a specific avatar to distribute content to "their channel" according to the Democratic Communication (DCOM) protocol so that the portals connect to each other seamlessly as with different users of a traditional social media website. This is generally done by publishing content to a public database rather than a website, which is then accessed with a purpose-built Netportal portal. The Avatar Portal design theme is generally expected to be controlled client-side and be uniform to everyone’s Avatar Portal. Customizations to each avatar are within limits set by participant customization range settings. During transition to

Zeronet (ZNET), all of a participant's linked social media activity on traditional websites is generally expected to be "screenscraped" into their Avatar Portal automatically using a Screenscraper Cog (ref Service Cog:Service Cogs and Cogs for Cogs:Screenscraper Cog). Any activity in their Avatar Portal may then be distributed according to their participant settings to their favored websites, if any. Participants are expected to distribute content to peers in any Public Content Network (PCN) format as public posts (ref Democratic Communication:Public Messaging:Public Post).

Messaging Portal

An interface for submitting public and private messages. See Democratic Communications for public and private messaging sections.

Cog Portals

(copied from Service Cog:Cog Portals)
Most Cogs will have an associated service portal to interact with that service. Service cogs are expected to provide a user interface for their service via a service portal. See Netportal:Portals to Replace Websites for details.

Portal Themes

Portals are expected to be based on a visual theme. Each portal is expected to be able to be fully customized by participants not just by editing the portal but also the visual theme upon which it is based.

Metastream Portal

A primary display of Netportal is expected to be the Metastream. See Public Content Network:Key Features:Metastream for details.

Metastream Zero (M0)

Metastream Zero (M0) is expected to be a default Information Graph (Iggy) metastream for new participants and could be compared to Reddit.com or Steemit.com for example. This metastream is a public avatar constructed by averaging the topic interests of all public avatars. This acts as a starting point for new participants until they communicate their interests and content preferences more specifically. Different metastreams providers may have different perceptions of this public avatar. This metastream likely requires filtering because different participants have different language understanding capacities. Automatic language translation Service Cogs (ref Democratic Communication:Protocol Resolution:Sigil X Protocol) translation may solve some language barriers. The main problem with this stream is that by appealing to everyone on average, the stream appeals to nobody in specific. New participants are encouraged to express some of their interests so they don't have to use the M0 stream when starting on Zeronet (ZNET).

HTML Portals

This is a technical topic regarding "HTML". Early version of Netportal are expected to support HTML files. Operating systems are expected to have a "home

directory". Portal files as HTML are expected to be at [home directory]/Netportal/Portals/[Portal Name]. Portal names are expected to be plainly and briefly named according to what they accomplish. Portal files are expected to be named according to the author or publisher of the file followed by the the date. The date is expected to be as specific as the frequency of updates to the portal. So portals updated monthly would be named "MyPortal 2022 Jan", the next one "MyPortal 2022 Feb.", and so on. If an update is more frequent than originally planned the date can be made more specific such as "MyPortal 2022 Jan 28".

Companion Data

Theme

To use specific themes as CSS files, such as a theme named "My Theme" with a CSS file named "myTheme.css" the directory to use would be [home directory]/Netportal/Themes/My Theme/myTheme.css where "home directory" is the operating system directory where netportal files are expected to be located.

Default Values with Javascript

HTML elements may all have an identifier tag as the "id" element. These values are expected to be set by a Netportal-specific script using a text file for each id element. So if a form contained an element like "<input type="text" id="myFieldValue" value="seeking default...">" where "myFieldValue" is the name of a textbox id as an example, the directory to use for default values would be "[home directory]/Netportal/Portals/[Portal Name]/" where "home directory" is the operating system directory where netportal files are expected to be located. In that example "My Portal" is the name of the portal as an example. Then for this example, a file named "myFieldValue.txt" would be created in that directory. The default value would be the contents of that file. A Javascript script expected to be linked to for all HTML portals would then load the values from those files upon loading of the form to the participant’s browser.

Other Data

Other data associated with a specific portal may be images and special file data. All such data belongs in the "companion data" folder at ""[home directory]/Netportal/Portal/My Portal/My Portal Data/"

Zeronet Distribution Portal:

Summary

See Portals:Zeronet Distribution Portal:Summary section.

