A NON-HIERARCHICAL BINARY MODULAR SYSTEM FOR THE ORGANISATION, STORAGE, DELIVERY AND MANAGEMENT OF CONTENT IN MULTIPLE LOCATABLE PRIVATE NETWORKS ON AN OVERARCHING PLATFORM

FIELD OF THE INVENTION

[1] The present invention relates to software applications for delivery, storage, organisation and management of electronic content in user constructed and infinitely expandable LPN's (Locatable Private Networks) and in particular to software applications for non-hierarchical delivery, modular organisation and management of content by multiple non-related persons acting without administrators or moderators.

[2] The invention has been developed primarily for use in methods and systems for a binary modular, self-searching platform for non-hierarchical electronic content delivery, organisation and management and will be described hereinafter with reference to this application. However, it will be appreciated that the invention is not limited to this particular field of use.

BACKGROUND

[3] Any discussion of the background art throughout the specification should in no way be considered as an admission that such background art is prior art nor that such background art is widely known or forms part of the common general knowledge in the field in Australia or worldwide.

[4] Known methods of electronic content delivery, organisation, storage and management in a computing environment are typically based on a hierarchical organisation and access-base model in which content is organised to a tree-like structure with access via an administrator. The electronic content in such known methods is stored as named records that are connected to one another through hierarchical links commonly known as folders. A record is a collection of fields with each field containing only one value. The entity type of a record defines which fields the record contains.

[5] Such hierarchical content-base models are preferentially suited to structured electronic content and become less useful as the content becomes semi–structured or unstructured content. Unstructured content refers to computerised information that does not

have a rigorous internal structure. Unstructured content can be found in, for example, emails, text messages, reports, presentations, phone notes, agendas and photographs. It is estimated that up to 80% of the content in the real world is unstructured in nature as is a large degree of the civilian communications using that content. Accordingly structured hierarchical content-base systems struggle to maintain the content in a manner that is coherent to all users and is easily managed and searchable by all users, all of the time. Such structured hierarchical systems usually have to negate almost all the needs of some users and some needs of all users, at the same time as satisfying most fully the needs of just one or a few appointed administrators who define all the parameters. For such a system to function, all users must adhere to the administrator's systems of ordering and purpose hence they are by definition hierarchical systems even when the level of hierarchical interaction is discernibly small.

[6] Typical content-base methods of a hierarchical nature force a structured hierarchy onto unstructured content or communications, which results in a less than efficient content storage, delivery and/or management system, particularly if efficiency is defined by the satisfaction of all users as to purpose, access, security, management and delivery.

[7] Accordingly there is a need for a communication method and content management, delivery and storage system able to adapt to and efficiently manage, deliver and store unstructured electronic content in a non-hierarchical manner that still enables the content to be regularly searched, shared and recalled as required by all users, all of the time.

SUMMARY

[8] It is an object of the present invention to overcome or ameliorate at least one more of the disadvantages of the prior art, or to provide a useful alternative.

[9] One arrangement provides a computer program product for providing a system as described herein.

[10] One arrangement provides a non-transitive carrier medium for carrying computer executable code that, when executed on a processor, causes the processor to provide a system as described herein.

[11] One arrangement provides a system configured for providing a system as described herein.

[12] According to a first aspect of the present invention, there is provided a non-hierarchical binary modular system for organisation, storage, delivery, and management of

electronic content in multiple Locatable Private Networks on an overarching Platform. The system may comprise at least two upload portal (ULPs) that may contain information of interest to at least one or a plurality of users. The upload portals (ULP) may each be of a binary compatibility with distinct and inter-related control mechanisms enabling a modular construction, by one or a plurality of users. The system may further comprise contact means between the users in respect of information of interest being a binary modular based omni-directional and private notification system for maintaining real-time interaction between users in respect of information of interest. The system may further comprise moderation means for the maintenance of Locatable Private Networks formed on the Platform being a binary modular based consensual self-moderation system for maintaining a logical purpose without site administrators or third-party moderators. The system may further comprise security means for the continued existence of Locatable Private Networks formed by users activating at least one ULP containing information of interest on the Platform being a binary modular based security system formed by binary locks attached to each individual ULP and activated by each individual user subscription to the Platform and each individual user activity on the Platform. The system may further comprise a filing means for the user only placement and retrieval of content by distinct hyperlink using a 3 dimensional point placement of all ULPs into a replicate-able multiple point n-dimensional 3D array, each multiple point 3D array having an 'n' reference that allows layering of said multiple point 3D arrays into each other, and each point position being designated by an n-dimensional nomenclature, to create a limitless, anonymous, non-administered, non-hierarchical compartmentalised and uncommon database. The filing means may be an n-dimensional 3D filing system comprising an anonymous n-dimensional 3D tag (a plurality of layers in the same virtual space designated by xyz@n). The anonymous n-dimensional 3D tag provides a direct hyperlink distinct to each and every ULP deposited within the filing system as the LNP's are randomly constructed by users, which negates the need to use a normal tree-like hierarchical filing system created by a normal sequential system. This n-dimensional 3D filing system is expandable in the n-dimension(s) being a direct individual hyperlinked filing system of limitless additional 3-dimensional file fields layered within the same virtual space as previous and future layers. The location of an LNP within an n-dimensional file area gives rise to its nomenclature as a Locatable Private Network containing files tagged only on the basis of a position uniquely referenced by a location/position of the form xyz@n. The virtual location of any particular unique LNP within the many layers of the n-dimensional file area space is also its actual visual position (as visualised in a user interface) as part of a whole and all its related positions

as searchable elements exclusive to distinct users within an LNP. Thus the particular LNP is accessible directly from any user's interface via a corresponding 3D visual representation of the file areas which are advantageously navigable and accessed using simple drag, tap and drag functions as would be appreciated by the skilled addressee.

[13] Preferably, the system further comprises computer program code means for an infinite n-dimensional 3D filing system enabling 'Locatable' Private Networks to be visually represented for instant user only access, placement and retrieval purposes, anonymous filing purposes, fractured encrypted filing purposes, visual interface purposes, all governed by the attachment of ULP to other relevant ULP in a logical user only controlled 3 dimensional sequence into an endlessly replicated (n-dimensional) multiple point 3D array file location with no hierarchical file path or file tree that could be hacked by an outside party.

[14] According to an arrangement of the first aspect, there is provided a non-hierarchical binary modular system for the organisation, storage, delivery and management of content in multiple Locatable Private Networks on an overarching Platform, the system comprising: at least two upload portals (ULPs) containing information of interest to at least one or a plurality of users, the at least two ULPs each being of a binary compatibility with distinct and inter-related control mechanisms enabling a binary and modular construction, by one or a plurality of users; connection means for the users to define a logical connection between the at least two modular ULPs being a Binary Modular Platform based self-searching system; contact means between the users in respect of information of interest being a Binary Modular Platform based omni-directional and private notification system for maintaining real-time interaction; moderation means for the maintenance of Locatable Private Networks formed on the Platform being a Binary Modular Platform based consensual self-moderation system for maintaining a logical purpose without site administrators or third-party moderators; security means for the continued existence of Locatable Private Networks formed by users activating at least one ULP containing information of interest on the Platform being a binary modular based security system formed by binary locks attached to each individual ULP and activated by each individual user subscription to the Platform; and filing means for the user only placement and retrieval of content by distinct hyperlink using a 3 dimensional point placement of all ULPs into a replicate-able multiple point n-dimensional 3D array, each multiple point 3D array having an 'n' reference that allows layering of said multiple point 3D arrays into each other, and each point position being designated by an acceptable n-dimensional nomenclature, to create a limitless, anonymous, non-administered, non-

hierarchical and compartmentalised data-base. The security means may further comprise adding a contact's username to a ULP the content of which they intend to thereby share. The binary locks may be slip-paired binary locks comprising a user's own password and a secret auto-generated password formed from that user's username by the platform.

[15] The ULP may be adapted to retain electronic content in multiple formats.

[16] The connection means may utilise a title associated with each ULP to enable a self-searching function to control dual purposes of assembly of person into Locatable Private Networks and the collection of the content contained within the ULPs of interest to each individual user for the purpose of group formation based on conceptual relevance only.

[17] The ULP may be one of a selection of two different types of ULP: an Origin ULP or a Related ULP for the purpose of assembling Locatable Private Networks. The two types of Binary Modular ULPs may be used to create large systems comprising connected ULP. The ULPs may be thought of as a Binary Modular depository of a selected content type containing content, which generally is linked to other, related, ULP by relevance to the depositors who have formed a group or association. The origin ULP may have the property of being able to be placed by a user in relation to a specific topic or subject matter and may generally serve as an anchor for any further ULPs (whether these are Origin ULPs, Related ULPs, or any combination of a plurality of Origin and Related ULPs logically connected to an initial Origin ULP as may be determined by a user or users of the system who have formed into a group via the self-search function inherent to all ULPs). These collections of ULPs that form an LNP are the means by which the communication channels are established within an LNP for the purpose of making available the content they contain to be retrieved in privacy and may be regarded as temporarily placed, permanently placed or semi-permanently placed as needs be for the purposes of a network, as they are not in themselves the communicated content. They are to the content as an envelope is to a letter in that by default setting, they are dumb to the actual content except in-so-far as to file size and data type. They may also, by deliberate configuration by a user, be made to reveal their content publicly in the form of several resolutions of thumbnail sized representations (icons) that may comprise a visual representation of the actual content, which may or may not make deliberately selected parts of a private network, publicly visible as needs be according to the users.

[18] The at least two ULPs may be selected from a ULP type comprising either an Origin ULP or a Related ULP. The Origin ULP may be adapted for storing content. The Related ULPs may be adapted for storing content of relevance to the Origin ULP.

[19] The system may further comprise a plurality of Related ULPs each comprising a logical connection to at least one or more Origin ULPs and/or to an associated Origin ULP. Each Origin ULP and each Related ULP may accommodate an associated title. The title may or may not be reflective of the type of content contained within the associated ULPs. Construction of a content collection may thereby be constructed in a Binary Modular manner where the content contained within the ULPs may not be searchable. The title of each of the ULPs may be searchable within the Platform.

[20] The system may further comprise a consensus based self-moderated system for the exclusion of irrelevant content from a group LPN.

[21] According to a second aspect of the invention, there is provided a computer program product having a computer readable medium having a computer program recorded therein for providing non-hierarchical binary modular system for delivery, organisation, delivery and management of content in multiple Locatable Private Networks on an overarching Platform. The computer program product may comprise computer program code means for at least two ULPs containing information of interest to at least one or a plurality of users, the at least two ULPs each being of a binary compatibility with distinct and inter-related control mechanisms enabling a modular like construction, by one or a plurality of users. The computer program product may further comprise computer program code means for connection means for the users to define a logical connection between the at least two modular ULPs being a binary modular based self-searching system. The computer program product may further comprise computer program code means of contact means between the users in respect of information of interest being a binary modular based omni-directional and private notification system for maintaining real-time interaction. The computer program product may further comprise computer program code means for moderation means for the maintenance of Locatable Private Networks formed on the Platform being a binary modular based consensual self-moderation system for maintaining a logical purpose without site administrators or third-party moderators. The computer program product may further comprise computer program code means for security means for the continued existence of Locatable Private Networks formed by users activating at least one ULP containing information of interest on the

Platform being a binary modular based security system formed by binary locks attached to each individual ULP and activated by each individual user subscription to the Platform.

[22] According to an arrangement of the second aspect, there is provided a computer program product having a computer readable medium having a computer program recorded therein for providing non-hierarchical binary modular system for organisation, delivery and management of content in multiple Locatable Private Networks on an overarching Platform the computer program product comprising: computer program code means for at least two ULPs containing information of interest to at least one or a plurality of users, the at least two ULPs each being of a binary compatibility with distinct and inter-related control mechanisms enabling a modular like construction, by one or a plurality of users; computer program code means for connection means for the users to define a logical connection between the at least two modular ULPs being a binary modular based self-searching system; computer program code means for contact means between the users in respect of information of interest being a binary modular based omni-directional and private notification system for maintaining real-time interaction; computer program code means for moderation means for the maintenance of Locatable Private Networks formed on the Platform being a binary modular based consensual self-moderation system for maintaining a logical purpose without site administrators or third-party moderators; and computer program code means for security means for the continued existence of Locatable Private Networks formed by users activating at least one ULP containing information of interest on the Platform being a binary modular based security system formed by binary passwords attached to each individual ULP and activated by each individual user subscription to the Platform.

[23] The ULPs may be adapted to retain electronic content in multiple formats. The notification system may be continuously adjustable, omni-directional and variably compartmentalised by virtue of the Binary Modular construction.

[24] The computer program product may further comprise computer program code means for providing a consensus based self-moderated system for removal of irrelevant content from the Binary Modular ULPs in their binary constructed format.

[25] The connection means may provide a logical connection between at least two users.

[26] According to a third aspect of the invention, there is provided a computer program for providing a non-hierarchical system for delivery, organisation and management of content. The program may comprise code for providing at least two ULPs containing information of

interest to at least one or a plurality of users. The ULPs may each be of a binary compatibility with distinct and inter-related control mechanisms enabling a modular like construction, by one or a plurality of users. The program may further comprise code for providing connection means for the user to define a logical connection between the at least two ULPs. The program may further comprise code for providing an omni-directional binary-based notification system for maintaining real-time interaction between users in respect of information of interest and relevance to the plurality of users in the subsequent Locatable Private Networks.

[27] According to an arrangement of the third aspect, there is provided a computer program for providing a non-hierarchical system for delivery, organisation and management of electronic content, the program comprising: code for providing at least two ULPs containing information of interest to at least one or a plurality of users, the ULPs each being of a modular binary compatibility with distinct and inter-related control mechanisms enabling a binary modular like construction, by one or a plurality of users; code for providing connection means (self-search system) for the users to collectively define a logical connection between the at least two ULPs and therefore between a plurality of users; and code for providing thereafter an omni-directional binary-based voluntary notification system for maintaining real-time interaction between users in respect of information of interest and relevance to the plurality of users in the subsequent Locatable Private Networks.

[28] The computer program may further comprise code for providing a consensus based self-moderated system for removal of irrelevant content from the Locatable Private Networks formed by a plurality of users assembling the binary ULPs in their modular constructed format.

[29] According to a fourth aspect of the invention, there is provided a computer program element comprising computer program code means to make a computer execute a procedure for providing a non-hierarchical system for delivery, organisation and management of electronic content. The program may comprise code means for providing at least two upload portals (ULPs) containing information of interest to at least one or a plurality of users. The ULPs may each be of a Binary compatibility with distinct and inter-related control mechanisms enabling a Modular construction, by one or a plurality of users. The program may further comprise code means for providing modular connection means for the user to define a logical connection between the at least two ULPs using titles. The program may further comprise code means for providing an omni-directional notification system for

maintaining real-time interaction between users in respect of information of interest and relevance to the plurality of users.

[30] According to an arrangement of the fourth aspect, there is provided a computer program element comprising computer program code means to make a computer execute a procedure for providing a non-hierarchical system for delivery, organisation and management of content, the program comprising: code means for providing at least two ULPs containing information of interest to at least one or a plurality of users, the ULPs each being of a Binary compatibility with distinct and inter-related control mechanisms enabling a Modular like construction, by one or a plurality of users; code means for providing modular connection means for the user to define a logical connection between the at least two ULPs using titles; and code means for providing an omni-directional notification system for maintaining real-time interaction between users in respect of information of interest and relevance to the plurality of users.

[31] The computer program element may further comprise code means for providing a consensus based self-moderated system for removal of irrelevant content from Locatable Private Networks using Binary ULPs in their modular constructed format. The consensus-based self-moderated system may be responsive to the plurality of users whether or not the consensus-based self-moderated system activated on a particular ULP is related to a ULP 'belonging' to any other user.

[32] According to a fifth aspect of the invention, there is provided a computer readable medium. The computer readable medium may have a program recorded thereon. The program may be configured to make a computer execute a procedure to provide a non-hierarchical system for delivery, organisation and management of content in multiple Locatable Private Networks on an overarching platform.

[33] According to a particular arrangement of the fifth aspect, there is provided a computer readable medium, having a program recorded thereon, where the program is configured to make a computer execute a procedure to provide a non-hierarchical system for delivery, organisation and management of content in multiple Locatable Private Networks on an overarching platform

[34] According to a sixth aspect of the invention, there is provided a security system for a computing environment. The security system may be formed from the binary modular construction of a ULP shared between at least 2 users and comprising at least 4 unique

content elements, at least 2 unique content elements being associated with each one of the at least 2 users and one's own password being sufficient for any one user to access their own content. The security system of 2 unique elements (binary password) associated with any one user being comprised of one self-elected password formed by that user and one secret robot generated password formed by the platform comprised of a 3 character extension to the username of each unique user. The security system of 4 unique elements on a single ULP being activated by the presence of both usernames concomitant with the intention of both parties to privately and securely share it's content, said content having been placed in the ULP by one of the parties who then invites the other party to share that content by adding the other parties username to their ULP.

[35] According to a particular arrangement of the sixth aspect, there is provided a security system for a computing environment, the security system being formed from the binary modular construction of a ULP shared between at least 2 users and comprising at least 4 unique content elements, at least 2 unique content elements being associated with each one of the at least 2 users and being sufficient for any one user to access their content. The security system is further enhanced by the 'origin' party inviting a plurality of users to share the content in a single ULP by adding each party's username to the ULP and thereby adding each party's binary passwords to the ULP thereby giving each user access to the ULP via their own self-elected password and enclosing the ULP against all others by a plurality of binary passwords with no limit to the number of binary passwords that may be attached to the ULP.

[36] The security system may be a Binary Modular security system. The Binary Modular security system may be an at least 2 half, binary code system with various unique codes in at least 6 parts of 3 slip-paired format or, at least 7 parts of 3 slip-paired format and universal verification code or, at least 4 parts of 2 slip paired format or, 5 parts of 2 slip paired format and a universal verification code.

[37] The Binary Modular security system may be adapted for a computing environment. The Binary Modular security system may be formed from the Modular construction of the binary ULPs shared between more than two users that each of the at least two unique content elements (slip pairs) associated with each user is added to the number of unique content elements associated with the binary security system when the plurality of user increases beyond two users. In this arrangement, every username in a contact list attached to a ULP, there may be an increase by two in the number of unique content elements locking the ULP

in the case of the at least four part code and three the number of unique content elements locking the ULP in the case of the at least six part code

[38] According to a seventh aspect of the invention, there is provided a Binary Modular based security system for a computing environment. The Binary Modular based security system may be formed from the modular construction of one or more binary ULPs shared between at least 2 users. The Binary Modular based security system may comprise at least 4 unique content elements. At least 2 unique content elements may be associated with each one of the at least 2 users. The binary modular based security system may further comprise a universal verification code.

[39] According to an arrangement of the sixth aspect, there is provided a binary modular based security system for a computing environment, the security system being formed from the binary construction of one or more binary upload portals (ULPs) shared between at least 2 users and comprising at least 4 unique content elements, at least 2 unique content elements being associated with each one of the at least 2 users, and a universal verification code..

[40] According to a seventh aspect (binary modular based mobile device messaging application), there is provided a binary modular security system for a computing environment, the binary modular security system being formed from the modular construction of the binary ULPs shared between at least 2 users and comprising at least 5 unique content elements, at least 2 unique content elements be associated with each one of the at least 2 users, and a universal verification code. The verification code may comprise a randomised code generated by a centralised processor associated with the system of the above aspects and from parts of which a daily encryption flip and skip code may be sourced (see Figure 9 for explanation of the flip and skip encryption regime).

[41] According to an arrangement of the seventh aspect, there is provided a binary modular security system for a computing environment. The binary modular security system may be formed from the modular construction of UPLs shared between at least 2 users. The binary modular security system may comprise at least 5 unique content elements. A least 2 unique content elements may be associated with each one of the at least 2 users, and a universal verification code. The verification code may comprise a randomised code generated by a centralised processor associated with the system of the above aspects in association with a user's email address for identification purposes, and from parts of which a daily encryption flip and skip code may be sourced.

[42] The at least 2 content elements associated with each of the at least 2 users may be selected from the group comprising: a user's own account access password, a user's username including a random auto generated 3 character extension provided by the Platform.

[43] According to an eighth aspect of the invention (Ultra-high binary security system), there is provided a binary modular security system for a computing environment. The binary modular security system may be formed from the modular construction of the ULPs shared between at least 2 users. The binary modular security system may comprise at least 7 unique content elements. At least 3 of the unique content elements may be associated with each one of the at least 2 users and a verification code may comprise a randomised code generated by a centralised processor associated with the system of the above aspects in association with a user's email address for identification purposes, and from parts of which a daily encryption flip and skip code may be sourced.