Setup and Distribution: Resource Trust Chain

New participants fully trust the participant who they obtain Zeronet (ZNET) software from, as expected be

shown in the Web of Trust Zeronet Resource Control (Zerco) upon installation. The participant they get software from first is a person they are trusting the most on Zeronet (ZNET) because that person includes Web of Trust information including recommended contact points for Service Cog Providers (Cog), Contact Discovery Providers (Cdisc) and Data Discovery and Synchronization (Disco) (see associated sections). Zeronet (ZNET) is expected to expand in a peer-to-peer way, especially by transfer of USB memory sticks. Each time someone is given access to a resource, that is a point of trust. This resource trust chain can be edited directly by the Zeronet Distribution Panel. If you are a reliable and trustworthy person and either have or know someone with technology expertise, please distribute Zeronet (ZNET) to your community so we can have trustworthy installations with those we care about. Reference Web of Trust:Perspective Development:Network Synchronization:Data Discovery and Synchronization Service for details about that service.

Setup and Distribution: Installation

The participants assigns specific device resources to Zeronet (ZNET). They may assign a different amount for personal usage (expected to be unlimited) and for shared usage (expected to be limited). Upon installation, the Zeronet Distribution Portal is expected to use Private Information Technology Resource Exchange (Pitrex) functionality to determine available computing resources and then automatically auction them on the open market according to participant preferences and settings. Available location data will be used to estimate the user’s electricity costs, which can then be changed by the participant. A prompt will ask the participant for energy cost information and whether they are willing to share that with the general public through their Data Negotiation Service provider (which keeps identities masked, see Web of Trust:Data Negotiation Service) as information associated with an avatar of their choice. This amount determines the profitability of the activation of Zeronet (ZNET) services for their system. Participants are expected be informed how much they can expect to receive without any further management activity that changes profitability.

Service Portal Trustee:

Peer Manager Portal

People sufficiently rated on their Web of Trust may act as trustee contracted peer managers. This is accomplished with the appropriate Netportal Settings Portal setting which will prompt the participant upon installation. After being granted Zeronet Distribution Portal (ref neighboring section) trustee status, they are granted control over available system resources for the purpose of reselling their resources using Private Information Technology Resource Exhange (Pitrex), or

alternative and therefore less supported means, in exchange for a percentage of the generated service revenues. A percentage such as 8 1/3% is given to this resource reseller. For charitable reasons it might be a low fee, and for entrepreneurial or other creative reasons it could be a high fee. Participants hand control over their Zeronet Distribution Portal to a Peer Manager, and this person most often manages their system for expansive wealth creation. This person is given remote access to all of extra system resources and therefore must be a trusted person on the Web of Trust.

Connection Manager Portal

As described in Democratic Communication: Zeronet Protocol, different content types are expected to be transferred using different protocols. The connection manager establishes and closes connections such as TOR connections, Bittorrent connections, Komodo connections, and direct peer connections according to the connections management settings. The connection manager sends and receives data according to each integrated protocol. The connection manager ensures VPN is used when specified. The connection manager continuously manages internet connections according to participant settings. A number of settings are encouraged for security purposes. For example, Bittorrent protocol traffic should only be sent over a VPN connection. If multiple connections are available simultaneously such as to merge available bandwidth, the connection manager portal may be used to distribute bandwidth over such connections according to the content type being transferred, both on an incoming and outgoing basis.

Installation Referral Reward

If the participant chooses to have their services managed automatically by a peer manager, the participant who suggested the peer manager is given a percentage of profits by the peer manager for the referral. A query to new participant determines who to relay this referral fee to, if anyone. A percentage which may be 9.6% of Pitrex management profits as determined and agreed by general consensus is expected to be relayed to referrers who help participants add Pitrex resources. Encouraging such a consensus-formed contract is encouraged to help reduce unfair personal contracts that could otherwise result. Referrers are expected to take a chunk of this funding flow according to the "golden spiral ratio", so that they receive 62% and then redistribute the other 38% to those who helped them refer others (the referrer of the referrer) which continues until reaching a minimal amount such as 2% of the referral revenues. All referral query options and decisions should be kept private with the participants involved including peer manager, referrer, and resource participant except as summary data unconnected to any specific people.

Peernet Competition

Zeronet (ZNET) uses a distributed peer-to-peer network

where each peer node operates under consent. Some compromised network nodes could have malware that consumes system resources without consent of participants, which reduces or eliminates the participants available resources. When such malware is installed, it is considered a "botnet infection". For this reason, an anti-malware cog is expected to scan the Zeronet Distribution Portal and optionally their entire computing environment for malware. System resources may be made available to specifically trustee participants as defined by the Web of Trust. Anti-malware service providers are granted access through participants Data Negotiation Service and  This service should only be activated when the Netportal Settings Portal is considered a secure environment.

Service Cog Menu

Service Cog Tree (COG)

Participants specify all Service Cogs (COG) to use. Each cog is linked to an Avatar identity which includes all needed contact details.

Advertising Strategy:

Netportal Advertising:

Personal Data Decentralization

Currently large centralized spy networks spy on everyone in an attempt to extract commercial value from those people. As detailed by Web of Trust:Data Negotiation Service, participants are expected to be in control over whether advertising is sent to them and if so, how it is sent. Zeronet (ZNET) participants are expected to regain control over their personal information.

Advertising Negotiations

Advertising on Zeronet (ZNET) is a negotiation among all participants involved involving multiple trust judgments of advertising information accuracy. Participants involved in advertising include marketers, ad exchange servicers, content creators, content distributors, content evaluators, and their Data Negotiation Service (ref Web of Trust:Data Negotiation Service). Because advertising is highly avoidable, there is honor in respecting fair advertising that supports a participant’s content creators, and dishonor in leeching content by suppressing all advertising. The negotiations are about what advertising is fair for participants to expect to interact with. Most participants are willing to interact with some advertising, but without them being an obnoxious distraction that overshadows the content itself.

Advertising Blocking and Filtering

Software developers, metastream providers and other content distribution channels are encouraged through social pressures to respect and uphold the advertising choices of content creators. Advertising that is considered socially acceptable to filter out is content that is delivered in unacceptable formats such as by hacks, interference with display, and output levels with

unacceptable volume characteristics including intermittent flashing. Any and all participants going beyond a general consensus of what is socially unacceptable to reduce advertising are expected to be centured(or scorned) and dishonored when such behavior is known. Content advertising leads to more content and sometimes higher quality content. While advertisers could negatively influence some content, some content may not be able to exist without advertising.

Traffic Reporting Accuracy

Participants are expected to use Public Data Traffic Reporting Cog (Trafcog) (ref Service Cog:Netportal Cogs:Public Data Traffic Reporting Cog) to help verify information accuracy and prevent advertising fraud.

Dynamic vs Embedded Advertising

Zeronet (ZNET) content sponsorship (differentiated in a nearby section against endorsements) is generally encouraged to be dynamic. Content creators are encouraged to leave placeholders in their content where the specific advertising delivered will depend on the participant receiving it. This is expected to result in higher revenues for content creators which in turn are expected to result in more content and higher quality content.

Advertising Roles:

Marketers

pay to have their content advertised on data content mediums or directly reviewed with direct marketing messages. A marketer chooses any number of other roles to interact with for purposes of advertising. Zeronet (ZNET) marketing options are expected to include ad exchangers, content creators, content distributors, content reviewers, content evaluators, and Data Negotiation Service Providers. Marketers are expected to be able to use the Open Exchange:Advertising Service Cog to purchase ads for any of these interactions. See Open Exchange:Standard Exchanges:Advertising Exchange for details.

Ad Exchangers and Agencies

help match advertisers with content on which they can place advertisements. The Advertising Exchange (Adex) (Ref Open Exchange:Standardized Exchanges:Advertising Exchange) is expected to reduce the expense of advertising brokers. Content review services are expected to provide sufficient information of what content best matches with which advertising, while the Advertising Exchange (Adex) is expected to provide the information system to make purchasing of such advertising efficient.