[44] According to an arrangement of the eighth aspect, there is provided a binary, modular security system for a computing environment, the binary, modular security system being formed from the modular construction of ULPs shared between at least 2 users and comprising at least 7 unique content elements, at least 3 unique content elements be associated with each one of the at least 2 users and a verification code may comprise a randomised code generated by a centralised processor associated with the system of the above aspects in association with a user's email address for identification purposes, and from parts of which a daily encryption flip and skip code may be sourced.

[45] The at least 3 content elements associated with each of the at least 2 users may be selected from the group comprising: a user's own account access password, a user's username including a randomly generated 3 character extension, a site-generated personally unique verification code. The personally unique verification code may comprise a randomised code generated by a centralised processor associated with the system of the above aspects and from which a daily encryption flip and skip code may be sourced.

[46] According to a ninth aspect of the invention, there is provided a relay solution computational arrangement using a modification of the binary modular system as disclosed in any one of the preceding aspects. The relay solution computational arrangement may comprise a notification system. The relay solution computational arrangement may further comprise a bi-polar ULP title system. The relay solution computational arrangement may

further comprise a self-search system adapted to accelerate the solving of complex mathematical problems.

[47] According to a particular arrangement of the ninth aspect, there is provided a relay solution computational arrangement using a modification of the binary modular system as claimed in any one of any one of the preceding aspects comprising a notification system; and a bi-polar ULP title system and a self-search system adapted to accelerate the solving of complex mathematical problems.

[48] Other aspects and arrangements are disclosed below.

BRIEF DESCRIPTION OF THE DRAWINGS

[49] Notwithstanding any other forms which may fall within the scope of the present invention, a preferred arrangement / preferred arrangements of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

[50] **Figures 1A, 1B and 1C** show a conceptual depiction of a non-hierarchical system for delivery, organisation and management (storage) of content as disclosed herein, namely the Binary Modular Document (BMDocument) formation sometimes described as a table, **Figure 1A** at a high level of zoom, **Figure 1B** at a medium level of zoom and **Figure 1C** at a low level of zoom;

[51] **Figures 2A** and **2B** show a conceptual depiction of the ULPs of the system of **Figure 1**, **Figure 7**, **Figure 8** and representative of the background activity of **Figure 10** and representative of the button activity of **Figures 4A** and **4B**, all comprising an assembly of Origin ULP and a Related ULP respectively as described herein;

[52] **Figure 3** shows a computing device adapted for methods and systems for a binary modular, self-searching platform for non-hierarchical content delivery, organisation and management (storage) of content;

[53] **Figures 4A** and **4B** show conceptual depictions of the Origin and Related ULP's particular features and control options respectively as described herein including a summary of the typical characteristics of each type of ULP in the Binary ULP system;

[54] **Figure 5A** shows a schematic depiction of the relationship links between Origin and Related ULPs;

[55] **Figures 5B** & **5C** show schematic depictions of the process by which many Origin and Related ULPs may be linked to form a complex platform. From this figure, it would be

readily appreciated by the skilled addressee that the Origin and Related ULPs may be linked together in a plurality of strings, tables and 3dimensional (3D) grids to form a complex string, table or 3 dimensional grid of ULPs;

[56] **Figure 6** shows a schematic depiction of a complex array of Origin and Related ULPs linked to form a complex platform in the form of a Table construction and indicating possible link routes within the Table construction. The Table is referred to in this document as a Binary Modular Document or BMDocument;

[57] **Figure 7** shows a schematic depiction of a complex array of Origin and Related ULPs linked by a plurality of users to form part of a complex Locatable Private Network in the form of a 3 dimensional construction and indicating possible link routes within the 3 dimensional constructions, and indicative of the organic relationship between tagged files within a Locatable Private Network. For clarity the illustration shows just one n-dimensional 3D file area and is indicative of only one dimension of the n-dimensional 3D array filing system which may have thousands or millions of such layers all in the same virtual position;

[58] **Figure 8** shows a hypothetical illustration of the background connections between locations within the complex array of Origin and Related ULPs linked to form part of a Locatable Private Network as shown by the User Experience Interface of the file area illustrated in **Figure 10**. **Figure 8** illustrates what areas of the n-dimensional file area are being accessed at **Figure 10** and represents only a fraction of an LNP file area;

[59] **Figure 9** shows the flip skip code through its permutations from a sender to a receiver within an LNP for the encryption of data transferred when a notification of a deposit in an existing ULP is accepted and opened. Because the encryption is occurring within an already secure private network there is no need for a matching key regime between parties. A single encryption key is sufficient for all parties sharing the same verification code from which the flip skip code is derived within a high secure network. Encryption here is to protect content at retrieval and deposit via the public hardware of the Internet where it may be intercepted by tapping the data stream and is in addition to current end to end encryption systems.

[60] **Figure 10** shows an example depiction of a visual interface **1000** adapted to show a file within an LNP of the form shown in the inset **1001** (i.e. a replication of **Figure 8)**, showing a fraction of the entire database with location of areas A, B and C indicative of close quarters retrieval of one's own ULP deposits and related ULP deposits close by in a shared LNP area. Files are located within in the LNP by three different levels of density in a n-

dimensional file area and how they relate to the visual interface where they are swiped across within a density layer (e.g. strings A, B & C) and swiped upwards to open at the top of the screen. Section **1003** shows a representation of the entire database with only one's own files visible and manipulatable with interface **1000** as, for example, bright coloured dots inside duller coloured conceptual area bands. Colour coding enables compartmentalisation of one's own files by one's own colour choices. One single dot represents a file location within a concept area and includes areas A, B and C within which one's own ULP's may appear several times or just once within the related area. A double tap action by the user is preferably used to open a single ULP deposit and a single tap action by the user used to close the ULP and revert to the default location interface of **Figure 10**. Single tapping any ULP in the interface screen is preferably used to immediately bring it to the top of the screen where double tapping will open it. Bringing any ULP to the top of the screen from any location will preferably populate areas A, B, and C with all related file areas and their corresponding file densities. The vertical bars with dots at the bottom of 'screen' represent the entire database as visible to a user where the bars and dots would be differing colours representing conceptual file areas and the dots would be brighter areas indicating the presence of a user's own files within the otherwise inaccessible file areas of the platforms database. The user as relating to a particular file subject would define the colour of a particular file on a user's own modular interface. The platform would only assign each ULP file location an n-dimensional file tag (xyz@n), particular files of which are then assigned a colour on the interface screen by the user. Although the bar and dot screen represents the entire database it will in fact only display the areas of the database where a user's own files are located.

[61] **Figure 11** shows a conceptualisation of the Wyrdom non-hierarchical systems disclosed in detail herein as applied to existing internet networks compared with a complementary conceptualisation of the current hierarchical state of the internet.

DEFINITIONS

[62] The following definitions are provided as general definitions and should in no way limit the scope of the present invention to those terms alone, but are put forth for a better understanding of the following description.

[63] Unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by those of ordinary skill in the art to which the invention belongs, except those included in the uncommon terms and definitions list provided below for

the purposes of the present invention. It will be further understood that terms used herein should be interpreted as having a meaning that is consistent with their meaning in the context of this specification and the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein. Furthermore, all definitions, as defined and used herein, should be understood to prevail over dictionary definitions, definitions in documents incorporated by reference, and/or ordinary meanings of the defined terms, unless there is doubt as to the meaning of a particular common term, in which case the common dictionary definition and/or common usage of the term will prevail. In the case where a concept as described herein has no previously existing terminology, the uncommon terms and definitions as defined herein in conjunction with any common usage of the term that is not in conflict with the uncommon definition will prevail.

[64] For the purposes of the present invention, the following terms are defined below.

TERMS AND DEFINITIONS OF UNCOMMON USAGE

[65] It will be appreciated that some of the terms here listed derive from the need to describe functions that have not previously been defined, as the functionality they describe has not previously existed or the new functionality described has not previously been ascribed to the commonly understood definition but is used because the previously understood definition has had applied to it a binary modular modification that extends the previously understood definition.

[66] *Users:* Refers to random and unrelated members of the public who may come together in net space by means of the non-hierarchical Binary Modular Platform. Users may also be referred to here as members of a Net based LPN, group or association. Users in this document does not refer to members of a closed network, VPN, institution, association, forum, website or other traditional hierarchically based hosted site where they are commonly interacting with the host in isolation to all other users of a site, or if they are interacting with other users are doing so only within the terms and conditions of access dictated by that host, including censorship, fixed interfaces and user shared commonly accessible databases.

[67] *Author:* refers to a person whose initial posting of an Origin ULP is considered within a conceptual group to be the main conceptual progenitor for which every other user has joined the relevant LPN regardless of subsequent postings by other users and especially as regards the Binary Modular Document formed by the mass content dump feature that translates a standard static document (such as an Excel table of manufacturers data) into the

core operability of an interactive supply chain network and therefore consists of a table of origin and related ULPs (**Figure 1a,b,c & 6**). All members of any other LPN could be considered to be authors of their own conceptually relevant content uploads attached to an initial document or any other part of a network and Author is therefore also an interchangeable term with User,

[68] *Locatable Private Network (LPN):* Refers to the network of random unrelated users who have formed a group or association on the Binary Modular Platform using the binary modular ULPs and whom, by virtue of the attributes of the binary modular Platform described herein, are interacting within a Locatable Private Network. Formation of an LPN can occur by the deposit by an Author of a BMDocument consisting of a large table of strings itself consisting of one Origin ULP and a fixed number of Related ULPs in strings replicated into tables to compartmentally contain all celled information in an original static document, or a single string of one Origin ULP and one or more Related ULP. An LPN is assembled on the n-dimensional 3D grid array filing system of the Binary Modular Platform and accessible over a public network, such as for example, the Internet, by any number of participants unrelated by hosted purpose or institution, controlled by no one other than the participants directly engaging 'peer-to-peer' for their own purposes, and accessing content in a voluntary manner unfettered to the hosted Binary Modular containment method. This is opposed to a browser based closed network with a definably limited number of participants related by hosted purpose and institution, controlled by administrator, moderator or hosted channel manager, and accessing content in a manner fixed and defined by the host in a singular containment method.

[69] The term Locatable Private Network (LPN), makes clear the difference between the non-hierarchical Binary Modular Platform disclosed herein and any other hierarchical network platform that may normally be associated with, for example, a Virtual Private Network (VPN) in that the binary modular platform supports private interactions between random users who have found each other on a publically accessible platform (also hence 'Locatable Private Network'). A VPN uses tunnelling protocols, point-to-point Wide Area Networks (WAN) and encryption and any group formed in a VPN whether on a single hosted site (e.g. Facebook) or a physically assembled WAN (e.g. multiple nationwide university campus connections), must be accessed by administered subscription only. A VPN cannot support random self-invited inclusions of members of the public from outside the VPN without compromising the internal privacy of the whole network. To access an LPN

supported on the binary modular platform does not require any further subscription process than the platform access itself as all ULPs in an LPN are secured independently of the platform security. Invitation into an LPN group and the LPN itself is not hierarchically controlled by platform administration or moderation. Subscription to join the platform is for the purpose of accessing the platform only. Locked and compartmentalised binary modular ULPs allow the creation of an infinite number of Locatable Private Networks on the platform by random members of the public and *can* therefore support further random inclusions of members of the public from outside the LPN's without compromising the internal privacy of any other areas of an LPN supported on the platform. Any such random inclusions of members of the public into an LPN that turn out to be undesirable for existing members of an LPN can be reversed immediately and totally by any user attached to the ULP in question by virtue of the compartmentalised construction of the LPNs using binary modular ULP, without affecting the privacy and security of any other associated ULPs.

[70] *Binary Modular:* Refers to a combination construction methodology that involves a blending together of (i) two distinct binary entities that by their nature are compatible and inseparable for the purposes of their continued existence and/or function and (ii) a modular construction method that requires modules that are by their nature compatible but *not* inseparable for the purposes of their assembly and reassembly into elements that are functionally greater than in their isolated condition. Binary Modular refers specifically to the Origin ULPs and the Related ULPs, which are designed and function as outlined directly above.

[71] The binary modular design of the ULPs on the platform is the unifying technique across the whole platform, in that the following non-hierarchical attributes of the platform are impossible without the compartmentalised binary modular construction method described above, i.e.:

(a) The uploading of all content to the platform is via the binary modular Up-Load Portals (ULPs) with the only time that a user will be entering any content in a non-hierarchical, non-binary modular method being the initial user's subscription process to become a member of the Platform and the regular entering of their verification codes in the case of the subscription only High Security version.

(b) The Omni-Directional Notification that allows the ability to create multiple layers of secure Intranet with highly nuanced directing of messages and content

within the same contact list of a Locatable Private Network with no moderated intervention or administrative oversight, is only possible in a binary modular system, due to the ability of binary modularity to allow each user to control their own infinite variability in the notification settings that is impossible in any hierarchical notification system controlled by an administrator.

(c) The Binary Password System that attaches binary passwords, one part controlled by the user and one part controlled by the platform, for all users to every single ULP thereby creating a publicly accessible but overarching platform secured Locatable Private Network with enormous flexibility of content management and no administrative oversight or moderated interference, which is only possible in a non-hierarchical binary modular system of compartmentalised ULP's.Note that throughout this document the use of the term 'password' denotes at least one or the other part, possibly even both parts, of the binary password system that may be made up of a minimum of two passwords in the case of a single user or 4 passwords in the case of two usernames on a single ULP or may be part of a multiple password regime of upwards of hundreds of passwords in the case of 50 plus usernames attached to a single ULP. Therefore 'password' in this document does not refer to one password as in a normal hierarchical single password access system.

(d) The Self-Search System that creates the ability for multiple unrelated users to join together into LPN according to concept and purpose, with no common database 'search of content' facility and no ability to impose an administrative oversight, is only possible if the interactive facility is composed of two compatible but distinct and separated entities for each user that 'find each other' in order to enable the users to come together by using the same modular system of binary modules with similar or same titles. It cannot function when there is only one interactive facility that is shared by all users as in almost all hierarchical systems, as this type of system relies on a common resource content database whereas the binary modular platform relies on having no common resource content database. The Self-Search System to create the Self-Moderated Locatable Private Networks is therefore only possible on a Binary Modular Platform as disclosed herein.

(e) The Consensus Based Self-Moderation system for eliminating irrelevant content from the LPN's is driven by all the users in LPN's on the platform being on an equal footing within the system and is only possible on a system using compartmentalised

and individually locked ULPs in a non-hierarchical Locatable Private Network. Such a non-hierarchical Locatable Private Network is impossible on any other type of hierarchically organised Platform or site as they all need some sort of administrator or moderator for the groups to function around a common resource database. Because there is no common resource database and therefore no hierarchical administrators or moderators, a Consensus Based Self-Moderated system that works by any user being able to autonomously unplug offensive ULPs from a modular based network is the only possible way for a non-hierarchical binary modular data organisation system to maintain function and purpose.

(f) The n-dimensional 3D filing system that relies on the automatic mapping of the modular construction placement of the binary ULPs in LPN's by random members of the public, to create the platform interface, the xyz@n tagged hyperlink non-hierarchical (treeless and pathless) content retrieval system, the virtual compartmentalised location of the Located Private Networks and parts thereof, the universal virtual 3D drag and tap file opening Interface system and the Establishment system for LNP continuity. All these things are impossible without the user-operated non-hierarchical n-dimensional 3D filing system, which in turn is impossible without the binary modular construction method of the ULPs as it, and all the above 3D features (a to f), is a direct result of the binary modular construction method of the ULPs.

[72] *ULP (Up Load Portal):* Refers to one or other of the binary modular elements, Origin ULP and Related ULP (formerly referred to as Start envelope and Other envelope or data packages), which are fundamental to the action of all other elements of the platform described herein and are critical to the purpose of making available, managing and storing content for multiple unrelated participants in an unlimited publically accessible Locatable Private Network on the non-hierarchical platform. A ULP does not refer to a webpage, node, website, folder, file or file tree, forum entry or any other traditional mode of content transfer or storage. A ULP contains a means of entering a title, which guides the Self-Search function of the platform enabling the introduction of like-minded users. A user of the Platform beginning or initiating an interaction with another user activates a ULP string by entering a definition term/s into an Origin ULP and Related ULPs, inserting any type of electronic content, making settings in either the Origin ULP or both Origin and Related ULPs and then posting the strung-together ULPs on the Platform. By posting any ULP into the Platform or

into an existing LPN the user is in effect plugging their ULP into the notification system of other ULPs in the system. At upload every distinct ULP is assigned an n-dimensional file location tag commensurate with its user assigned position in a LNP. This n-dimensional tag is anonymous, bears no relationship to the content or the title of a ULP, and forms a direct hyperlink to a ULP that can be shared with others.

[73] All ULPs at posting contain a minimum of two password locks comprised of the user's account access password and a platform-generated (i.e. automatically generated using a random number/character generator) password based on a secret 3 character inclusion into a user's username. The moment a string of ULPs made up of Origin ULP and Related ULP/s is posted to the site it is a live ULP string, which may or may not be searched by all other users by its titles and/or username. If searched, another user may request access by attaching their own Origin ULP to any of the Related ULPs in a string and may be granted access to the content of some or all the associated ULPs according to settings by the original poster of the searched ULP string and that user adding the requester's username to the relevant ULP contact list. As soon as a user grants access to another user (by adding their username to a ULP) the two users will form a group made of the contact details of their usernames being in a shared contact list. This group is now a Locatable Private Network, which can in turn be found by others via the self-search function.

[74] When the ULP/s are accessed and become shared ULPs by virtue of the shared usernames attached to them they become locked by at least four passwords comprised of both user's account access passwords and two platform generated password based on a secret 3 character inclusions into both user's usernames. As the LPN gains more members various different ULPs in a string gain more locks as they gain more usernames in the attached contact lists. As a ULP notification is activated between members of the LPN over a network communications medium, such as, for example, the Internet, it presents to any other third party, whether they are other members on the platform or as intercepted by a hacker from outside the Platform as a string of individually locked and titled folder-like entities. The appearance of the ULPs as locked entities with only a ULP self-search title visible on each ULP is in no way the equivalent to any other normally open-able 'folder' such as a zipped folder accessible simply by downloading and clicking to open. As the ULP is not an isolated folder or file tree of folders, is not relocatable and cannot be downloaded or otherwise adjustable by anyone other than the original user who placed it on the Platform, it is therefore not a common relocatable resource as a normal file folder would be considered.

[75] *Delivery of Content:* Refers to the transmission of content over the Internet between unrelated parties on the Platform using the locked binary modular ULPs in the resultant LPN; as opposed to the transmission of content over the Internet within a closed network of related parties or a VPN or the open transmission of unsecured content between any hosted net users. 'Delivery of content' in this document implies that the content, like a traditional sealed and addressed envelope, is sealed from and unreadable to anyone who is not the intended recipient within an associated LPN. In effect the ULP's themselves are not delivered, as they are semi-permanent entities in which content is deposited for retrieval by others. A notification goes to a user in the contact list that the content of a ULP has been changed and is now available by all users in the attached contact list for viewing or download. Upon retrieval the content is then transmitted over the Internet as a download or as a URL location for viewing, hence delivery of content, not delivery of ULPs.

[76] *Omni-directional Notification:* Refers to the multipliable application of notification settings made available by and integral to the binary modular system which allows for highly nuanced directional and discretionary capabilities open to every user and not normally associated with either open or closed hierarchical network systems. The notices are transmitted over the Internet within the Platform from distinct users to other distinct users in multiple directions within each Locatable Private Network formed on the non-hierarchical Binary Modular Platform for the purpose of notifying any other user within a same Locatable Private Network on the Platform they so choose to include in a notification schedule made up of multiple contact lists directly and individually associated with each distinct ULP. Every other user included in a notification schedule within a Locatable Private Network electing to either receive or not receive the notification, further controls such notices. This is in no way equivalent to a network broadcast or internal notification system, or external email notification system or RSS feed as in a normal hierarchical platform, website or forum which is dependent on or controlled by a network administrator otherwise known as a site administrator, or a forum moderator or a channel manager etc., in which the recipient has minimal or no control over the sending or receiving of such notices and the administrator or moderator or manager has unilateral control over the sending and receiving of such notices and the notice is generally sent from a single common database source to multiple destinations with limited or no rights of reply or rescind.