Content Review Service Cog

Reviewers may determine ethics and moral categorization of specific content for features such as the level of reproductive activity, gore, cussing, and any number of other moral, ethical, and cultural behaviors represented

in the content. Reviewers may determine characteristics of content to help match content to the best fitting audience and also determine which governments may censor the content by force. This information can be communicated by reviewers to the target audiences by methods including tagging (ref Netportal:Content Tagging) and certifications (ref Web of Trust:Assurance:Trust by Certification). Furthermore, the content review service collects information from the Data Exchange (Datex) (ref Open Exchange:Standardized Exchanges:Data Exchange) provided by Data Negotiation Service (ref Web of Trust:Data Negotiation Service) and also directly by individual participants to determine the demographics and characteristics of the audience of specific content. Advertisers seeking to influence social behavior of participants can filter in or out content based on the characteristics of the content beyond what is legal in their jurisdiction. Both Content Review Service Cogs and marketing participants are expected to report such filtering to a Data Negotiation Service Cog so that content creators may be aware of the type of content filtering that makes advertising more or less likely.

Content Creators

chose any number of advertising choices to integrate into their content. Content creators have a number of options that range in potential influence from minimal to maximum available. These options from minimum influence to maximum influence range from producing entirely from their creative instinct while rejecting even donations, to paid sponsorships. The general order of influence from least to most is donations rejected, donations accepted, personal endorsements, blinded sponsorship, and open sponsorship.

Donation Rejection The most radical option would be to reject all donations for the reason being that they could influence the type of content being produced to popular content, where the author may wish for popularity of content not to be a factor in deciding what to create.

Donations Only Content creators may find a great deal of creative freedom by accepting content creation reward only through donations. This eliminates commercial influence over their content.

Personal Endorsements Content creators may find specific appreciation for commercial offerings of some sort, and seek out such providers to advertise their offerings in exchange for funding. If a sponsor approaches a content creator before an endorsement is given, then the advertisement is a sponsorship rather than an endorsement. If an advertiser is hoping for an endorsement from a new content creator, it is suggested that they wait for a specific period of time such as three months. So, new content creators who want to advertise the best possible offerings may want to

endorse products from their start.

Sponsorship  Content creators may specifically designate parts of their content for sponsored advertising which funds their creative efforts. To minimize influence that sponsors have over content, they could set up their contracts as "blind sponsorship" in a way that they have little to no way of knowing who sponsors their content. Generally the highest bidder on the Advertising Exchange (ref Open Exchange:Standardized Exchanges:Data Exchange) will be the organization to sponsor the content.

Advertising Transparency

Content sponsorship type is expected to be made known to the content evaluators by content creators and relayed by any intermediaries so as to be transparent about the potential for commercial influence over content. This is done by announcing advertising as either an endorsement or a sponsorship.

Content Evaluators

The people who review, load, evaluate, or otherwise "consume" content are content evaluators. Content evaluators are expected to publish opportunity pricing for direct receipt of advertising from marketers, providing a direct route for marketers to communicate with their target audience. This is essentially a route to receive paid private messages (ref Democratic Communication:General Concepts:Private Messaging) as advertisements from marketers using postage, (ref Democratic Communication:General Concepts:Private Messaging:Postage) tokens (ref Token Pack), or a combination of both.

Data Negotiation Service Provider Advertising Role

Data Negotiation Service anonymizes the identity of a content evaluator for improved security and privacy. This service helps prevent "big data" monopolies and oligarchies from having an unfair advertising advantage over small businesses. See Web of Trust:Data Negotiation Service for additional details.

Netportal Security:

Network Device Security:

Collective Business vs. Personal Division

Those who can afford it are encouraged to use a separate device to connect with family and friends as they do to conduct business, contact organizations, or participate in an organization.

Software Firewall

We encourage the use of a software firewall for each operating system. Service Cogs (COG) may be developed such that they can provide such software more directly as Zeronet (ZNET) Service Cogs (COG) rather than installing a separate software. Until firewall Service Cogs (COG) are standard, a software firewall is expected to be included with Zeronet (ZNET) applications such as Netportal. Current software firewalls may break some

applications without informing the firewall user that the application is blocked. This unwanted behavior by firewalls is expected to be avoided.

Operating System Security Checks

Anti-virus and anti-malware efforts are the focus of operating system security checks. Operating system checks require full system access, so any operating system security Service Cog (COG) requires the highest level of trust for system access. Only after further development of Zeronet (ZNET) will such security be enabled. Anti-virus and anti-malware systems are expected to be incorporated to Netportal. Systems that automatically direct real-time streams of audio or video over the internet have higher security risks in doing so, and these risks should be communicated to senders. Risks include privacy breaches and display of harmful behaviors. When such streams are being sent, such status should be made obvious such as by a status icon on the device display and/or intermediate audio alerts. So, systems like Amazon Alexa and Apple Siri are expected to be replaced with more privacy respecting alternatives. Zeronet (ZNET) is strongly discouraged for any usage on insecure systems such as a Siri-enabled device or any device which records all voice activity for indefinite amounts of time.