[77] *Consensus Based Self-Moderation* (Formerly referred to as Democratic Self-Moderation)*:* Refers to a manner of selection and removal of content from groups on the

binary modular Platform that involves a set percentage limit of participants within a group, incrementally arrived at, that actions a decision for the rest of the group when content is to be removed from the entire group LPN content collection. Self-Moderation therefore refers to a group of people moderating together their shared content collection by incremental consensus. It does not refer to any sort of banishment or removal or site exclusion and does not involve any unilateral decision by a single member of a group acting in isolation as per any administrator, moderator, channel manager or any other hierarchically appointed or created position within a group of otherwise unrelated people as is found in many hierarchically organised forums and websites. It does not refer to the complete removal of content from the Platform itself. It refers to the consensual exclusion from a group LPN of content in a ULP, which then may or may not remain on the Platform at the discretion of the excluded user who originally placed the ULP in an LPN on the Platform. Content so excluded from a group may or may not form into a new LPN of similar or relevant content at the discretion of the original uploaders of the previously excluded ULP. Content so excluded may or may not remain active at the discretion of the original user who placed it in the ULPs connected to their username. After a time period of inactivity a user will be automatically notified by the Platform that their ULPs may be removed entirely from the filing system due to inactivity, thereby clearing file space for other users. Until such time, a ULP removed from a group is simply 'unplugged' from the group notification system of its former LPN and is therefore invisible to the LPN it was excluded from, but otherwise remains on the Platform and as ULP belonging to a username is equally capable in terms of all other user-named ULPs of joining with or forming another LPN.

[78] *Self-Search Function:* Refers to the search that is activated from within the Platform by the titles that are assigned to each binary modular ULP placed by a user on the binary modular Platform and which are fundamental to the formation of groups and associations by unrelated persons in a non-hierarchical LPN. It does not refer to an internal search of a common resource database made on a website or search engine by a single user from their own browser which has no affect what-so-ever on any other user of a website or forum that the search is made. It is also in no way equivalent to a content search facility on a normal website or forum which is designed to find the content of documents (in the normal sense) or whole files from a common resource that is administered by hierarchical oversight of a site administrator, forum moderator or channel manager. The binary modular Platform has no unilateral site administrator, forum moderator or channel manager and so it cannot have any

commonly accessible content, and so it does not have any commonly used search facility because it has no common database.

[79] *Document or BMDocument (Binary Modular Document):* Refers, especially when discussing the consensual activity of a group, to a collection of ULPs understood to be the core collection of content originating from a single user/author and added to for a logical common purpose by the members of an LPN that has formed around the original core material. For example, this may be the case where LPNs that have formed around a manufacturer's parts and services lists or a social media group's 'favourite movies' list, etc. as the core reason for their existence. Because the 'Document' is modular in its assembled format it is possible for the members of a group with access to the Document to pull it apart and reassemble it as each of them see fit and to view it in different user interfaces according to their own individual preferences without altering the 'Document' as it appears to any other members of the group or interrupting the notification system settings attached to it by an original author or any subsequent recipients. Document therefore refers to a Binary Modular Document (or BMD) that has omni-directional and scalable networking functionality only possible on the Binary Modular Platform.

[80] *Slip Paired Binary Lock:* Refers to the action of the binary passwords on a ULP whereby the separate content elements comprising a complete lock on the ULP are made of password pairs derived from at least two users whose usernames appear in the contact list attached to the ULP. One half of a Binary lock is derived from either of the passwords of at least two users sharing a ULP. These code pairs are changed at similar but not the same time on either side of the binary lock based on the login times of the usernames, but at different rates in relation to the other code pairs attached to the ULPs which are based on the users own passwords, and in the case of the Ultra high security version the third code pair based on a unique verification code generated by the platform for each user. At any one time one half of a pair of passwords in relation to the other half of the pair on the same ULP is 'slipping behind' in the rate at which it is changing because a user's own password may change monthly to annually, a verification code may change weekly to monthly and a 3 character username extension may change hourly to daily. This 'slip-pairing' creates an enormous element of randomness to the password regime as a whole, thereby vastly reducing the window of time in which a hacker or brute force code breaker has to successfully crack all the password combinations on a single ULP. A hierarchical password regime that is normally changed only by habit of the user might afford a hacker or brute force code breaker several

months or even years to crack usually a single password. Due to the likely frequency of users logging in to the system thereby triggering a change to code pairs, a slip paired password regime as described above will afford only potential hackers with a very limited window of opportunity in which to crack a password pair to gain access to the secure areas of the system, typically, for example, a day at most or significantly less time, possibly on the scale of hours, to crack a minimum of four passwords because two of them are automatically changing at every user login and every username added to a contact list adds two more passwords to each ULP.

[81] Access by authorised warrant is not impossible. It requires the warrant to be served on the user and the user account on the Platform, in which case due to the binary modular construction of the Binary Lock system, only that user's account material would be accessible, not their recipient's material or more generally to other user's in the LPN's that a person under warrant may belong to. A user is only totally privy to their own material but shared material will require a warrant to be served on at least one party who is privy to shared content. That does not allow access to any other user's account, only to what that user has shared with the person affected by the warrant. Warranted or user-authorised access to the public version of the Platform LPN's can be granted by turning off the 3-character username extension to that unique username and retrieving the warranted user's password from the Platform subscriber data-base, if the user doesn't abide by a warrant to divulge that password themselves or the warrant is a covert warrant. Warranted access to the subscription only High Security version will require the consent of the subscription holder's head authority to turn off the warranted person's 3 character username extension, retrieval of the warranted person's password from the Platform data-base, and then the additional supply by the Platform to the legal authority of a specially issued unique verification code for the legal authorities to access that account. Under 'normal' political circumstances a court would never grant a general access warrant and no specific warrant can compromise the overall privacy of any other ULPs in any LPN's on the Platform.

[82] *N-Dimensional 3D Filing System (xyz@n):* Refers to the means of organising, managing and storing ULPs and LPN's on the Binary Modular Platform in a non-hierarchical manner. Normal hierarchical filing systems can use ordering and organising based on alphabetical placement, date of upload, date of update, file size or sort, name of uploaders and or recipients, but none of these systems is suitable on a non-hierarchical Platform. The content of the Platform is completely private even from the Platform itself and the Locatable

Private Networks by definition are absolutely private. There is therefore no common database, no hierarchical classifications, designations or upload facilities, no common administrator and no way of having usernames attached to the content other than for user defined notification purposes. Therefore the only file system possible on a non-hierarchical Binary Modular Platform has to be a system based on a relationship of user only placement within a field of conceptual relevance to which only the users have access to their own and similar content, which dictates a 3-Dimensional grid array that uses the 3D position as an anonymous hyperlinked tag on the shared ULPs attached by the platform at placement by the users. To use a single 3 dimensional axis grid with limitless axis, (rather than limitless n-dimensional layers of fixed 3D axis locations) would create a file system based on the assignment of anonymous sequential file numbers and would therefore become a hierarchical file path and would reveal the location of files by identifiable user placement based on sequence and would therefore not be compartmentally private. This n-dimensional embodiment however provides visual location for the fixed interface purposes while providing a limitless non-hierarchical file system in the background to the interface because a normal 3D axis (xyz) has a maximum of 6 consecutive placements around a conceptually relevant ULP whereas an n-dimensional 3D axis (xyz@n) is completely limitless. These xyz@n position tags are attached to each ULP as it is uploaded and cannot bear any relationship to the content of those ULPs or the usernames or titles attached to them. It can only bear relationship to the position at which a ULP is attached to other ULPs based on the users individual conceptual reasoning's only, which in turn is based on the titles they use, the fields of relevance and the acceptance of invitations to remain attached to other related ULPs. An n-dimensional 3D axis (xyz@n) makes it possible to compartmentalise the database to maintain user privacy so that users and only users can build their own databases inside the main database using the binary ULP modules, and modularize the user interface operability, as well as centralise all the user separated databases for overall platform management purposes.

[83] Every attachment of a unique ULP into an LPN is therefore located on a virtual n-dimensional axis position in direct 3D relationship to its associated ULP postings within a specific LPN and more broadly within a shared conceptual area defined by that part of the n-dimensional axis grid. The positions can be represented visually on a 3D axis represented by for example 3 planes of 10,000 units left to right (x), 1000 units top to bottom (y) and 100 units front to back (z), making, for example, a one-billion point positions per axis grid area.

[84] These example one billion point positions may be vertically divided into roughly 100 general subject areas left to right, graduated into transitioning volumes of subject according to usage fluctuations and each assigned a colour on a standard spectrum with every ten positions in each x, y plane assigned a single pixel giving a long narrow slit of pulsating and moving colour at the bottom of an example interface screen. Over time the fluctuations of subject volume will largely settle to roughly consistent amounts and these roughly consistent volumes on an n-dimensional grid will be filled as axis positions next to and surrounding other ULPs on the same layer or corresponding layers of grid positions as described below.

[85] N-Dimensional refers to the 1 billion-grid area being infinitely replicable in the same virtual position as the grid onto which it is layered previously and into the future. As each conceptual area of a one billion point 3D axis grid fills, a new 3D grid position will appear in exactly the same place but will have the designation of a new n-dimension group of one billion. For example xyz@1, xyz@2, xyz@-40 etc. ad-infinitum in both negative and positive directions. Each new 3D grid position will slightly intensify the colour in that area representing the amount of activity within that conceptual area. As ULP are unplugged from an LPN by the consensus moderation system the colour intensity will diminish, as new ULP are placed the colour intensity will increase. As point positions become available via the deletion of redundant ULPs due to unused irrelevant content its position can be assigned to new ULPs in the same proximity even if the relevant LPN is on a numerically distant 3D grid layer to the newly available position. This ability to keep adding ULPs to an LPN by filling n-dimensional layers of 3D axis grids that are 'virtually' in the same position even as they may be numerically separated by multiple layers enables a limitless size for the same conceptual file position in virtual 'space' and enables every single ULP deposit to be directly hyperlinked without any form of hierarchical file tree system being in either the LNP database inside the platform's own databases or external cloud based databases potentially used as external storage. This ability to pack the same visual and virtual 3D position with multiple tagged ULPs overcomes the inherent problem of hierarchical filing systems that must have a single value for each file with numerous folders within folders that must be clicked through to both open and close any particular file, and therefore must at some point become too burdensome in the length of the file path to reach a desired file within a typical file tree. For a typical user, their own content is visible only as a point of colour to which they can associate meaning due to its 'conceptual' position and corresponding colour and all their files are therefore instantly accessible at any time no matter how deeply within the n-

dimensional layers of 3D axis they are placed. No matter how many 3D axis layers have built up over the lifetime of an LPN a user's content is always visible as highlighted points amongst a constellation of relevance with no reference to a hierarchical sequence of placement that would disrupt it's conceptual position. Regardless of the actual file densities during placement and the rates of change in densities over the life of all LNPs across the total database, everyone's own files will always appear be in the same virtual position further augmenting the colour coded file recognition for the modular user interfaces.

[86] The only commonality of the n-dimensional file system is in visually being the common storage and retrieval area for all Locatable Private Networks on the Platform even though as a whole it is not commonly accessible and the only distinct ULP to which a user has access by virtue of their username can be retrieved. Therefore all the colour changes visible to any one user only need to be based on the user's own account, LPN activities and modular interface choices, and does not relate to any other users on the platform, who's ULP's can simply be greyed out. Because it is not a common resource database it is a point position file locator based on relevance within an LPN that is retrievable and locatable instantly for any particular member of an LPN and it's only 'common' aspect is to provide a visual cue to the existence of other relevant material which users may request access to or may already have access to by virtue of the LPN they're a member in. By virtue of the binary modular construction method of joining one's own ULPs to other ULPs one's own activity always has a distinct 3D axis relationship to any other relevant ULPs within a LPN. This means there is no need to assign colour coding to anyone else's ULP in the virtual n-dimensional file field since to find other relevant ULP's means locating one's own in any case.

[87] The visual representation of the n-dimensional 3D axes will enable users to note areas of greater and lesser activity as the constellation of concept is navigated but will enable with a single drag in that area, to the top of screen, to take the user to the ULPs associated with their own content at that axis position and their own associated ULPs. Each of the xyz@n positions assigned to a ULP will be the hyperlinked tag of that particular ULP and can be used by the Platform to retrieve the ULP from storage in the cloud the moment it is touched upon by a user.

[88] Before a ULP is placed in the n-dimensional 3D grid by a user, it has only one username attached to it and no active notification settings and therefore does not need an axis position. It therefore can reside in an undesignated state accessible and visible only to that

user in a virtual 'foyer' prior to placement in the Platform database where it can be checked for malware etc. As soon as the user attaches it to another ULP in a LPN in anticipation of their request to join being accepted, it becomes a designated file with an n-dimensional 3D axis position tag.

[89] The n-dimensional 3D axis filing system enables the following features on the Platform:

A. Visual retrieval by any user of their own content as their ULP is assigned an n-dimensional 3D axis position and an n-dimensional 3D axis tag both associated only with the neighbouring ULPs in that concept area they joined. Within the constellation of an n-dimensional 3D grid positions only their own files are visible to them as more intense points of colour within the general colour field of the LPN they are a member of. This allows a simple visual cue of the entire conceptual database to enable location of a user's own files and their own LPN's only, at the same time as enabling a user to wander through other file areas of interest where they can see titles, usernames and may see thumbnails of content if allowed by those users, without compromising anyone else's privacy or content in any way and with no access what-so-ever to the entirety of the database. The n-dimensional 3D axis grid system creates the three following methods of file retrieval for any user.

B. The pathways of logical connections formed between ULPs in an LPN as mapped in a limitless n-dimensional 3D axis grid formed by ULP placements by 'plugin'. It is this pathway that allows a user to send and receive notifications from all ULPs within an LPN, and to no other LPN, as they are all connected to each other by 'plugin'. Access to the notification system of any LPN for a member is not possible until the system has tagged that ULP as to its distinct conceptual relationship to other ULPs of same or similar concept in the same LPN with commensurate n-dimensional 3D axis positions.

C. Point positions in the n-dimensional 3D axis grid are accessible at any point with drag and tap of random or particular ULPs to bring them into view, in and out of the grid constellation formed by the virtual 3D representation of the entire platform's tagged database. It should be noted that the representation is not of (and does not have to be) the actual entire database but only a thin skin of active ULPs associated with each users own account activity backgrounded by an algorithmic statistical representation of the entire database. Even so, the statistical representation area not directly

associated with a users own account can be accessible by dragging in an area of interest and bringing forth the closest ULPs and their LPN's for inspection as they appear in the UX interface due to the proximity of the user's own account activity to associated concepts around them.

D. N-dimensional 3D grid axis file tags of ULPs are based directly and solely on the ULPs n-dimensional 3D axis position number and can be sent as hyperlinks simply containing the tag as the retrieval code, to other users via internal notification or external email but a receiver cannot access the content unless their username is in the ULP contact list associated with the hyperlink. This enables the location of any ULPs in an LPN to be shared by any user with any other user or external non-user with the intention of expanding an LPN membership without compromising the privacy of any other member. Because the tag is anonymous, bears no relationship to the content of a ULP, links only to that ULP deposit and only invites the recipient onto that sole ULP's contact list, the sharing of any material on the Platform is possible without compromising the internal security of anyone else's user accounts in the rest of an LPN or the Platform database.

E. The n-dimensional 3D system enables the interface to be designed around a fixed area of virtual file locations that can be divided up into a manageable number of conceptual areas. For the purposes of the current example of a billion point file position, the screen can easily represent a 1000 across and 100 high (see **Figure 10**) which can be divided into around hundred areas of conceptual relevance, each with conceptually related xyz coordinates and each assigned a colour which the user will associate with the content they know they have placed into ULP at various locations. The ability to layer many new 3D layers onto the same xyz location enables an infinitely expandable and numerically adjustable file system that can accommodate the consensus based moderation system of eliminating irrelevant content and a standardised fixed 3D touch screen interface to represent it individually for each user access. Since it isn't a commonly accessible database n-dimensionality enables every file location for every user to be compartmentalised per user interface without needing to actually represent every file in existence to every user. A non-hierarchical system must accommodate at the same time the platform's need for a coherent file system based on conceptualised relevance that is coded with anonymous 3d axis hyperlink

tags controlled by users but managed by the platform, and the needs of the users to maintain compartmentalised privacy.

[90] This system of file storage & retrieval using anonymous n-dimensional file tags also has implications for the security system. Because the tag is based only on a 3D axis location and not the content at that location, it allows the relevant ULP to be fragmented into multiple storage places in the cloud for extra security. A hyperlink can be made to link with many different locations without replicating the entire content of a ULP, as the hyperlink relates only to a single fractured ULP, not its entire content. This allows the content to be divided into numerous fractured parts filed on different servers all with the same tag meaning an attack on any particular server may reveal only part of a deposited file the discovery of which reveals nothing about the location of the other parts of that tagged file since chasing the various fractured hyperlinks involves first breaking into the Platform database to find their various locations from a unified hyperlink stored only in the platform database. Therefore the file system, being completely anonymous and fractural, is a backup system to the binary modular password security system of the LPN's. This fractural file storage ability allows the Platform to offer ultra-high security services with cloud-based storage, as opposed to mildly secure storage on separate but dedicated secure servers.

[91] The n-dimensional 3D axis filing system forms the basis of the establishment procedure for maintaining an LPN in perpetuity as desired by its members. This establishment procedure is a voluntary procedure undertaken by all members of an LPN wishing to establish their group on a more permanent basis than the standard consensus based self-moderation system will allow for. The procedure involves the members of an LPN agreeing to isolate a core constituency of ULPs from the consensus based self-moderation system thereby 'Establishing' the whole LPN against a possible eventual shifting from an original conceptual purpose. The core, of not necessarily more than 5% of an LPN membership as decided by consensus of at least 50% of the group, will by its established existence perpetuate the surrounding LPN that can then continue and expand as described above. This procedure may have a fee attached to the establishment of the core file area elected for establishment, as it is in effect an undertaking by the Platform to archive that core area on behalf of the LPN by turning off the ability of those ULPs to be unplugged from the LPN. The establishment procedure may, in effect, create virtual, if not actual, online real estate as the n-dimensional 3D axis positions covered by an establishment procedure represent an 'authorised' conceptual location that can be on-sold by the LPN group that

purchase it if they wished at some stage to devolve themselves from the responsibility of maintaining the LPN and the LPN has by such time gained a value worth maintaining or selling to the general or potential membership. Note that this procedure is unrelated to and is not the same as purchasing or selling a domain name since a domain name has a value associated only with the branding of a particular website or business address, not a consensus based establishment of real authority within an LPN on a global Platform that may have and/or represent an actual income within an established authority in a consensual LPN.

Further Definitions

[92] The articles "a" and "an" are used herein to refer to one or to more than one (i.e. to at least one) of the grammatical object of the article. By way of example, "an element" refers to one element or more than one element.

[93] The term "about" is used herein to refer to quantities that vary by as much as 30%, preferably by as much as 20%, and more preferably by as much as 10% to a reference quantity. The use of the word 'about' to qualify a number is merely an express indication that the number is not to be construed as a precise value.

[94] Throughout this specification, unless the context requires otherwise, the words "comprise", "comprises" and "comprising" will be understood to imply the inclusion of a stated step or element or group of steps or elements but not the exclusion of any other step or element or group of steps or elements.

[95] Any one of the terms: "including" or "which includes" or "that includes" as used herein is also an open term that also means including at least the elements/features that follow the term, but not excluding others. Thus, "including" is synonymous with and means "comprising".

[96] The term, "real-time", for example "displaying real-time notification," refers to the display of the notification content without intentional delay, given the processing limitations of the system and the time required to accurately process and direct the notification content.

[97] The term. "near-real-time", for example "obtaining real-time or near-real-time content" refers to the obtaining of content either without intentional delay ("real-time") or as close to real-time as practically possible (i.e. with a small, but minimal, amount of delay whether intentional or not within the constraints and processing limitations of the of the system for obtaining and recording or transmitting the content.

[98] Although any methods and materials similar or equivalent to those described herein can be used in the practice or testing of the present invention, preferred methods and materials are described. It will be appreciated that the methods, apparatus and systems described herein may be implemented in a variety of ways and for a variety of purposes. The descriptions here are by way of example only.

[99] As used herein, the term "exemplary" is used in the sense of providing examples, as opposed to indicating quality. That is, an "exemplary arrangement" is an arrangement provided as an example, as opposed to necessarily being an arrangement of exemplary quality for example serving as a desirable model or representing the best of its kind.

[100] The various methods or processes outlined herein may be coded as software that is executable on one or more processors that employ any one of a variety of operating systems or platforms. Additionally, such software may be written using any of a number of suitable programming languages and/or programming or scripting tools, and also may be compiled as executable machine language code or intermediate code that is executed on a framework or virtual machine.

[101] In this respect, various inventive concepts may be embodied as a computer readable storage medium (or multiple computer readable storage media) (e.g., a computer memory, one or more floppy discs, compact discs, optical discs, magnetic tapes, flash memories, circuit configurations in Field Programmable Gate Arrays or other semiconductor devices, or other non-transitory medium or tangible computer storage medium) encoded with one or more programs that, when executed on one or more computers or other processors, perform methods that implement the various arrangements of the invention discussed above. The computer readable medium or media can be transportable, such that the program or programs stored thereon can be loaded onto one or more different computers or other processors to implement various aspects of the present invention as discussed above.

[102] The terms "program" or "software" are used herein in a generic sense to refer to any type of computer code or set of computer-executable instructions that can be employed to program a computer or other processor to implement various aspects of arrangements as discussed above. Additionally, it should be appreciated that according to one aspect of the fundamental binary modular construction of the platform, one or more computer programs that when executed perform methods of the present invention will not reside on a single

computer or processor, but must be distributed in a modular fashion amongst any number of different computers or processors to implement various aspects of the present invention.

[103] Computer-executable instructions may be in many forms, such as program modules, executed by one or more computers or other devices. Generally, program modules include routines, programs, objects, components, content structures, etc. that perform particular tasks or implement particular abstract content types. Typically the functionality of the program modules may be combined or distributed as desired in various embodiments/arrangements.

[104] Also, content structures may be stored in computer-readable media in one suitable form. For simplicity of illustration, content structures may be shown to have fields that are related through 2 dimensional location in the content structure but is based on or derived from a 3 dimensional array as is found in common drafting software and which forms the basis of the tagged filing system for storage and management of the content of the Platform and forms the basis of the default user interface of the Platform. Such relationships may likewise be achieved by assigning storage for the fields with locations in a computer-readable medium that convey relationship between the fields of ULPs and each ULP. However, any suitable mechanism may be used to establish a relationship between information in fields of a content structure, including through the use of pointers, tags or other mechanisms that establish relationship between content elements.

[105] Also, various inventive concepts may be embodied as one or more methods, of which an example has been provided. The acts performed as part of the method may be ordered in any suitable way. Accordingly, embodiments/arrangements may be constructed in which acts are performed in an order different than illustrated, which may include performing some acts simultaneously, even though shown as sequential acts in illustrative embodiments or arrangements.

[106] The phrase "and/or," as used herein in the specification and in the claims, especially as it applies to the binary modular construction method of Locatable Private Networks on this Platform, should be understood to mean "either or both" of the elements so conjoined, i.e., elements that are conjunctively present in some cases and disjunctively present in other cases. Multiple elements listed with "and/or" should be construed in the same fashion, i.e., "one or more" of the elements so conjoined. Other elements may optionally be present other than the elements specifically identified by the "and/or" clause, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, a reference to "A and/or B,

when used in conjunction with open-ended language such as "comprising" can refer, in one embodiment/arrangement, to A only (optionally including elements other than B); in another embodiment/arrangement, to B only (optionally including elements other than A); in yet another embodiment/arrangement, to both A and B (optionally including other elements); etc. For clarity it shall be appreciated that, in terms of the Binary Modular construction of a Locatable Private Network by a plurality of users using ULPs on the Platform, that an Origin ULP may be placed on its own as an initial origin point for the creation of an LPN or the joining of an LPN by an individual user, but that a Related ULP cannot be placed unless it directly follows the placement of an Origin ULP.

[107] As used herein in the specification and in the claims, "or" should be understood to have the same meaning as "and/or" as defined above. For example, when separating items in a list, "or" or "and/or" shall be interpreted as being inclusive, i.e., the inclusion of at least one, but also including more than one, of a number or list of elements, and, optionally, additional unlisted items. Only terms clearly indicated to the contrary, such as "only one of" or "exactly one of," or, when used in the claims, "consisting of" will refer to the inclusion of exactly one element of a number or list of elements. In general, the term "or" as used herein shall only be interpreted as indicating exclusive alternatives (i.e. "one or the other but not both") when preceded by terms of exclusivity, such as "either," "one of," "only one of," or "exactly one of." "Consisting essentially of," when used in the claims, shall have its ordinary meaning as used in the field of patent law.

[108] As used herein in the specification and in the claims, the phrase "at least one," in reference to a list of one or more elements, especially as it applies to the binary modular construction method of Locatable Private Networks on this Platform as disclosed herein, should be understood to mean at least one element selected from any one or more of the elements in the list of elements, but not necessarily including at least one of each and every element specifically listed within the list of elements and not excluding any combinations of elements in the list of elements. This definition also allows that elements may optionally be present other than the elements specifically identified within the list of elements to which the phrase "at least one" refers, whether related or unrelated to those elements specifically identified. Thus, as a non-limiting example, "at least one of A and B" (or, equivalently, "at least one of A or B," or, equivalently "at least one of A and/or B") can refer, in one embodiment/arrangement, to at least one, optionally including more than one, A, with no B present (and optionally including elements other than B) but *not* in another

embodiment/arrangement, to at least one, optionally including more than one, B, with no A present; in yet another embodiment/arrangement, to at least one, optionally including more than one, A, and at least one, optionally including more than one, B (and optionally including no other elements); etc.

[109] It should be noted of the systems disclosed herein that the Binary Modular network construction system has as an essential progenitor of Locatable Private Networks the initial placement of an Origin ULP and subsequent placement of Related ULP or Origin ULPs. As the terms imply, the Origin ULP contains the instructions for the more nuanced subsequent notification and media controls of its Related ULPs. This does not limit the further placement of new Origin ULPs or their Related ULPs within the same string or LPN. In any string of Origin ULPs and Related ULPs no matter how long and convoluted, the first initial placement by any user must be an Origin ULP. A Related ULP by definition cannot precede an Origin ULP unless it is NOT directly related by author. This feature allows a single user to construct multiple contact lists within the same LPN and thereby allows for the creation of multilayered highly secure Intra-networks using the same names in authoritatively separated contact lists within the same organisational LPN. Normally such Intranets are currently associated with Internet-separated secure-server systems, which the Binary Modular system makes redundant because only one Internet connected server is necessary to use the much more secure binary modular system.

[110] In the claims, as well as in the summary above and the description below, all transitional phrases such as “comprising,” “including,” “carrying,” “having,” “containing,” “involving,” “holding,” “composed of,” and the like are to be understood to be open-ended, i.e., to mean “including but not limited to”. Only the transitional phrases “consisting of” and “consisting essentially of” alone shall be closed or semi-closed transitional phrases, respectively.

[111] For the purpose of this specification, where method steps are described in sequence, the sequence does not necessarily mean that the steps are to be carried out in chronological order in that sequence, unless there is no other logical manner of interpreting the sequence.

[112] In addition, where features or aspects of the invention are described in terms of Markush groups, those skilled in the art will recognise that the invention is also thereby described in terms of any individual member or subgroup of members of the Markush group.

DETAILED DESCRIPTION

[113] It should be noted in the following description that like or the same reference numerals in different embodiments/arrangements denote the same or similar features.

[114] Described herein there is provided a non-hierarchical system **100** shown conceptually in **Figures 1** to **10** for non- hierarchical organisation, delivery and management of content between unrelated individuals over a communications network, such as, for example the Internet, in a multitude of Locatable Private Networks. The system **100** comprises an Omni-Directional voluntary notification and self-searching system for maintaining real-time interaction between users in respect of information of interest. The system **100** further comprises at least two content upload portals (ULPs) **101** comprising information of interest to at least one user; connection means **102** for the user to define a logical connection between the at least two ULPs, the binary modular elements shared between the at least two ULPs, enabling the Omni-Directional voluntary notification system; and the title elements on each ULP enabling the self-searching system for logical group formation.

Why does the Internet need a Binary Modular Platform?

[115] The three foundation techniques of the Internet are the creation of bytes using the binary system of 1 and 0, packet switching of the byte streams, and Hosts (instead of routers), being assigned responsibility for the security and transmission reliability of packet switching, that is, decentralised security. The Internet itself, not including node software such as hosts and your own browser, is mostly electronic hardware that carries and routes data in the form of 'bytes' according to 'packet switching' set by software on 'hosts'. Incidentally these three foundation techniques are almost the only non-hierarchical features of the Internet.

[116] These founding principals were all well-established features of computer networks within the 20 years from 1963 when network computing was still on drawing boards and Jan 1st 1983, the official birth date of the Internet, when all the old separate private networks that had built up in that time switched over to the global standard TCP/IP Internet protocol to create the 'network of networks' we know today.

[117] This legacy system overall is now indispensable but as historian and critic Hans Ulrich Oberist recently said with a touch of regret:

[118] "The invention of the Internet once promised to make knowledge open and accessible to anyone across the world, a perfect, radically open tool that encouraged the sharing of information and knowledge across societies and specialisms."

[119] His regret stems from a crucial design fault built into the system, which is so pervasive it also prompted Julian Assange, founder of Wiki Leaks to recently lament:

"*The era of mass surveillance is here to stay*".

[120] The problem is the global standard TCP/IP joined all the private networks together to form one giant Network of networks. The security system based on single passwords to access a host, by default became access to the back door of all other hosts and almost free access to all data via the hardware of the entire Internet. Paradoxically, by joining together, the old networks became exposed and vulnerable to 'attack' but no one yet knew what that would mean. Now in 2016, most people know it means multiple passwords that are habitually vulnerable and an underlying stress that your data, identity or credit is compromised. If a user needs real security or privacy, that user or organisation must separate their computer/s from the Internet using dedicated secure servers.

What's missing from the equation?

[121] On the Internet there really aren't many Hosts that are much more secure than each user's personal browser software because all computers are on the edge of the same open Internet hardware. All databases at every node are accessible by anyone with the right password and very often a single password can compromise a whole site. Consider that a user's browser needs an operating system to access the Internet, but there is no operating system for the Internet itself? What's missing is a giant operating system to efficiently manage the security of the giant network. What is needed is a Giant Host that has back end and front end security and gives all network users a publicly accessible Internet at the same time as the ability to form scalable private networks.

So how is a Giant Host created?

[122] There's no point reinventing the wheel but the existing foundation techniques of the Internet can be repurposed into a parallel Internet that mimics the way the Internet itself is constructed to create private networks on the public hardware of the Internetwork. A binary system is the basis of computing but its principals have never been applied above byte level. Packet switching isn't actually packaged since the byte stream is like letters with no

envelopes, and Host security isn't actually secure because all hosts and users are exposed by the open hardware of the Internet.

[123] To solve these significant issues, the systems disclosed herein together apply binary systems, packet switching and decentralised security to user accounts and not just the byte stream alone. The networks would form by people and hosts joining their 'artificial' nodes together, and these data packages in this newly disclosed system must actually be securely packaged. The binary modular systems disclosed herein comprise networks built using a binary modular form of packaging. By design, the presently disclosed binary modular system shifts primary security responsibility from thousands of individual hosts at the edge of the Internet to a single giant host inside the Internet. This 'artificially' recentralised security responsibility uses decentralised usernames to automatically create the 'back-end' passwords that then enables the public and hosts to autonomously utilise binary modular packets equally without host interference, to create their private networks 'peer-to-peer' and access them via their 'front-end' passwords. In addition the binary modular system with automation of half of the binary passwords and up-scaling the number of passwords according to user sharing habits makes networking secure by default rather than by individual user effort alone.

[124] Therefore, it will be appreciated by the skilled addressee that the presently disclosed binary modular systems apply the foundation principles of existing binary systems, packet switching and decentralised security to user accounts and the way individual users share content, thereby to enable anyone to create truly private networks on a public operating system running on the hardware of the Internet.

So what's different with a Giant Host?

[125] A Giant Host must be free and open to everyone and everything, so it can't have an administrator or a commonly accessible database since it would fail someone's expectations. By being non-hierarchical, the binary modular systems disclosed herein allow everyone to tailor their own sense of hierarchy, order and purpose inside their own networks. Individual users can have as much hierarchy in as many Intranets of access as they wish precisely because the system is so thoroughly non-hierarchical. Additionally the networks need some way of finding each other and the only non-hierarchical system is one based on matching indeterminate conceptual relevance. The modules are therefore like blank envelopes that the users put together by 'addressing' them according to their individual needs.

[126] The binary modular systems disclosed herein has its own database but there is no public access into the platform database because there is no common interface and no need for common access. Instead, users build and access their own networks inside the binary modular non-hierarchical and inaccessible database. Every single content upload is in self-contained private binary modules accessible only to the user who uploaded it and their intended recipients and retrievable by direct hyperlink. A Giant Host therefore handles user privacy and security without needing to know, other than file size and type, what the specific content is. The binary modular systems disclosed herein is the digital age version of a truly secure private postal service but it's done by enabling 'miniature' private Internetworks that users build and manage themselves on the hardware of the greater public Internet.

[127] A Giant Host gives users private networks where each user, not the host, is responsible for how their content is shared and who joins their networks because the Giant Host manages overall security and thereby provides the means to communicate and network privately. Additionally, the absence of a common interface or database eliminates the main access route typically employed by hackers into the platform database thereby doubly protecting the individual networks created within the system. The Giant Host comprising the binary modular systems disclosed herein puts all hosts and the public on equal footing to go online, peer-to-peer, to do what before could only be done on a hosted site on a host's terms. The binary modular systems disclosed herein let's individual users use the Internet like a private citizen because it makes the Internet their private space. Giant Host security, or 'Ghost' security, is so in the background and all around the underlying platform that it barely affects the user experience at all as it is not the user's responsibility.

Practical operation of a binary modular platform

[128] For centuries civilians have relied on a secure private postal services of sealed envelopes and messengers to build networks and spread knowledge and yet the Internet today is not as secure as that system used to be. Everything, even email can be easily hacked and encryption is the only guarantee of secure privacy during data transmission on the Internet. The binary modular systems disclosed herein returns to the Internet the ability for individual users to create and interact within truly private networks.

[129] The binary part of the binary modular systems disclosed herein is the two inseparable digital modules, referred to herein as Up-Load Portals or ULPs. An Origin ULP is a main controller of contact lists, media content and access permissions and Related ULPs are an

interdependent level of control that, in unison with the Origin ULP, creates enormous flexibility in control and upload of user content whilst minimising data processing. By putting them together in any order, beginning with just a single Origin ULP, users can have public and private Intranets blended together in networks all using the same contact list.

[130] The modular part of the binary modular systems disclosed herein is that the ULPs are plugged together by any number of people to collectively build private networks for any purpose and autonomously create the private notification paths between network members. They are akin to semi-permanent, flexibly addressable envelopes but these are not sent repeatedly. A users will just set them up with their preferred contacts and change the content as needed, and the user's network contacts are notified of those changes according to more settings that both the user and their intended recipients control.

[131] When placing ULPs, the user gives each ULP a title, which guides the 'Vernacular Switch' function of the binary modular systems disclosed herein to introduce like-minded users and thereby build networks. A user initiating an interaction with another user activates a ULP string by entering titles into an Origin ULP and Related ULPs, inserting any type of content and making settings in either the Origin ULP or both Origin and Related ULPs and then posting the strung-together ULPs on the Platform. By posting a string of ULPs on the Platform or into an existing network, a user is, in effect, plugging their ULPs into the notification system of other ULPs to expand networks initiated by the vernacular switching system of the Giant Host platform.

[132] Without hierarchy and using only the vocabulary that members use to guide the building of the individually created networks, the hub of Internet activity in the binary modular systems disclosed herein revolves around conceptual, up-to-the-minute relevance only. Without hierarchy, communication in the binary modular systems disclosed herein is completely free of data stagnation, hierarchical ownership or user precedent. Any number of users can gather relevant data in a network without affecting the ability of all users to manipulate the parts of a network most relevant to them.

How is a non-hierarchical network controlled?

- *Joining Networks:*

[133] In a non-hierarchical un-administrated system people still need to find each other so in the binary modular systems disclosed herein, each user's username and the title given by each user to their ULPs is publicly visible. The content and the addressee remain confidential.

The binary modular systems disclosed herein uses the public face of each ULP to self-search and invite networks and individuals to join together. Members of networks can deliberately locate each other, but similarly named ULPs randomly placed on the binary modular systems disclosed herein will seek out each other to form new networks or join existing networks. It's a 'vernacular switching' system that allows the binary modular systems disclosed herein to be both a randomly public and a deliberately private DIY network builder. The more ULP titles that are added to a self-search string of ULPs, (a string of at least one Origin ULP followed by any number of Related ULPs) the more refined and nuanced the searches will be. In ULP's that members elect to allow it, a variable-resolution thumbnail of content will also be visible which, in further arrangements of the binary modular systems disclosed herein, may be utilised to provide self-search capabilities based on jpeg and docx files, as well as allowing the ability for such things as public social media mixed into private commercial media networks as in an eminently flexible supply chain network.

- *Moderating Networks:*

[134] For housekeeping in totally non-hierarchical networks, without administrators or moderators, the binary modular systems disclosed herein use consensual moderation internal to each network (LNP). All users in any network can action a 'Hide' button on every ULP posted to a network to which they have access, including their own, to eliminate trolls and irrelevant content. The 'Hide' action unplugs that particular ULP and its content from the user's notification system. When a critical mass of users in an LPN, for example 50%, all "Hide" a particular ULP, that particular ULP is deemed by the system to contain irrelevant content and is 'unplugged' from all users within the network. This consensus-based hiding eliminates the need for internal moderators or external administrators and makes the decision to hide content immediately effective for the users in a group who activate the 'Hide' action.

[135] Hiding a Related ULP unplugs just that particular ULP, however, hiding an Origin ULP unplugs the entire string of Related ULPs associated with that Origin ULP. In terms of overall peace-of-mind, a contributor of offensive and irrelevant content will be unplugged completely from a network unless 51% of others deem it to somehow still be relevant but 49% don't have to see it or waste energy on it in the meantime. Content trolls can still exist within the binary modular platform disclosed herein, but eventually they'll all end up in networks comprising only other like-minded users trolling each other.

[136] In a particular arrangement, the binary modular system disclosed herein may also be used as secure database storage for users, and this functionality may be offered as a paid archival service to users. For instance, since the binary modular system has no access to a common database, it is therefore not an archive of any one user's material. Users wishing to utilise the archive functionality of the platform may be provided the possibility to isolate their content from the consensus moderation system. Thus, archived ULPs would have their consensus "Hide" ability turned off, and the user may be charged a fee for this particular service. These archive ULPs would effectively be private non-networked repositories.

[137] Because the networks are formed only around conceptual relevance amongst members of a network, the opportunity also exists in unison with archiving outlined above, to 'Establish' parts of networks as an authority over that conceptual area of a Network. This may involve an establishment fee and a vote by network members that would be suitable for such things as corporate identity, social endeavour, services associations, etc. In essence, the platform's conceptual relevance algorithm offers the Internet its first ever online real estate and 'Institutionalised' networks as it will encompass preserving a lot more than a mere domain name.

- *Managing network content:*

[138] Because the content is uploaded into Networks via binary modules it allows a user's personal interface to also be modular regardless of the shared content of a network. All information in a network exists independently from the way in which network members choose to access it. A user can customise their own interface to suit their personal whims, sense of order or aesthetic, and dashboards can be designed or customised to suit a user's specific commercial, consumer, administrative, banking or browsing needs, all without affecting the actual content or overall purpose of any Network. Modularity also means users can create their own interfaces, and users that are so-inclined can start making Apps for the platform when open source coding is released. Because the integral Ghost Security protects users so thoroughly in the 'back end', the binary modular systems disclosed herein gives users real private networks that they can manage individually at the 'front end'.

How does Ghost Security work?

[139] Traditional host based passwords work by individual passwords entered by a user that must match a password on the other side of a Host's gateway. Once a user is authenticated on a system, they pretty much have run of the whole host and there's usually no more

passwords protecting the user from other users in a host with them. If a mal-intentioned user is clever enough, they can work out how to hack into the main database and either wreak havoc or steal data and/or money from other users. The binary modular Platform disclosed herein, however, has no common interface, no common administrator, and no commonly accessible database. It therefore does not have the huge security hole outlined above that normal hosts have to worry about.