Physical Security

Even if you are so generous that you openly give away all you have, your current items or possessions should be secure at all times. When you intentionally give something to someone expecting nothing in return, others will respect and appreciate your generosity, but there is no such respect for unintentionally giving away property. So, when you leave your possessions unattended, they should be locked down. When you leave your possessions attended, give each one of them attention of security.

Side Channel Security Auditing

For high security, all potential outbound data channels should be checked on an ongoing basis for data leaks. High security would require an advanced oscilloscope that directly checks Ethernet ports, an RF spectrum analyzer that checks wireless radio channels, and a microphone to check for sonic side channels. Because both wired and wireless full frequency spectrum analyzers are an expensive (such as USD $10,000) investment to cover all available spectrum, it is only feasible for large organizations. The scanned data is compared with expected data connections, with any unidentified data considered suspicious. Noise patterns are expected to be explored for possible data. Such wide spectrum analysis is a feature expected to be incorporated to most Zeronet (ZNET) devices to help eliminate the prolific voyer and spy networks that currently plague the internet.

Security Research Considerations

Side-channel attacks using rarely used parts of the electromagnetic (EM) and vibrational spectrums may be contemplated but unlikely to be cost effective to scan regularly. There are theoretical security risks based on WIMP (weakly interactive massive particles) and other particle emission channels which are also considered infeasible by requiring such machinery as particle accelerators. Malicious device configurations may also be able to be detected by unintended signals such as unexpected infrared emissions as the device needs more power than anticipated.

ZERONET PROPAGATION:

Summary

If others sometimes refer to you as a reliable or trustworthy person, and you either have or know someone with technology expertise to help, please distribute Zeronet (ZNET) to your community so we can have secure installations with those we care about. This is important for every aspect of security, especially privacy. You can also make attempts to audit Zeronet (ZNET) code or improve on the code if you consider yourself interested in technology.

Preferred Propagation

1 to 1 Direct Propagation. Participants directly share network access software with friends and family.

Direct Access Media: Paper, Memory Stick, Smartphone Link.

Participants may be encouraged to load their Zeronet (ZNET) media device such as a memory stick. In that case, USB Media is loaded with contact keys and a crosslink database (ref Information Graph:Network Synchronization:Crosslink Metacode for crosslinking explanation). QR codes are a convenient option as well.

Indirect Propagation

Occurs when two people have no direct contact. They find a participant to connect them together by providing two participants with a shareable encryption key for secure transfer of the Zeronet (ZNET) software.

Matchmaker Propagation

Participants are connected through a trusted third person or group. The local interest group selected as the matchmaker is expected to align as closely as possible in philosophy as the peers being connected.

Access Methods

Kiosk, Mail, Wireless Link, Internet

Startup Kit

Contains all Zeronet components and CrossLink database as formatted and modified according to the preferences of the distributor. Trust in the distribution source is essential to a successful startup.

Security Propagation Motive

The more systems that run Zeronet (ZNET) and its associated protocols like TOR, the more there is safety

in numbers. So, each participant is encouraged to increase secure protocols supporting values such as the freedom of speech to the majority of prospective devices or more such that for example most endpoints having ISP service have one or more Zeronet (ZNET) Service Cogs(COG) running.

Donation Wallets:
BTC 1KgT45YnhWKfVbnQmsadm934xpYCN9QWV4
BTCH qrg3ugzv028p5zxsvkrxrts36g9z0xs2hutswar3wy
DASH XmfCdNkRMiREi36XHJiirmV7HB6J2U6ao4
MNRO
41nqYooePgJRSo9CtWfVm7V7b6gBEhS528BBeAJRxfVjfC5igqokWgD6zjWd
WsyJGaP2Jd9JxiSMACfdqKueUNVnSFmyjv6
ETH 0xfb84b64df9283257e20eb4e4dd5c583f7bf3952d
LTC Ld7XZ5xAFH8WohoqeosjuQUVoKs4sivQgK

end