[140] All users of the binary modular systems disclosed herein have their own password that gains access to their own account. The user is not part of any networks hosted on the platform until they are issued with a further, secret, platform password that gains access to the networks. Even then, the user is only granted access to the parts of a Network that are their own ULPs and if their username is added to the contact list associated with the other ULPs by the relevant owner. In the binary modular systems disclosed herein, the primary security system is the binary passwords attached to the Binary Modular ULPs. Every single ULP has both a user password and a platform password attached to it. The platform password is secret and may advantageously comprise a randomly inserted 3-character extension to each user's username so all users are inside the password regime together, not outside trying to get in. Therefore, instead of having to cross a gateway to access data, everyone a user shares data with has already attached that user's passwords to their own ULPs (and vice versa) by way of the contact lists, so there is no longer any need for password matching. Users build the Networks together by plugging their already secure ULPs together. Since the user must already be inside the Platform to be in any Network, the user's half of the binary password pair is always sufficient to view their own content. Indeed, users can actually build their own private Networks involving just them because it's still a binary password that's protecting the content. In effect the user is responsible for their own security but the overall network security is handled by the Platform via their combined usernames.

[141] Furthermore, as there is no common database access route, a hacker trying to crack a shared ULP has to attack at least two separate associated user browsers to obtain the content of just a single shared ULP and the hacker must crack at least four passwords rather than two, because everyone's binary passwords are attached to any shared ULP. To make it further secure, new people that a user allows into their ULP contact lists add their own binary passwords to each shared ULP their name is added to. Within a network, therefore, all ULPs have a minimum of 4 passwords but potentially could have many more - only limited by the size of the contact list comprising users that are permitted access to a particular ULP.

Security of a ULP is increased the more people are attached and enabled as users of that particular ULP. This is the polar opposite of hierarchical sites where security decreases the more people are involved in a site.

[142] It's common knowledge that the weakest link in Internet security is a user's own password. A whole industry revolves around just getting people to safeguard their passwords, change them often enough and adopt strong password practices. The binary modular systems disclosed herein eliminate that issue outright because the platform's username extension passwords are changed each time a user logs in to the system without the user needing to be aware that it is happening. Even if a user never changes their password, the binary modular systems disclosed herein constantly and randomly changes it's associated platform password to protect all user's content, plus the platform uses the binary interaction of those multiple passwords constantly changing to do what's called 'slip pairing'.

[143] Because many users are constantly logging in and out of the system at different times the multiple pairs of password changes are 'slipping' behind or ahead of each other in relation to their change times. This dramatically reduces the window of opportunity a hacker has to crack all the codes from weeks or months (as the case is for normal hosts), to hours or days at most. With the further addition that every ULP gains two more passwords for every contact sharing it, the presently disclosed system is likely to signal the end of hacking of networks for nefarious purposes.

[144] It has to be appreciated that the Ghost Security systems disclosed herein are potentially the strongest password regimes in existence and certainly the only one so strong in which all users need only one password to remember, and the only system that increases in strength the more people are given access to each ULP. Ghost security as disclosed herein, at a minimum, makes every ULP twice as secure as an individual user's own account access, and at least four times as secure as anything on the Internet today. All this is achieved by the binary modular nature of the binary modular systems disclosed herein with a user only needing to remember their own password whilst being protected by a minimum of 3 other passwords.

Ghost Security explained further

[145] The binary lock for two people in a private network on the binary modular systems Platform disclosed herein is assembled from the passwords outlined below. As contacts are

added to ULP postings, all recipient user's binary passwords are added only to the ULPs they share. Such binary password include:

- A randomly generated and randomly inserted 3-character extension to all usernames. This is changed daily at each person's login time and an automatic logout ensures continual regeneration of the password. No user knows what it is, needs to know what it is, or has access to its platform database location.
- All user's own account access passwords, which will change whenever the user chooses and the Platform will encourage regular password changes as best practice.

[146] In addition, the Ghost Security as described above will have encryption included in an associated software messaging program (app) adapted for use on a mobile computing device (e.g. a smartphone or tablet device) and another paired layer added to the Ultra high secure subscription versions as discussed herein (see also monetization discussion below) (see **Figure 9**).

[147] For preferred arrangements of the app software, a universal Platform generated verification code is periodically forwarded e.g. monthly, to all subscribers and their recipient contacts. The verification code may be changed by automatic regeneration from the Platform to all users' emails. In use, a user would simply copy and paste the verification code each period to continue using the software application, where the user advantageously is not required to remember it or even know what it is. Because all users are already within the same Platform hosted private network they all share the one encryption 'key' rather than having two 'keys' that have to match. For example, a 12-digit universal monthly verification code may be employed as the common source for a shorter encryption key changing daily, to run the shared encryption engine.

[148] For an Ultra high security arrangement of the binary modular systems disclosed herein, a distinct Platform generated verification code may be sent to each user's email on a periodic schedule e.g. weekly, calculated from the date the user signed-up to the Platform. This would will turn every user's 4 slip paired password into a 6 slip paired password unique to each of them. Even though it could be assumed that a corporate or government subscriber may have enough browsers in their private network in close enough proximity for a hacker to gain access to two computers at once, there is no super computer yet invented that could brute force all 6 passwords on a ULP in the window of opportunity that a slip pairing of this

size leaves open. Also remember, a ULP would usually contain a single document at most, not a corporation's entire database so a random type fishing expedition as in most credit detail theft would be rendered practically impossible.

[149] The 6 part Binary password regime provides potentially the strongest Internet security to date. The possible combinations assuming 6 9-digit passwords are around 151,200 billion only using numbers. If the entire keyboard character list is involved and the 6 passwords are 12 characters minimum, the possible combinations are 151,200 billion multiplied by 67,000 trillion. That's not including the fact all 6 parts of the code are constantly changing at different rates so the window of opportunity to crack them all is even smaller than the 4-part version. Also those figures assume just two people sharing a single ULP containing a single document or file. It doesn't account for the extra three passwords added for every recipient added to a ULP or the number of ULP's being shared in a large network.

[150] Turning back to the figures, there is depicted various aspects of the binary modular systems disclosed herein. As shown in **Figures 2A** and **2B**, the two ULPs **101** may be considered in terms of an "Origin ULP" **101A** and a "Related ULP" **101B** where there can be any number of Related ULPs **101B** associated with any particular Origin ULP **101A**. Logical connection **102** in general will comprise a link back route **102A** and a link forward route **102B** via the assembled ULPs. Logical connection **102** may also comprise a further connection **102C** to a further Origin ULP to form a logical connection between Origin ULPs which may further comprise a link back route **102D** to the initial Origin ULP. Any user can connect a further Origin ULP **101A** to any existing ULP (either an Origin ULP **101A** or a Related ULP **101B**) to form an interested group. Accordingly, the description above could also describe the logical collection of content of interest to any number of people or to a single person.

[151] **Figures 2A** and **2B** also show an example of the particular attributes that each Origin ULP **101A** and Related ULP **101B** may have in various arrangements of system **100**.

Wyrdom Binary Modular Platform System 100

[152] In particular arrangements of system **100**, the system may be referred to as an Unlimited Locatable Private Network Builder. System **100** may also be referred to herein as The Wyrdom Binary Modular Platform or more simply: "Binary Modular Platform".

[153] Binary Modular Platform system **100** comprises an Omni-Directional notification system to maintain real-time interaction for groups in strings, tables and 3 dimensional grids

throughout each Locatable Private Network on the Binary Modular Platform system. (See uncommon definitions for Binary Modular Platform, Omni Directional Notification, and Locatable Private Network).

[154] Binary Modular Platform system **100** comprises two distinct ULP types (or ULPs) **101A** and **101B** which are adapted to be logically connected in a Binary Modular construction in any order according to the desires of the platform users, each ULP type (or ULP) being adapted to order and rearrange potentially un-connectable content for amplified usability by allowing any number of users to join together with a common purpose and/or subject matter in a Locatable Private Network and the ability to form an unlimited number of Locatable Private Networks within the same Platform.

[155] Binary Modular Platform system **100** has a Modular user interface system distinct from the Binary Modular delivery of content system which allows re-arrangement of the content of ULPs **101A** and **101B** into random or patterned arrays distinct to each browser accessing the Platform according to personal habit or desire using the Modular user interface and thereby rearranging of a tabulated 'document' made up of ULPs selected from an original compilation or arrangement. (See the above definition for the term 'document' as used herein) without the need to adhere to any other user's preferences and without disrupting the links (except voluntarily and in certain privacy situations) between ULPs established by the publishers of the original core ULPs 'binary modular document' that began the Locatable Private Network content collection.

[156] Binary Modular Platform system **100** permits unlimited exercise of consensual preference with no rules of hierarchy, moderation, censorship, precedent, or pre-determined arrangements or classifications, to inhibit or hinder user relationships, intentions or purpose that could conflict with the conceptual denominator of any Locatable Private Network formed on the Platform. (See the above definition for the term 'Locatable Private Network' as used herein).

[157] Binary Modular Platform system **100** makes dialect and group intention integral to search functionality to form community adherences within and between consensual groups to form Locatable Private Networks by making the self-search parameters governed by naming or coding of the ULPs title facility **101A** and **101B** rather than by the content of the ULPs which is not readable by the Platform and as such the Platform has no administrative

oversight of the content of ULPs placed by the users and operates by way of a 'vernacular switching' system (see the above definition for the term 'Self-Search' as used herein).

[158] Binary Modular Platform system **100** allows consensual and preferential formation of communities into Locatable Private Networks by a continual updating of intention and purpose by 'unplugging' irrelevant content from an LPN via the user controlled Consensus Based Self-Moderation system. (See uncommon definitions for Consensus Based Self-Moderation as used herein)

[159] Binary Modular Platform system **100** exists as a distinct platform to transmit and augment preferential and privileged content as interrelated entity within an LPN where every user builds and rebuilds the Locatable Private Network to suit their needs using the available ULP types **101A** and **101B** and making logical connections with other users according to their personal requirements or interests in the privacy of a secure LPN.

[160] Binary Modular Platform **100** uses compatible digital ULP types, or ULPs **101A** and **101B**, which form a Binary Modular foundation for user groups to collectively build strings, tables, 3-dimensional and n-dimensional grids of information of any size for any purpose within an LPN. The modular strings can comprise any combination in any order of the two ULP types in accordance with their individual requirements. The Origin ULP type **101A** is a main controller and can be a secondary controller and the Related ULP type **101B**, of which there can be one, a plurality, or any number of such Related ULPs **101B** connected to any one or other previous Origin ULP **101A**, are an interdependent level of control that in their modular unison creates enormous, almost infinite flexibility. Focus amongst a group is provided by the continuous removal of irrelevant content via a Consensus Based Self-Moderation system. For example, at the moment 50% of participants engaged with a particular Related ULP **101B** have chosen to hide that ULP from their individual instance of the Binary Modular Platform system **100** then that particular hidden ULP will be determined to be no longer relevant to the group LPN as a whole and as such the hidden ULP will be 'unplugged' from the LPN of the group. Continuous progress of dialogue and content exchange in the LPN is unimpeded by content stagnation, hierarchical ownership or user precedent.

[161] The Consensus Based Self-Moderation system in the Binary Modular Platform system **100** has four functioning levels that allow all users on the platform to clear out irrelevant or offensive material from their LPN without having to rely on an external moderator on the

Platform or an internal moderator within any LPN. The Consensus Based Self-Moderation system functions immediately for a person activating it and incrementally for a group until more than 50% of the LPN group activate it, at which point the ULP is 'unplugged' from the LPN's notification system and becomes invisible to the whole LPN but remains on the Platform. A second level is purchased Advertising ULPs, which use the same system but selected ULP are removed completely from the Platform when more than 85% activate it. A third level that applies only to 50% ULPs is the ability of users to check within 2 weeks if a ULP they have hidden from view has been deleted by the whole LPN, giving that user a chance to reconsider their hide which can be either ignored or acted upon by reinstatement into the LPN. A fourth level is users of a ULP that have been 'unplugged' from an LPN group are notified of impending complete removal from the Platform after a set period of inactivity of that ULP.

[162] The Consensus Based Self-Moderation system enables any number of users to accumulate relevant content without compromising the ability of all other users to focus on and manipulate the most relevant parts to them. Its functions utilise a model of consensual human interaction with irrelevance clearance where no one user can prevent a group's LPN from continuously maintaining consensus on relevance and purpose.

[163] Content is handled by mimicking the attributes of a binary system combined with a modular system to speed up the manipulation of ULPs and minimise lineal or uni-directional paths of content transfer. It facilitates the omni-directional intentions of any group by accommodating many different types of content and/or privileges, and incorporating a free consensus model for ongoing group engagement. As simple packaging the Binary Modular Platform does not have the ability, or need, to read content contained in the ULPs and therefore the search parameter is determined only by the titles each ULP is given by the users when uploading content into a ULP, which strongly enhances 'local' knowledge, 'vernacular' language and conceptual purpose as primary search parameters. This makes the search functionality of the system **100** irrespective of the content and, enables interaction without third party or host interference in how or what any group interacts about. The Binary Modular construction of system **100,** by providing the Binary Locks which create a Locatable Private Network no matter how big or small a group is, makes it certain that the system can be adapted to provide many more applications than those outlined in the Examples below.

[164] At upload and deposit, the content of the ULPs **101** is privileged and inaccessible to the owners of the Binary Modular Platform **100** or to anyone not in an LPN recipient list of

the uploaders. Like a normal postal service, Binary Modular Platform system **100** has no business knowing the content of the ULPs and treats that confidentiality like a traditional sealed delivery postal service by removing the ability to read the ULP content being delivered. Since the Binary Modular Platform system **100** or system administrators have no ability to read content and therefore no ability to archive content, and all participants carry out the continuous removal of irrelevant content themselves, byte storage needs will be relatively small compared to the volumes of content being transferred through the platform.

[165] Locatable content archiving for purposes of the Binary Modular Platform system **100** is preferably limited for a short duration to file size of content at upload for the continuous review of storage needs and statistical purposes, and for a longer duration, international banking identity codes to license hosting of financial institutions, the username identities attached to each ULP on the platform to guide the notification system, maintain user accounts and subscriptions, administer the advertising and banking licence revenue and facilitate the satisfaction of official agency access via court ordered warrant. Most other user content is parked temporarily or longer term behind their own LPN 'fire walled' privacy and as such is being stored by the Binary Modular Platform system **100**, but not archived. As its storage is not guaranteed like an archive most of the content will likely be in the form of links to external archive locations. Any archiving of content is the sole responsibility of the individual users of Binary Modular Platform system **100**.

[166] In a broad context, the system **100** is a shareable content organising tool that allows users including group participants and invited recipients of links to content within system **100** to add relevant content to an existing string of content ULPs (using Origin and/or Related ULPs) and to allow all authors (i.e. users) of that string of ULPs to access the content collected by the group participants and connected within the string of ULPs. It allows a string or line of relevant content to accumulate organically without compromising the ability of authors and recipients in the string to hone in on the most relevant parts to them. The value of the system **100** lies in the ability to quickly build focused searchable strings of content files in any format, for any purpose, by any interested party in the total privacy of a Locatable Private Network.

[167] For example, system **100** allows interested parties, such as closed academic circles or privileged business-to-business groups, to share, control and add to relevant content strings or tables (BMDocuments) of content ULPs. It also allows acutely interested parties to send and receive standard content tables, such as business to business price lists or parts lists that can

also act as sales content records, direct marketing tools, adjustable and updatable price and parts lists. It also allows non-acutely interested parties to join as for example; bloggers or forum members connected to the same functionality as more privileged members of the LPN.

[168] Those same lists can also become extendable discussion feeds for unrelated but interested members of the public so that everyone from a manufacturer to a consumer can gather relevant information in both directions without compromising the core relevancy to each member using that content line or table (BMDocument). This allows a simple list to be adjustable to each parties needs and allows for both direct market research and instant notification of such things as parts recalls, parts redundancies, special offers, clearance sales and direct banking purchases.

[169] A key aspect for business to business interactions is that the system **100** allows an extremely fast upload of existing content formats into the ULPs system **101** so that, for instance, the vast reams of content contained in an Excel parts list can be loaded into an interactive table (BMDocument) simply by feeding the first row of content in the original table into a row of ULPs, then activating the Set Mass Content Dump at the ULP corresponding to the last item in the original content row. The, for example, Excel document rows are then automatically loaded as new lines, each individual line or individual table becoming a live feed adjustable string of a ULP 'binary modular document' for any recipient without losing the order of the original static document, and can become almost anything beyond its origin as a simple parts list such as a marketing tool, a public or private forum, a wholesaler, retailer and consumer sales point and/or a fully interactive notification system. System **100** as a modular format can be hidden behind the content so that the content it contains may look exactly like a normal Excel document depending on user generated templates or it can remain as content in a visible table of ULP system **100** templates.

[170] System **100** allows members of broadly interested groups to access and sift relevant content strings for their needs directly on their desktop or device, such as being able to isolate discussion threads from social media or any forum and blog poster without the need to trawl through past history or have one's mailbox inundated. For academic circles this would allow members to isolate particular matters of interest to them within a large group but have to hand any other relevant content attached in the string without the need to search for it separately from memory or ask participants to forward it. Of particular interest for academics is the ability to receive notification for any changes to or uploads of ULPs, which would allow live editing of complex theory discussions without losing track of the development of nuanced

alternatives or special interest discussions, and keeping the ability to maintain confidential privilege and focus within a potentially vast discussion board.

[171] In particular arrangements, system **100** is a pre-eminently flexible content management, sales and blog system that relies on a non-hierarchical infinitely reorganizational arrangement of the content contained in ULP tables (BMDocuments). The content is tagged to the original source document via each Origin ULP and is searchable by the title, whether unique or not, but thereafter the receiver of the new binary modular document (BMDocument) can reorganize the ULP strings to suit their purposes by adding or subtracting any Origin and Related ULP strings, 'plug in' extra information as needed or desired using their own ULPs, including preferred ordering and payment systems for in-house clients or the general public, forums, blogs, images and forwarding new rearrangements of ULPs etc. The new attached ULPs become both searchable by title (and this search-ability can be exploited by any third parties wishing to join an LPN formed around the original BMDocument) and linked via the notification system back to all users and authors of the original BMDocument inside an LPN.

[172] To create an interactive BMDocument (See the above definition of the term 'binary modular document' as used herein) data is entered into a parsing engine algorithm called a mass content dump from an original digital document relying of the number of columns but not the order of columns. The individual number of initial ULPs at time of content entry is only incumbent on the original document preferences. Thereafter the ULPs (each line of Origin and Related ULPs) are given a name (from a drop down of pre-sets/standards or completely free vernacular). Only the first row of content in the original static document is necessary to input for the parsing engine algorithm to fill all the rest of the new BMDocument's rows automatically from the original digital document.

[173] Once the BMDocument (table or grid of ULPs of Origin and Related ULPs in rows) is filled, extra Origin ULPs can be added at any point in each row by any other user that allows the plugging into the BMDocument of images, blog references, forums by the sender or receiver, alerts, ordering systems, etc. The addition of a new Origin ULP by any user triggers a notification to every other user of a new Origin ULP in the string or table unless they have elected not to receive default notification from any or all individual ULP sources. This is controlled from their own Origin ULP under the notification drop down containing all other users privileged by the initial users (Show Notifications).

[174] Once the string or table of ULPs is received (for example from merchant to wholesaler) the receiver can adjust the string of ULPs without breaking the link to the source string of ULPs including being able to reorganize dozens or hundreds of source ULPs that may look different and be labelled differently into a rearranged string or table of ULPs with the receivers own naming and ordering system. The key to this possibility is that each ULP is independent of others but shares the same tag/serial number via its associated Origin ULP so that it doesn't matter if the content is separated and rearranged. This means that the original string or table of ULPs can be searched from any individual ULP to which the serial number is attached and the string or table author can send updates back the other way to anyone holding the serial number tag whether or not the string or table has been rearranged.

[175] Once a string of ULPs is set by the initial author, updates, discontinued items, recalls, special discounts, new blog posts etc. can be forwarded automatically to any receiver of that table of ULPs via the notification system whether or not they have all or part of the ULPs and even if they have changed the names of the columns, as the tagged serial numbers of each Origin ULP associated with that initial row of content never changes no matter how it's rearranged. A receiver can elect to receive all or part of the updates depending only on which or all of the Origin ULPs they've decided to keep and/or unblock in their rearranged document. A warning of some sort would preferably be given prior to turning off the update function of each individual Origin ULP or would appear as a re-defaultable setting.

[176] The users of a string of ULPs may be the initial publisher or the rearrangement publisher and each such user can set who can and can't open only their own individual Origin ULPs in the string of ULPs. This is to protect the publishers copyright and privileges and help preserve the raison d'être of an existing LPN formed around that initial BMDocument. The initial publisher or new user/publishers can also request that information on sales can come back to them from wholesalers and retailers as an automatic ordering/notification system, but those subject persons can elect to turn off that default notification function to protect their privileges.

[177] Because the string of ULPs can be rearranged without affecting the tag/notification system any interface can be available that may or may not look anything like the Interface set by the original BMDocument author. Interfaces are therefore a plug-in app type additional choice unrelated to the Locatable content of the ULP tables and is reconfigurable by any interested user creating or purchasing their own interface from a modular selection. The ULPs are therefore adjustable in their look, such as colour, shape, size, font, position on

screen without losing the link to the original content contained or interfering with notification controls. Interfaces are able to be added to as modular plug-in options that anyone can build and sell to other subscribers just like a normal app.

[178] A default interface would be made available to access the Platform but thereafter any user accessing their LPN's can create their own Interfaces distinct from the Interface all other members of an LPN are using or simply as distinct for each LPN they are a member of which suit the raison d'être of the LPN. (For example, some interfaces will suit social media purposes more than some sales interfaces because members of the same LPN may have differing reasons for using the same BMDocument content.) Several optional drag and drop Interfaces with a notification system primarily using colour codes instead of numerals will be available. Additional 'plug-in' apps ports that allow insertion of other 'home-made' interfaces will be available as licensed additions created by the public from open source coding and/or available from professional app builders.

Monetising the Platform

[179] Utility fee: As a wholly utilitarian entity providing the ability to form scalable networks for any purpose with default privacy as an overall primary function, and no hierarchical host to user engagement entailed, the Binary Modular system as disclosed herein may at some stage have a utility fee attached for its usage on a par with or marginally less than the normal utility fees as found on delivery systems for such utilities as gas, water and electricity but applied globally on a pro rata basis nationally.

[180] Financial facility fee: Most sales sites rely on commissions of around 5% of a sale items cost paid by the seller. Because the Binary Modular Platform has both functions of inventory and sale of items as a private matter unknown to the Platform by virtue of the LPN's it instead will rely on a simple pay per week licence to allow a financial transactor of choice into an LPN. Particular ULP arrangements of system **100** may therefore have a billing system attached to each subscribers username account to track financial institution attachments and requisite fees. This billing system may, in particular arrangements, be contained in a drag and drop feature to enable any person to add a financial transaction facility to their own ULP strings. The financial transaction itself will be a matter completely between the user and their banking authority agreed through, for example, a financial drag and drop facility included in the Platform. With no ability to track content there is also no ability to levy sales commissions so a flat financial licence fee regardless of sales volumes

can be automated across the Platform. Since the primary attribute of the Platform is unlimited numbers of Locatable Private Networks it will be a relatively simple step, and desirable in terms of statutory control, to expand the automatic financial transaction license to apply for an International financial transaction overlay license in which case the Platform will itself become a financial institution for the transfer of funds via the Locatable Private Networks. Until that time, the Platform will be licensed to use an overlay service of an established financial institution such as, for example either MasterCard or Visa to transfer funds but this will be a direct seller to bank relationship that does not involve the Platform. The Platform will only gather a small weekly fee to install that facility into a user's ULP string and maintain the connection. In preferable arrangements, the platform is not the broker, but instead only provides a private venue suitable for the broker and the seller to engage in, for which service the Platform may charge a small flat fee applied globally.

[181] Advertising fee: Special advertising ULPs that are completely deleted from the Platform after 85% of users hide those ULPs. There are several types of advertising revenue possible on the Platform including banner adds, directed adds and focused adds but this source of income will remain mindful of the LPN nature of the Platform both in access limits to advertisers and the functionality of Advertiser ULPs.

[182] High security subscription: Subscriber only high security LPN licences. This may, in particular arrangements, involve the sale of annual licenses to use the 7-part Binary lock system within any associated LPN system. This may, in particular arrangements, be available only to large corporations and government agencies because the binary password regime is susceptible to multiple browser access in the case of a hacker accessing browsers side by side in the same LPN network. The high security version (3 slip paired passwords instead of 2 on the public system) would substantially reduce the multiple password-cracking time-window. The large advantage for such an entity is that the multiple LPN's available on the Platform with a single contact list enables corporations and governments to dispense with their own secure and separated servers and to be able to store encrypted content in the cloud. The fee would preferably be applied on a number of browser basis

[183] 'Establishment' of LPN's: To maintain a core group or document against the potential for an LPN to change its focus over time by the action of the Consensus Based Self-Moderation system, members of an LPN can elect to turn off that function for a core file area of the LPN that will in effect institutionalise their group inside a more permanent

'established' LPN. To do this only a core area of the LPN file storage area needs to be protected from removal so the group will elect to pay an annual fee for LPN Establishment.

Security

High Security Binary Lock

[184] As discussed above, the Binary Modular Platform system **100** may be secured by a unique form of ultra-high security measures termed herein as a Binary Lock or Ghost security implementations and variations thereof as would be appreciated by the skilled addressee.

[185] Binary Modular Platform system **100** uses the compartmentalised construction of the modular ULPs to create the Binary Lock. The difference between the Binary Modular Platform and traditional 2 key password locks is that the Platform does not need a matching key pair to individual user keys because the ULPs and hence the users are already compartmentalised inside the platform. All the users have their own keys to all of their shared deposits so the platform provides each person another unique and secret key that is intended only to keep anyone else out.

[186] It is a Binary code lock attached to every user's ULPs. Each time a ULP is shared by adding another user's username the system adds those binary locks as well. The more senders and receivers who join a ULP the more locks that are attached to it. Therefore it is not a fixed pair of matching keys on either side of a uni-directional firewall into the platform. It is a constantly changing firewall encircling every individual ULP inside the platform so that a user can contact any recipient within a Locatable Private Network group without noticing the pass lock regime in action around them. Since they must already be inside any group, each user's own part of the Binary Lock is sufficient for a user to view their own ULPs (i.e. ULPs that they themselves have posted).

[187] The Binary Lock system contemplated by system **100** is easily the strongest password system in existence. It is very simple to use and augments by a factor of billions the security of third party hosting agencies that may be linked to in a ULP. For example, with the high security version of 6 slip paired locks and a universal verification code, the possible combinations assuming an average 9 digit password are around 151,200 billion without each part constantly changing and only using numbers, not the entire keyboard character list. If the entire keyboard character list is involved and the passwords are 12-character minimum the possible combinations are 151,200 billion times 67,000 Trillion. Now add to that the fact

that as each additional user is added to a ULP contact list so too are the passwords of their part in the Binary Lock…

[188] The larger a group of people in which all recipients have access to all other recipients increases the number of combinations needed to open a ULP from outside an LPN but every user inside the LPN only needs their own lock. It is safe to say that the Binary Lock is likely to remain for a very long time the most secure password regime in existence. (Adding a distinct password to an ULP is intended to allow a user to leave their computer open while away from it.) From inside the LPN group security is added simply by adding another Origin ULP to a string group and resetting the recipients that appear in the contact list migrated from ones first Origin ULP. This method is the basis of the multiple secure Intranets made from a single contact list inside a single LPN, suitable for governments and corporations. Because the ULPs are by themselves highly impenetrable to anyone not in the ULPs contact list the entire content-base of ULP titles, usernames (and thumbnails in some circumstances) can be visible as searchable ULPs on any other web search engine.

[189] Every author and recipient has only their part of a Binary Lock that changes according to their own pattern of behaviour and the dates they log in. Neither party has to be online to affect the Binary Lock; they only have to be on each other's list of recipients in each particular ULP. The only noticeable change in current password regimes for any user is the resetting of verification codes once a month in the High Security version. The verification code may comprise a randomised code generated by a centralised processor associated with the system **100**, and sent via a user's email for reinstallation. In the general public version the Platform provides a constantly changing password in the 3-character extension of a username every time a login is affected so there is no difference for the user except that they may need only a single password to go to all their other sites if they're stored as open links in the Platform.

[190] Particular arrangements of the system **100** utilising the high security version of the 6- and 7-part Binary Lock will typically only store the original username and title as 'visible' with each ULP. The secret 3-character inclusion to usernames, user's Platform access passwords and verification codes will be ideally stored as fractured files in separated secure cloud locations. If a hacker gains access to a user's ULP, they have to also gain access to attached recipient ULP account details and therefore both pairs of secret 3-character extensions to the username in two separate ULP files from two separate computers and both user passwords. This means the only 'easy' way to crack a Binary Lock is to break into two

houses/computers at the same time in the hope you can access their computer passwords and their site password if they're not already logged in, and if so lucky then guess the three-character extension to a user name on two separate computers. That will potentially give a hacker access only to two authors' strings within a vast content-base and that's it and that's only if the ULP under attack is shared only by two people. To access a ULP shared by more than two people means hacking every computer in a contact list. To get to the whole content-base would require breaking into every computer of every user. To focus an attack a hacker has to know which computers are worth breaking into so will have to know what is being loaded into the site or retrieved before it's loaded or received and will have to know how many people are attached in a ULP contact list to begin with.

[191] In particular arrangements, the 6 part, 3 slip-paired, binary code system is assembled from at least, for example:

- An author's username plus a randomly generated 3 character extension;
- An author's regularly changed platform generated verification code;
- An author's own account access password;
- A recipient's username plus a randomly generated 3 character extension;
- A recipient's regularly changed platform generated verification code; and
- A recipient's own account access password.

[192] These 6 passwords, in certain arrangements, are re-generated in the following manner:

1. Potentially daily at login for every user, an automatically generated 3-character addition will be secretly added to their username and anywhere within it. No user or administrator of the Binary Modular Platform system **100** will know what it is or have access to it and an automatic logout will ensure continual regeneration.
2. All verification codes will be randomly changed by automatic generation from the site and may be sent as a secret asterisk string to a user email on a monthly basis from their sign-up. (i.e. the verification code is known only to the site administrator – the user must copy and paste only that secret asterisk string to log them back in to the Platform each month) A user just copy and pastes the secret verification code or clicks the link from email every month to continue using the site but does not have to remember it since it is secret anyway.

3. Randomly whenever a voluntary username account password change is affected which will be encouraged but is well backed up by password re-generation methods 1 and 2.

[193] As will be appreciated by the skilled addressee, only an author and any of their recipients will together have all six keys, whilst an author and any two recipients will together have 9 keys and so on ad-infinitum. For two parties four parts of the key were entered at site log-in, 2 of them automatically by the platform, with original verification codes being the remaining 2 keys. The six key pass-lock changes every time a user logs in, when the verification codes are changed and when the users themselves change their access passwords. This means 3 pairs of keys across a six part binary lock, each pair changing at a slower rate than the pair before it and at different times within each pair. The preferred arrangements of the Binary Modular Platform system **100** will only store the original username and title as 'visible' with each ULP. Therefore, even if a hacker gains access to a user's individual access details or files the user has created, they have to also gain access to their recipient access details and/or files using a separate computer and a pair of secret 3-character extensions to both user's usernames. If extremely lucky an unauthorised access through one computer will possibly reveal only the content of any ULP to whom no recipient has yet been attached.

[194] Medium Security Binary Lock (1)

[195] A less strong security scheme may also be adopted for the Binary Modular Platform system **100** which, as before, utilises the same binary construction to create a four part lock which is somewhat simplified for normal usage requirements. This four-part Binary Lock system would be a standard publicly available feature in preferred arrangements of system **100**.

[196] The 4 part, 2 slip-paired, binary code system is assembled from:

- A user's own account access password;
- A user's original platform generated verification code;
- Another user's own account access password; and
- Another user's original platform generated verification code.

[197] These 4 passwords are re-generated in the following manner:

1. All verification codes will preferably be randomly changed by automatic generation from the site on a monthly basis and is delivered to the user via their recoded email address as a secret asterisk string. A user simply copies the verification code from the email and pastes it into a dialogue box provided at a platform login page each month to be able to continue using the platform **100**. Preferably the platform login page will keep the verification code in its cached memory for each user whilst the code remains valid (i.e. for at most one month or until a new verification code is emailed to the user) so that the user does not have to remember the verification code each time they log in to the platform.
2. Randomly whenever a voluntary username account password change is affected which will be encouraged under common password security recommendations.

[198] This particular medium security Binary Lock system may be made available to users of system **100** as a standard version free with the website based platform.

Medium Security Binary Lock (2)

[199] An alternate version of the medium security Binary Lock disclosed above may alternatively or additionally be employed comprising a Five-part Binary Lock system. This particular Binary Lock system may be implemented as part of a secure, encrypted messaging service.

[200] This adjusted version of the Binary Lock may be specifically adapted for use on mobile computing devices such as a smartphone or tablet device in conjunction with texting or similar messaging service in conjunction with a document / pdf / image application on mobile devices. The five-part Binary Lock version enables system 100 to use the verification code as a source for the encryption regime so that all users are within the system of encryption rather than being on either side of it. They therefore share the one 'key' rather than having two 'keys' that must match. The four parts of the Binary Lock as discussed above enable security at either end of a text based 'discussion' between users with the fifth part providing the common source of the universal encryption code securing the content when it is in transit between the users.

[201] The five-part Binary Lock system may be incorporated into a software application specifically adapted for use on a mobile computing device. In particular arrangements, to encourage wide distribution of the five-part Binary Lock, the software application may be purchased by a user for a nominal fee. The purchasing user may then be provided with the

ability to distribute the software application to a selected number of others, e.g. between 2 and 10 other individuals depending on the fee paid). Each of those individuals who received the software application from the purchasing user preferably are provided the ability to freely use the software application for their own personal purposes, but may also be provided with the opportunity to purchase further distribution rights for the same nominal fee to distribute the software application to further individuals, and so on, with all users having the same verification code re-issued every month. The software application encompassing the five-part Binary Lock system in preferred arrangements may be a stand-alone messaging system adapted to use a distributed network such as the Internet and it will be appreciated that communications between users utilising the software application will be secure at the devices and between users. It will be functional as both a one to one system and a group conference / sharing system and it will always be a single Locatable Private Network protected by the additional verification code.

[202] Each half of a Binary Lock belonging to a user has the same site generated secret 3 character extension to a username and user password of minimum 12 characters (the 4 Parts) but all parties receive the same verification code changed weekly at a regular date (the 1 Part).

[203] In this arrangement of the Binary Lock, the 5 part, 2 slip-paired, 2 half, binary code system is assembled from:

- A user's own account access password of, say, at least 12 characters or more;
- A user's username including a login generated 3 character extension;
- Another user's own account access password of, say, at least 12 characters or more;
- Another user's username including a login generated 3 character extension; and
- All users' regularly changed site generated verification code.

[204] These 5 passwords are re-generated in the following manner:

1. Potentially daily at login for every user, an automatically generated 3-character addition will be secretly added to their username and anywhere within it. No user or platform administrator will know what it is or have access to it and an automatic

logout policy from the platform will ensure continual regeneration of the secret username addition.

2. Infrequently but randomly whenever a voluntary username account password change is affected which will be encouraged.

[205] All verification codes will preferably be randomly changed by automatic generation from the site on a weekly basis and delivered to the user via their recorded email address or mobile device number. A user simply copies the verification code from the email or text and pastes it into a dialogue box provided at a platform login page each week to be able to continue using the software application. Preferably the platform login page will keep the verification code in its cached memory for each user whilst the code remains valid (i.e. for at most one month or until a new verification code is emailed to the users) so that the user does not have to remember the verification code each time they log in to the platform.

[206] Thereafter distribution recipients making new distribution license purchases and redistribution receive the same verification code with each user instructed to re-enter the hidden verification code once a week via a copy and paste from a disappearing hidden code text. This hidden verification code preferably is a 12 digit number code with a sequential group of 6 numbers picked randomly from it on a daily basis as the flip and skip code to drive the encryption engine in the following manner: (see **Figure 9**)

1. Every day at a non-peak time 6 numbers in sequence are selected at random from the verification code and sent to the entire group as the daily flip and skip code. All users are unaware of this occurrence.

2. Each number in the group of 6 numbers represents the amount of bytes in the original byte sequence making up a message or document or image within a text message that will be flipped end to end in its original position. The flip numbers will be an integer value selected from integers 2, 3, 4, 5, 6, 7, 8 and 9 with 0 and 1 being instructed skip numbers.

3. As the flip and skip code progresses through the original message byte sequence it rolls each flip number to the back of the 6 digit sequence to ensure the next number is always the next flip or skip command.

4. When the end of the original byte sequence is reached the last available bytes that cannot be flipped as a whole group are moved forward un-flipped with the insertion of the flip and skip code between them and the flipped bytes. The last flip number used

becomes the new first number in the flip code. If by chance the number of bytes exactly matches the numbers in the flip code then the flip code resides at the end of the byte sequence with no bytes moved forward.

5. The entire binary number sequence and flip and skip code is then together flipped end to end with the flip code instruction of how to re-flip the encryption now at the front of the original byte sequence behind a small group of original message bytes, or at the front of the sequence, when received.

6. An instruction to find the 6 digit flip and skip code in it's new, or by a good chance its original sequence, is part of the recipient's receive procedure. The flip and skip code is found and checked against the recipients flip and skip code by matching the 6 numbers in sequence even if not in the same position. The un-flipped bytes remain as is and the inserted flip and skip code then rolls through the original bytes flipping and skipping them back into their original position using the reverse 6 digit number order.

7. The entire reordered byte sequence is then flipped back and the flip and skip code is checked it is in its original sequence before being stripped off and the message, document, image delivered.

Functionality of Binary Modular Platform System 100

[207] In the following description, the term 'author' refers to a user who publishes an initial Origin ULP in a string or table of ULPs notated herein with the term BMDocument. It will be appreciated that unless the 'author' can maintain control over subsequent published material many other authors of ULPs in an LPN will soon corrupt it. There-after they all become 'users' assumed to be authors only of their own ULP no matter how many subsequent ULP are attached by others to an initiating BMDocument and no matter how much or how often a BMDocument is manipulated by other 'authors' subsequent to being published.

[208] The main functionality of the Binary Modular Platform system **100** is non-hierarchical in terms of, for example: compartmentalisation of LNP into user controlled ULPs enabling non-hierarchical participant control, content manipulation, user management, content distribution, basic functionality, consensus content accumulation, and consensus content filtering.

Participant control:

[209] No one person controls the addition of new content or the deletion of existing content. All users can elect to permanently delete other content by the 'Hide From View' function associated with the particular ULP that the user wishes to hide from their personal view. Each person involved in a string or table controls only their content and elects to receive or not receive new content upload notifications. All new ULP attachments require setting access permissions, via reuse of previous ULP settings if deemed suitable or new distinct settings. Each post in a string or parts of a string, or parts of a table (BMDocument) can have distinct settings allowing different levels of access or visibility within the 'same' document / market place / forum / joint blog etc.

Content manipulation:

[210] No content is editable within any ULPs. ULPs in a string, table or grid can only be changed by deleting and replacing a ULP or by replacement of a ULP's entire content, and only the author of the Origin ULP they belong to can do this. A new Origin or Related ULP attachment or ULP content change triggers a notification through all Origin ULPs attached to that string, table or grid. All other Origin ULP authors are notified of a change only if they choose to receive it.

User management:

[211] Authors within a string of ULPs are equal in status to any other author in the string. Deletion of content is only via a consensus process of irrelevance elimination or self-removal by the author of each Origin ULP. If an author wishes to maintain total control over a string or table then their settings must reflect the level to which 'total' is deemed acceptable in terms of the functional intent and reach of 'their' document. In reality they can only fence off portions of their string or table deemed confidential to a select few and consent to the rest of the document being privileged or publicly available. The Binary Modular Platform system **100** is not designed towards complete isolation although a single user can lock out everyone else from his or her own solo use of it. Unless agreed the content format of a string or table is to be shared and manipulable and alterable by all users with the addition of new ULPs or the relocation of ULP portions of a string by other parties.

[212] Ultimately the management of the entire LPN is governed by the relevance bias of all the users unless otherwise agreed. A mixture of Recipient and Permission settings delegates access to an author's string or BMDocument for all other users within LPN's including

download rights, sharing rights, notification rights and messaging rights within the augmented limits associated with both Origin and Related ULP permit settings. This allows a flexible access regime that accounts for nuanced relationships.

Content distribution:

[213] Distribution is governed by very low voluntary hierarchical controls but Ultra High security protocols. Naming or coding the Origin ULP and Related ULPs in a string controls self-search-ability by acting as a 'vernacular switching' system. The Binary Modular Platform system **100** can behave like a private secure Intranet with search ability confined only to its own members or as an Extranet with elements of the group at different levels of security to other elements of the LPN. It can be a completely open forum or a completely closed forum or a blend of both conditions. It can be both an Intranet and Extranet network at the same time depending entirely on each member's notification settings in each ULP.

[214] Each individual ULP within a string or table can be altered to change access to suit the member or group using and distributing their content. Essentially the Platform does not distinguish between a sole user and 10,000 users because it is primarily a packaging system of sealed ULPs in sealed LPNs with distribution of content in ULPs entirely a prerogative of the users.

Basic functionality:

[215] The Binary Modular Platform relies on combinations for the first and second types of binary 'ULPs' (or ULPs as described above) that are modular, reusable digital repositories with a name or coding to identify the content to its author to make it searchable via a designated keyword or serial number. In alternate arrangements, the Binary Modular Platform **100** will be further adapted from the forms herein, thereby to use images as 'ULP identifiers. There is no search criteria for the content other than the author's own naming criteria and, by extension, the community to which they belong or indeed the community whom 'they' create. There is no limit to the number of authors who may join a LPN for their own reasons and who may or may not be visible to other authors depending on each member's access settings.

[216] In this sense the system **100** is like a library shelf with no universal access or Dewey number (referencing) system. Instead every item is privately code-worded and made searchable to other discreet recipients who have joined the LPN. Joining an LPN gives access to the ULPs in that LPN at levels expressed by each member's individual needs. Access to a

ULP does not grant access to the whole LPN, as each ULP is a distinct compartmentalised entity controlled by the uploaders alone and removed against their wishes only by the consensus deletion system. Access to the ULPs is by request and permission and gains access to other users also by request and permission. But once permission is granted recipients can take and use the content as they wish with the exception of direct text copying permissions, which are voluntarily controlled.

Consensus content accumulation:

[217] No one author within a string of collected content has hierarchy in the content string as all participants determine relevance. Community understanding and 50% consensus determines relevance, not hierarchical pre-determination, algorithmic filtering, host censoring or third party moderation. Consensus content accumulation creates a large resource of closest match to a search term. It's the difference between individually searching alone through millions of possibilities in a single Google search and searching through a resource already compiled from Google by many other similarly interested people who found and collated the information before you into a specific LPN.

Consensus Based Self-Moderation:

[218] A continuous method of updating LPN's on the platform that accounts for the intentions of any number of participants including just one. Controlled by determination of relevance that removes irrelevant, unwanted or offensive ULPs from any content string or BMDocument. Hiding an ULP in a string activates a consensus system. When more than 50% of participants in a group have determined irrelevance by hiding, those ULPs or strings are automatically unplugged from the LPN (meaning unplugged from the notification system within that LPN, but immediately for each person as they use the hide function. Hidden ULPs stay available in a drop down for 2 weeks to allow a recipient to reconsider their hide and reinstate an ULP or string if desired. Unplugged ULPs remain on the platform outside that particular LPN but they may form new LPN as they re-join with others. If an unplugged LPN is unused or inactive for a period of time it is removed with notice, from the Platform entirely to save file space.

[219] Hiding an Origin ULP deletes the entire string associated with that Origin ULP whilst hiding a Related ULP within a string deletes only that ULP. This flexibility of hiding allows for the possibility of encouraging users to stay relevant by partial deletion as an anonymous warning without complete censure of all their contributions. It also allows a rash decision to

be reversed in the case of continued engagement by other members causing confusion for someone whose hide means they can't see an ULP mentioned in discussions.

[220] A second level of hiding is purchased Advertising ULPs, which use the same system but are removed completely from the Platform when more than 85% activate it and without the option to reconsider. Notice of this feature will be part of the subscription rules but will be anonymous in action. The inherent fairness of this system is that hiding normal or advertising ULPs is a vote of no confidence that also allows the hider to immediately put into effect their decision whilst entrusting a quorum to decide if everyone in the group should be prevented from seeing something or denied access to the LPN.

Flexibility of System 100

[221] Arrangements of system **100** are inherently flexible in a number of key areas including: accessibility to an unlimited number of participants or users; unlimited purposes and applications; organic accumulation of content; and eminently shareable.

Unlimited numbers of participants:

[222] Any number of interested persons is capable of joining an LPN on the platform. Consensus community participation coupled with omni-directional notification gives all communities on the Binary Modular Platform a life of their own, independent of the people coming and going (and of the Platform itself), but dependant on the majority currently interested in being involved. Theoretically this means a particular LPN could morph over time into a different purpose from which it originated but logically the larger the numbers of participants the stronger the LPN becomes in terms of longevity and usability to its members. The smaller the number of people involved in an LPN the more likely a Lord of the Flies situation could arise, but since the users are not trapped on a physical island it's much more likely that consensus principals would triumph and such dysfunction would be hidden out of existence.

Unlimited purposes and applications:

[223] Any type and any format of content are capable of being collected using the platform and many methods of line or table manipulation of content within the LPN's. This means that anything from single topic forums of hundreds of people to massive content spread sheets involving thousands of consumers can be created using just the two binary modular ULPs.

Organically accumulating content:

[224] Unlimited incremental and/or exponential content gathering patterns that are bound only by relevance determined by current participants. With the ability to name a ULP for search purposes without involving the content of that ULP in the search, relevance is determined and controlled by members of the LPN and not by external search parameters. This allows for highly confidential and/or highly specialised sharing and search abilities that together with the consensus clearing system reflects the overt intentions of a majority of participants in any LPN.

[225] Key to the organic accumulation of LPN's is the Search Similar Names/Codes and Search Similar Settings in both ULPs that together forms a binary focusing of search relevance for a whole string. This reduces a generalised search where thousands of vaguely similar posters are unnecessarily joined. The increased focus-ability of the Binary Modular Platform self-search means that groups of like-minded people are quickly assembled and the control of that LPN accumulation through the minimum four combined search settings (from a minimum one Origin and one Related ULP posting) can be as broad or fine-tuned as desired by all the members of an LPN. Once a relevant ULP poster is culled using their own settings an author then requests access to authors from a dropdown selection and so the community forms.

Eminently shareable:

[226] The platform **100** can be anything from a simple alternative to email, drop box, face book or twitter, or a massive interactive content retention and delivery system for large multinationals using private in-house functions, or hundreds of thousands of private market places for products and services eliminating the need for third party transaction hosts such as eBay, Face book, SEEK etc. Without third party governors restricting or manipulating patterns of distribution, a truly consensus based freedom of information is enabled where more secure packaging, increased flexibility of delivery and more focused aim of intention protects sharing. The ease with which participants can join an LPN and submit content ULPs, the control of particular recipients of content string ULPs by authors and the ease of eliminating irrelevant or offensive content means that individual requirements can be much more easily met within a singular platform of delivery. No one is excluded by any hierarchical deficiency of the underlying Binary Modular construction method.

Self-Searching

[227] The Modular nature of the construction of the platform enables a self-searching functionality whereby the system will enable at least two users to gravitate together if ULPs which they have authored/created are titled similarly. Within the platform the self-search function recognises similar posting titles and enables each to contact the other via a drop-down once a ULP has been uploaded. This is distinct from the notification system in that the awareness' of a similar ULP is via a voluntary request for such similarities done by activating the dropdown at the title window of an ULP, rather than an unrequested notice from already established recipient/contact lists. It is also distinct form the 'search similar settings', which is used to search one's own content/recipient settings for the purpose of speeding up posting and use of the platform.

[228] As disclosed herein, the system consists of two interdependent ULPs **101A** and **101B** that work in unison to give an infinite variety of applications of the content contained in them. They are respectively termed an Origin ULP **101A** and an Related ULP **101B**. The ULPs are preferably both user titled with no connection to the content they contain but the ability to automatically search for and suggest connection to similar ULP titles and settings by other users both within a closed group and within the open internet.

[229] The Origin ULP **101A** has a primary settings permission and recipient group and the Related ULP has the ability to fine-tune the first settings group and/or augment the content contained in the first ULP. In terms of a true binary application the Origin ULP **101A** can be the equivalent of a prefix and the Related ULP **101B** is the equivalent of the suffix or subtext, giving a user the ability to construct an infinite number of ULP sequences from just the two ULPs with differing titles and order of placement in a string.

[230] The ULPs themselves contain a much larger mass of unsearchable content with the title acting as the primary search parameter and the permissions and recipient lists the primary direction instructions for the content. For a user this condenses an unwieldy amount of content into a very few distinct terms that others with similar or the same intentions can easily find enabling autonomous groups to 'naturally' form according to intentions and biases of the group.

[231] In terms of a true modular sequence the Origin ULP **101A** is a non-restrictive governor of the Related ULPs **101B** and forms the marker for a new sequence with new behaviour instructions within a string of Origin and Related ULPs. The sequences of one

user can be joined to the Origin and Related ULP sequences of another user creating a new meaningful sequence for either parties or indeed, an infinite and transitioning number of parties.

[232] Similar to the way a DNA coil works to create multiple variations with simple protein codes, the mass content is condensed into strings of title sequences controlled by all user intentions that will only join to other similar sequences. This enables the creation of larger groups of intention, which with the consensus elimination system, is a self-administering and self-correcting autonomous group in a Locatable Private Network.

Default functions of ULPs 101: (See Figures 4A and 4B)

Origin ULPs.

[233] Controls the separation between interested parties in a line of assembled content and enables the individual tailoring of content without compromising the interests of anyone else in the line. Enables the primary control settings for a user's interaction with others. The properties and typical control functions of Origin ULPs are shown in **Figure 4A**.

Related ULPs

[234] Facilitates the uploading of any content format into relevant strings or tables of content as determined by Origin ULP authors and enables the interconnected relevance of searchable content no matter what format it is in. Enables or overrides the secondary control settings defined by the Origin ULP. The properties and typical control functions of Related ULPs are shown in **Figure 4B**.

Link Back Route and Link Forward Route

[235] Condition of all ULPs after the placement of an initial Origin ULP. Maintains the connection between all ULPs in a string or table no matter how many Origin ULPs different authors attach or how many recipients reorganise the ULPs. All ULP names and codes in a single table or string are searchable to any author or recipient belonging to that string or table, after which they can request an author for access to the content.

Malware Algorithm.

[236] System **100** recognizes and stops mass participants joining a string to prevent stacking of content strings by malware from hacker computers, malcontent or mal-participant group's intent on outnumbering an entire group in order to delete them.

Secure ULP Content

[237] Only ULP titles are searchable within system **100**. Only authors can view their own string with transparency setting of ULPs and thumbnails of content or text viewing on scrolling over ULPs. Maintains speed on the site, security of the content and functionality of the interface.

Recognise Banking in String

[238] System **100** allows the upload of permitted banking facilities into a string by author using a drag a drop facility to subscribe for a financial transaction licence and then provide the banking facility. Algorithm that recognises the international financial transaction identifier codes assigned to all Internet banking facilities. All ULP content is sealed after closing by authors. At the point of loading into ULPs all content is technically readable by the Binary Modular Platform system **100** but the bank recognition algorithm is the only reading of content that occurs. Allows the system **100** to stop the uploading of a transaction site onto the platform until a charge for an on-site transaction licence has been paid under the terms of subscription.

Drag & Drop String

[239] System **100** allows any author active in a multiple member string or table to relocate any other author's whole string for their own purposes. Automatically breaks the receivable notification system settings of the original author to protect privacy but preserves the deliverable notification settings. Allows for example, rearrangement of a manufacturers table by specialist retailers who may require only part of a larger parts list.

[240] Activating the Send Access Request option in any Related ULP allows re-joining original author's receivable notification system under that author's terms. Allows following the public activity of any author and rearrangement of the content into new formats as suits the recipient and, for example the re-joining of a manufacturer's ordering systems by an original BMDocument author.

Drag & Drop ULP

[241] Same function and purpose as for a String as outlined above but for individual ULPs of interest plucked from strings and tables. Allows an author or recipient to gather specific content from many different sources without having to deal with extraneous content. Note

that this process does not alter the original BMDocuments or strings from which the ULPs are sourced.

Functions of Origin ULPs 101A:

Permission Edits

Allow Origin ULP String

[242] Allows for the addition of relevant content to tables and strings by author that can be augmented at each line in a table by the addition of content from special interest parties further down the line of production and consumption as outlined above. Allows upload of content by author before allowing others to join the string or allowing a new string to go live. Allows an author to separate out within the same string different tangents of interest they may want to keep separate within the same group. Allows construction of tables of strings by the same author.

Set ULP String Limit

[243] Allows an author to close further additions from their notification system so that any new authors of the string are blocked to them and make their activities invisible beyond that particular ULP except for any ULP updates other authors have been entitled to. Allows for a special interest group or individual to remain insular within a larger group without blocking the link back **102A** and link forward **102B** path that may service other people present on the string via their uploads. Includes situations like a manufacturer uninterested in the dealings between retailers and clients that may be based on their original parts content table but doesn't disable the notification system from the manufacturer to any future 'unknown' users of their products.

Allow ULP Update

[244] Allows alterations to the content of a specific content ULP in a line of ULPs up to the next Origin ULP in that line by author. Generally refers to direct text messaging in ULPs and enabling the total removal and replacement of content within ULPs. Allows manufacturers to update parts lists for example and activate an update notice to all other users known and unknown.

Send String Update Notices

[245] Activates ULP notification system by author to all other authors within a string, of any changes including new ULP attachments or new content in existing ULPs that others

have requested notification of. Allows external site notification systems via hyperlinked contents. Allows many changes in an author's string to send notification via one notice. By default disallows notices to be sent.

Get String Update Notices

[246] Allows detection of changes to a string by members who have clicked on the 'Get ULP Update Notice' in Related ULPs of content changes by author or recipient. Allows detection of external notifications generated by sites linked-to in an author's own ULPs such as newsfeed updates in individual face book accounts, or new offers in subscription company websites, calendar notifications from third parties etc. Allows filtering of author's changes at the Origin ULP. Sets username address link for notices by author.

Send Collated Update Notices

[247] Allows all permitted notifications to be prioritised by sender and receiver. (Over rules Get String Update Notice, which is a general default permission) Notifications activated in own ULPs and other authors ULPs by right-clicking Send Collated Update Notice (Origin ULP) or Allow Link Notice Collation (Related ULP) Notifications displayed as colour coded expandable fans on front page of subscribers home page/entry interface (additional settings in Set Notification Regime) Notifications ordered by preferences set in any own Origin ULP but accepts routed notices from all ULPs in member strings and tables. Drop down allows authors to adjust acceptance of updates 'requested' from other authors within strings or tables including rescinding requested updates.

[248] Updates include any content associated with forums, blogs, banking, document edits, and calendar notifications, email address changes, social media etc. This allows the Binary Modular Platform system **100** to function as a social media tracker, task dedicated calendar, retail purchase/marketing information board, live spare parts list, live chat etc. Default algorithm to clear fan card notifications that aren't activated within a time limit of being received. (Clearance rate dropdown selection, e.g. 1 day, 3 days, 1 week etc.) Optional archive by collation preference settings into tables or graph for activity tracking.

Set String Password

[249] String level of password protection by author. Allows viewing access to a table by select recipients to be separated so that an author can load many different strings of information intended for different people into the one table. Allows for example, a manufacturer to collate many different product streams into one platform or an author to

exclude an additional layer of recipients not included in other settings. Also allows for secure access where accidental access is eliminated by author and adds a personal browser control layer to the recipient and permission settings for example where a user must leave their computer open while attending to something else.

Set Table Password

[250] Table level of password protection by author. Same function and purpose as for a String Password as outlined above but allows for many different tables to be stored on the same LPN. Allows for secure access where accidental access is eliminated by author. Adds a personal browser control layer to the recipient and permission settings for example where a user must leave their computer open while attending to something else.

Recognise Banking In String

[251] See above default functions of both ULPs.

Allow Emails, Calenders, etc.

[252] Presets content recognition in the Origin ULP for any Related ULP in a string ending at the next Origin ULP by author. Enables efficient running of the platform by not overloading strings or tables with unnecessary content searches. Assists loading of select file formats during a Mass Content Dump by not having to repeatedly run file recognition at every new line. In preferred arrangements, these functions may all be grouped together within a common dropdown with multiple option activation permitted.

Identity Edits

Set Any ULP by Name

[253] Final activation to begin posting an ULP or a string of ULPs to the platform. Dropdown confirms file types as selected at Allow Emails, Calendars etc. to be subsequently loaded and text window allows input of primary search definition title of ULP. Subsequent ULP titles form secondary search definitions and Locatable content deposition ULPs. Sets the file type in Related ULPs which can be over ridden as required in individual ULPs.

Find ULP by Number, Word, Image and/or File Name:

[254] (All under one dropdown with multiple option activation) Allows internal search of all authors and all ULPs within a string, table or LPN to which an author is a member using the ULP identifiers.

Drag & Drop String

[255] See above, default functions of both ULPs.

Hide Edits

Set Recipients

[256] Sets the primary list of all other authors within a group string or table from whom an access request has been received and granted and to whom notifications will be sent. Allows the selected recipient drop down list to be selected from when attaching Related ULPs to an author's string section. A single selection here will automatically be applied to all Related ULP attachments beyond this Origin ULP. Multiple recipient selections require re-confirmation at Related ULPs when the opportunity to revise recipients at that ULP is possible.

Set Permissions

[257] Sets the primary list of permissions by which all ULPs in an author's string section can behave. Allows author and recipient notification delivery systems to reach each other. Allows the Recipients drop down list to be selected from according to file types at Set Recipients, at the attachment of Related ULPs to an author's string section. A single selection here will automatically be applied to all Related ULP attachments beyond this Origin ULP. Enables current Origin ULP members to be contacted by new Origin ULP members before allowing full access to author's content. In conjunction with Set Recipients, allows for the 'fencing off' of distinct areas of BMDocuments according to privileges associated with levels of confidentiality in an organisation.

Set String Hides

[258] Sets the primary list of recipients in a string an author does not want to give access to via internal searches. Allows the selected recipient drop down list that will appear at attachment in all Related ULPs belonging to an author's string section. A single or multiple selection will be applied to all Related ULPs with the option to allow search access from a drop down at attachment of Related ULPs belonging to an author in that string.

Set ULP Transparency

[259] Allows an author only to view the contents of their own sealed ULPs by selecting from a dropdown of permitted file types. Once selected from Origin ULP dropdown transparency is enabled in Related ULP via their file recognition settings.

Set Thumbnails

[260] Allows an author to select from drop down size and type of thumbnail viewing applying to ULP Transparency settings. Thumbnails may be voluntarily viewable to users outside an LPN along with default ULP's title and username. Allows the mingling of private and public elements within the same LPN

Set String Notifications

[261] Allows an author to select from drop down other authors in a string they wish to receive notifications from. Other authors' need their settings open so Send Access Request can remedy notice of request blocked

Set Notifications Regime

[262] Allows an author to control frequency, longevity, prominence and position by select recipients on screen of incoming notifications. Default notification array uses colour coded 'fanned card' decks to notify updates from each Origin ULP in a string, rather than numbers. Different colour used to denote weeks, days and or hours since each notice was received and self-deletion to rely on longevity settings. Allows an author to control the appearance of notifications on their User Interface. Default link from the colour card notice to the relevant ULP within a string. Magnified ULP title on scrolling over colour cards on home page. Optional hidden numbered collation system that allows archive and survey of the notifications received and deleted via the colour method to allow traffic tracking in graph form.

Search Similar Names/Codes

[263] Allows an author or recipient to find similar users on different tables and strings. Facilitates the conglomeration of authors for goods, services and jobs markets etc. Together with Search Similar Settings increases twofold the focus of a relevant search and together with Related ULP settings increases it four fold.

Search Similar Settings

[264] Allows an author or recipient to find particular nuances of settings they may wish to maintain and continue with a new ULP posting. Copy and Paste Settings in Related ULPs allows quick transfer to new Origin ULP. Speeds up distribution and streamlines use of the platform. Enables the avoidance of confusion of relationships in a large group of users.

Hide String From View

[265] Allows the consensus elimination of irrelevant posts (See detailed description of this feature under 'Consensus Based Self-Moderation' above)

Save and Share String

[266] Enables an author or recipient to forward a string section as a hyperlink (based on its n-dimensional axis position tags) to any interested person who may or may not be a member of the Binary Modular Platform system **100**.

[267] Automatically breaks all notification links except to contained external public site hyperlinks and allows viewing of selected ULP contents if original author has released any or all password locks on individual ULPs.

Run Mass Content Dump

[268] Auto fills tables or single lines of content ULPs according to Set Mass Content Dump Limit in the last 'other' ULP of the first line of a proposed table. Allows for the entire contents of an original digitised document to be parsed by the Binary Modular Platform system **100** by filling only the first line of content into the platform. See explanation of procedure in Related ULPs.

Functions Of Related ULPs 101B

Content Edits

Add New Origin ULP

[269] Allows any authors in a string or table to Origin a new string of relevant content ULPs attached to the initial string or table if Origin settings allow it. All Origin ULP authors in membership receive notification. Activated by any author who has obtained membership via an Access Request by clicking the function in any ULP of a string. Enables the construction of non-linear tables of relevance by any members of a group. A New Origin ULP will automatically copy the file type settings of the Origin ULP that begins the string wherein the Add New Origin ULP option was clicked excluding that string author's recipient settings. The Author attaching a New Origin ULP must set recipients of new string from their own recipient list and if desired alter the copied file type settings from their own preferences. If an author has the Add New Origin ULP setting disallowed, Park Content Pending will appear and user can deposit their content in this ULP. It will remain private but a notice will be sent

to Requested author that will initiate a message chat in the pending ULP to negotiate attachment of the content.

Add New ULP to String

[270] Allows an author of initial string to continue to add relevant content ULPs to their string only. Cannot be used by another author to add to someone else's string. Automatically copies all Origin and Other settings used in the ULP of the string in which the user clicked the Add New Related ULP option including all primary settings of the Origin ULP of that string. User must alter recipient and permission settings by using drop down settings or copy and paste settings from a preferred ULP of another author.

Update ULP Content

[271] Allows an author to replace content of ULPs only within the author's string. Also refers to direct text in that ULP and external notifications via sites linked-to in that ULP. Default disallow unless Origin ULP permission is activated, prevents accidental loss of content. Allows manufacturers to update parts lists for example and activates an update notice to all other users. Facilitates use of any Mass Content Dump BMDocument

Get ULP Update Notice

[272] Allows request of notice to any member of a string of alterations within ULPs or addition of new ULPs by any members. The member must be on a recipients list to have access to this request function and is activated in Related ULPs by any member of a string or table after confirming username address and/or password. Notices are sent via the Origin ULP of each string.

Send Access Request

[273] Allow recipients to link their username to other author's recipient lists. Allow a recipient to request notices and send notices to specific authors and members.

Allow Link Notice Collation

[274] Allows a recipient to request a notice to their own Origin ULP where the selected notices are sorted. A default setting is no notice sent on request. Available only to members of a string accepted as a recipient by author.

Set ULP password

[275] Allows lock on an ULP for secure access where accidental access is eliminated by author. Adds a personal browser control layer to the recipient and permission settings for example where a user must leave their computer open while attending to something else.

Copy and Paste Formatting

[276] Allows quick transfer of setting and permissions onto new ULPs or new Origin ULPs. If done by author of ULP, copies entire setting and permissions list. If done by recipient, copies all setting and permissions except those that recipient doesn't have access to. Includes ability to grab all last settings on selecting 'new ULP' and then select from drop down of all setting 'revert to default' of individual settings as left click options, and then scroll over to drop down to change distinct permissions as right click options.

Allow Banking

[277] Nominates an ULP for banking facility to be attached by author. Must have first secured site permission via usage fee via Origin ULP and agreed to brokerage by which ever banking facility is selected

Set Content Dump

[278] Allows preset of line limit for content dump purposes in tables or long lines by author.

Recognise Emails, Calenders, etc.

[279] All under one dropdown with multiple option activation)

[280] Nominates a Related ULP for intended content format first established as load-able in Origin ULP by author. Allows additional content uploads to over-ride default settings in initial Origin ULP author settings in individual ULPs only. This saves having to return to the Origin ULP of long strings but prevents need to overload site with unused content ready ULPs.

Related ULP Identity Edits

Find Any ULP By Name

[281] Allows an author or recipient to locate similar ULPs from anywhere in the string with a single click using the ULPs given title or by filling in a search window

Set ULP By Number, Word, Image, File Name

[282] (All under one dropdown with multiple option activation) Allows override the default settings of Origin ULP title setting from anywhere within a string by author.

Drag & Drop ULP

[283] See above, default functions of both ULPs.

Hide Edits

Allow Recipient

[284] Allows fast posting by using default recipient settings in Origin ULPs by author. Allows alteration of recipient from drop down for particular ULPs during posting in one particular ULP.

Allow permissions

[285] Allows fast posting by using default permission settings in Origin ULPs by author. Allows alteration of permissions from drop down for particular ULPs during posting in one particular Related ULP

Allow ULP Hides

[286] Allows over ride of default setting of deliberately excluded users from anywhere in a string by author in one particular ULP.

Allow ULP Transparency

[287] Allows over ride of default settings in Origin ULP by author in one particular Related ULP in the same string. Allows for the potential sharing of non-private material by other users from within the LPN without compromising the privacy of the LPN

Allow Thumbnails

[288] Allows over ride of default settings in Origin ULP by author in one particular ULP. Thumbnails may be voluntarily viewable to users outside an LPN along with default ULP's title and username

Allow String Notifications

[289] Allows over ride of default settings in Origin ULP by author in one particular ULP.

Copy Permit Settings

[290] Allows an author or recipient to copy another authors permit settings to their own ULPs. Automatically copies every setting except recipient access not authorised to the new author.

Search Similar Names/Codes

[291] Allows an author or recipient to find similar users on different tables and strings. Facilitates the conglomeration of authors for goods, services and jobs markets etc. Together with Search Similar Settings increases twofold the focus of a relevant search and together with Related ULP settings increases it four fold.

Search Similar Settings

[292] Allows an author or recipient to find particular nuances of settings they may wish to maintain and continue with a new ULP posting. Copy and Paste Settings in Related ULPs allows quick transfer to new Origin ULP.

[293] Enables the avoidance of confusion of relationships in a large group of users.

Hide ULP From View

[294] Allows the consensus elimination of irrelevant posts (see discussion under 'Consensus Based Self-Moderation' herein).

Save and Share ULP

[295] Enables an author or recipient to forward a single ULP as a hyperlink (based on its n-dimensional axis position) to any interested person who may or may not be a member of the LPN on the Binary Modular Platform system.

[296] Automatically breaks all notification links except to contained external public site hyperlinks and allows viewing of selected ULP contents only if the original author has settings of individual ULP on publicly viewable and/or shareable.

Set Mass Content Dump Limit

[297] Nominates the last Related ULP of the first line of a proposed table. Allows for the entire contents of an original digitised document to be parsed by the Binary Modular Platform system by filling only the first line of content into the platform. See explanation of procedure in Origin ULPs.

EXAMPLES

Example 1 – Parts List to create a BMDocument

[298] A standard manufacturer's parts list that contains serial numbers and descriptions as part of the organising material can be turned into an expandable marketing, inventorying, surveying, ordering and notification tool called a Binary Modular Document.

[299] The binary modular platform may further include a Mass Content Dump feature which, in operation, inserts the first row of an original static excel document into a first row of ULPs that then automatically loads the rest of the table into a new Binary Modular Document (BMDocument – refer to the definition of this term as defined herein). This new BMDocument of ULPs is sent to clients who can then cherry-pick the rows that suit their needs without changing the interactivity or integrity of the original table for anyone else who receives it. Each original row becomes an interactive string of ULPs that any recipient can attach two-way inventory and ordering ULPs to, or invite special interest groups to join the LPN who may blog about and promote those products, or customers who may wish to buy them on a regular or irregular basis.

[300] As each retailer, supplier or client joins a BMDocument, their own privilege and recipient settings determine their communication paths within the network. The rows of ULPs attached to the original BMDocument will grow as long as needed and all users can access and exploit just the part of a BMDocument that is useful to them without compromising the data in either direction of them. A single tabulated 'document' such as a motorbike spare parts list for example, can be modularized into networks around which everyone who has anything to do with motorbikes can join in. Even bloggers and YouTubers can connect and engage with manufacturers and retailers to create huge omni-directional supply chain networks based not just on the goods but on all the information about those goods as well. The modular interface means all users can access the table in a way that suits their needs.

[301] The initial BMDocument is only editable by its author but gathers links to every group or person who joins the LPN so the author can thereby notify everybody into the future of any relevant changes to a parts list table. This eliminates the need to go through a separate platform such as email or a subscription page to add new suppliers and retailers or notify existing and future customers of changes. It also eliminates the need for total new document

update and resend, as each line of an original BMDocument becomes the individual live update portals for the whole Document, as it exists on many different user interfaces.

[302] As each retailer and/or supplier joins the LPN, their own privilege and recipient settings determine their communication paths within the LPN. The initial BMDocument creator maintains an original BMDocument that remains as first assembled for them, even as it becomes an expandable ordering portal, inventory tool, marketing survey tool, tracking notification system, etc., for everyone else. Even though the BMDocument in its original uploaded form remains distinct and uncorrupted, everyone using the list can transform it to suit their own needs without compromising anyone else's use of it. This enables the list to be a direct marketing and product survey tool both for the authors of the table but also any retailers or suppliers who join the supply chain.

[303] A manufacturer updates a BMDocument by 'editing' the relevant ULP in the table at their head office. The entire network of users will then automatically have their BMDocuments or parts thereof updated and be notified. In the other direction, any user of the BMDocument can upload content relevant to them into a ULP string (or BMDocument row) and a manufacturer/author can choose to be notified of these uploads about their products using their own notification settings. The strings of ULP can grow as long as it is long but all users of it can fully inhabit and exploit just the part of it that is useful to them without debilitating access to the content in either direction of them.

[304] The original BMDocument is only editable by its author but the table joins to its notification system every group or person who plugs their own ULPs into it so the original up loader can notify everybody in a network of any relevant changes to a parts list table. This eliminates the need to go through a separate platform such as email or a site-subscription page to add new suppliers, retailers or customers. The platform may also be configured to provide functionality to send recall notices and make obsolete the need for total document update and resending, as each ULP of an original BMDocument is by default the live update link for the whole table. At any point in the supply chain users can add their own drag and connect a banking-function ULP if they're selling something of relevance to the original BMDocument or can include links back to their own selling networks in the platform.

Example 2 – Special Interest Groups

[305] For special interest groups, many like-minded participants upload to the same string with a consensus filtering system ensuring that the most relevant information is maintained for the LPN as a whole. (See Consensus Based Self-Moderation in uncommon definitions.)

[306] The main difference between the Binary Modular Platform system **100** described herein and conventional social media or content sharing software is that no third party acts as a convenor, censor, categoriser or moderator of the group's use of content or members of the group itself. Maintaining a logical, personal and non-hierarchical search system revolves around key words, relevance bias and the intentions of the group as a whole rather than by an external or designated organiser or moderator. A mentor or 'leader' of a group could maintain hierarchy only by the agreement of at least 51% of other members of that group. Therefore hierarchy or exclusivity cannot be imposed on this platform. It can only be voluntarily acquiesced to.

[307] Growth of an LPN and their relevant content collection is controlled by a high deletion rate of irrelevant or outdated information. '*Hiding From View*' of any ULP considered irrelevant removes that ULP by unplugging it from the users notification system. At the point which 50% of the LPN has incrementally made the same decision, the ULP is unplugged from the notification system of all members of that LPN making it invisible to all users within that LPN. Eventually the Binary Modular Platform removes it entirely if an unplugged ULP subsequently remains inactive. Consensus Based Self-Moderation eliminates the need for internal or external moderators and makes the decision effective immediately for the 50% of users in a group who choose to activate it. Hiding a Related ULP clears just that ULP from view while Hiding an Origin ULP clears it and the entire string of Related ULPs associated with it. In social cohesion terms, a non-active contributor or offensive and irrelevant content will drop out of an LPN unless 51% of members deem it to still be relevant but 49% don't have to see it or waste energy on it in the meantime, and it will eventually drop off the Platform if not activated by the user so excluded.

[308] Of course the smaller a group the faster complete deletion occurs but for the purpose of maintaining the Binary Modular Platform system **100** described herein can expect to store long-term a manageable fraction of the content that actually goes through the platform.

[309] Each group using an LPN on the Binary Modular Platform system will behave like a vibrant community that reflects the current psychological existence of its members rather

than a growing historic archive that eventually becomes overloaded with content out of step with its current users. As no one person controls the addition and removal of any other members in an LPN, the community that gathers has to behave in a way that encourages a consensus assessment of relevance to maintain the community. The community exists as the preeminent entity driven by group preservation and not by external non-group considerations. As the access permissions required in opening ULPs involves binary ULP settings on each distinct ULP as well as both account holder's identity settings, the contained content remains largely inaccessible outside the LPN community, making flaming or trolling very easy to control. Because the system relies on Locatable Private Networks in which everyone has the right to delete offensive content immediately, flaming or trolling does not have to be tolerated or brought to a moderator's attention as under usual hierarchical content posting and archiving conditions. The constant reality of rapid banishment for infractions will discourage irrelevance and likely eventually prevent 'flaming' and 'trolling' entirely as users of the communications network are acclimatised to a non-hierarchical Platform in which their privacy and autonomy is completely accounted for.

[310] The Binary Modular Platform system **100** described herein creates access to vast amounts of similar content collected and collated by like-minded individuals in a potentially infinite number of previous similar searches. Because each user marks the ULPs as the searchable parameter, it eliminates the need for other individuals to conduct separate searches using similar key words or numbers. A user joining a group will potentially receive a library full of pre-searched results collected by a community of the like-minded.

[311] However, instead of relying on a universal cataloguing system such as the well-known Dewey Decimal System, the cataloguing and search-ability is entirely dependent on the language and intentions of the group members. Trawling through the content uses recognition of preference bias in others, which greatly accelerates the formation of virtual communities in LPN's augmented by the fact the ULPs work as easily with private messaging as they do with raw content uploads. Although users may remove themselves from a string and any selected content ULPs they alone contributed, or from an LPN as a whole, the resultant content collection remains largely unaffected in terms of usability to the LPN, as it's a shared entity maintained by relevance to at least 50% of the group at all times in the total privacy of an LPN.

[312] The main difference between the binary modular systems disclosed herein and conventional social media or data sharing software is that no one person or bot acts as a

convenor, censor, categoriser, administrator or moderator of the member's content so that no user's content can be removed from the platform unless 51% of members consent to it. Maintaining a logical, personal and non-hierarchical search system revolves around current concept and vernacular and the intentions of the network as a whole, rather than by an external administrator, filter algorithm or designated internal organiser or moderator.

[313] Growth of a network and its data collection is managed by a high deletion rate of irrelevant or outdated information. 'Hiding' any ULP considered irrelevant eventually removes that data from the network entirely. The possibility of banishment will discourage irrelevance and prevent flaming and trolling within networks but unplugging from a network does not banish such users from the Platform itself. Flamers and trolls can still access the Platform but they'll eventually end up in networks dedicated only to flaming and trolling each other. Any ULPs unplugged from a network have an activity counter attached that notifies the user concerned if no activity is registered for a period. If no reply to such a notice is registered the content is deleted entirely. In this way the binary modular systems disclosed herein will only store long term a sizable fraction of the content that actually goes through the platform disclosed herein and the users themselves will determine elimination simply by doing nothing. Archiving is not a default situation.

[314] The binary modular systems disclosed herein creates access to vast amounts of data collected and collated by like-minded individuals in previous searches. It's the difference between individually searching alone through millions of possibilities in a single Google search and searching through a list already compiled from Google by many other like-minded people who collated the information for you into a network of conceptual relevance. Because each user titles the ULPs as the searchable parameter, it eliminates the need for others in the network to conduct separate searches using similar key words or numbers. A user joining a network will receive a collection by a community of the like-minded. Trawling through data uses preference bias in others, which greatly accelerates the formation of virtual communities augmented by the fact ULPs work as easily with private messaging as they do with raw data uploads so users are not restricted by having to shift, for example, from a website to email.

[315]

[316] Networks formed in the binary modular systems disclosed herein will behave like vibrant communities that reflect the current existence of their members rather than an historic archive out of step with its users. As no one person controls the addition and removal of any

other member in a network the community has to have a consensus based assessment of relevance to maintain the community. The community is driven by internal preservation and not by external or moderated considerations.

Example 3 – Academic Collaboration

[317] For academics, the Binary Modular Platform system **100** described herein enables thousands of documents to be shared with distinct focusing of the recipients by every contributor at the same time as allowing informal general discussion in the total privacy of an LPN.

[318] The Binary Modular Platform system **100** allows members of broad or narrow interest groups to access and sift many content strings relevant to their own needs directly to a single page on their desktop or device, without the need to trawl through past history or have one's mailbox inundated. Academic users can isolate documents or matters of interest from within disparate groups and sub groups in various strings, without the need to search separately from memory or remind other participants to forward it all in the same LPN

[319] All documents or links to documents are 'temporarily' stored on the Binary Modular Platform system **100** with recipients given or denied access as required and being solely responsible for any archiving. Each new Origin ULP **101A** represents new recipients but existing users can add layers of Origin ULPs within the same string allowing confidentiality and informality amongst many different subgroups. New and existing participants are joined without the need to hand out passwords or repeatedly upload the same documents to email or move from one platform to another to discuss and share documents with different parties.

[320] Of particular interest for academics is the ability to receive notification for any changes to or uploads of the ULPs that are engaged with, which would allow live editing of complex theory discussions without losing track of the development of nuanced alternatives or special interest discussions elsewhere. This would facilitate remote conferencing on a grand scale with archiving a sole responsibility of each of the attendees. Delivering 'edit in progress' papers and conducting confidential side conferences is possible and many different confidential, privileged and focused discussions within a potentially vast discussion board is greatly enhanced, all with the confidence that the entire proceedings are not recorded anywhere other than with whom they are privileged to be recorded or archived.

Example 4 – Secure Communication

[321] The Binary Modular Platform system **100** described herein allows the completely secure transfer of information between people or groups. Unauthorised acquisition of any content whilst in the custody of the Binary Modular Platform system **100** is virtually impossible. The Binary Modular Platform system **100** is the hosting agency for all the LPN's **101** but, similar to a safe deposit box repository, the system has no interest in knowing, and no regular way of accessing the content once it's deposited in a ULP within an LPN. Transparency of an ULP is possible but only to a logged-in author viewing their own ULPs using thumbnails. From outside an LPN the username and title of the ULP is visible with thumbnails of content voluntarily visible. The content of a ULP may be shared by users with others outside an LPN or even outside the Platform, but only if the original author allows it and only by breaking all links back into the LPN and the Platform.

[322] The site itself has secure foyers. Foyers in this context means at the moment of upload of content and opening of a content ULP, the content ULP is not linked to the rest of the platform, only the user name account connected to the particular ULP. The ULP is therefore like an anteroom, airlock, or foyer in respect of the rest of the platform. While it is at the user's interface being either loaded into the platform or opened from the platform, it may be overlaid with an algorithm searching for malware, shadow IP addresses that may belong to a hacker, cookies that will interfere with the platform, or the like. Malware scrubbers warn against and prevent incursions into the main content-base via or from users.

[323] In terms of external security unrelated to the internal 'foyer' security the continuously rearranging and changing barrier of the Binary Lock has significant resistance to cracking by any intruder. The Binary Modular nature of the ULPs of the system **100** means that where a six-part Binary Lock security system is utilised as a subscriber only sanctioned system, a hacker has to attack two separate computers at once at a minimum and if lucky enough to get past the first four passwords must crack the last two that are secret even from the users and the Platform administrators. The complexity of the task for the intruder is somewhat simplified when only the freely available standard security four-part Binary Lock system is employed, but still poses significant hurdles to be overcome, (being, at a minimum, twice as difficult as commonly available security arrangements by virtue of the binary construction of the site) before access to any information stored with the site can be accessed maliciously. As soon as a user gains more than a single recipient in their contact lists they gain that users Binary Locks on their shared content as well. This doesn't slow down the users access to the

content of any ULP in an LPN they are privileged to as they are already inside the Binary Lock system when they log into the Platform and they therefore have immediate access to their own and shared content The Binary Locks are not there for a user to negotiate, they are there to stop a user accessing other people's content within an LPN without permission, to stop anyone following a user into the LPN's on the Platform via that user's browser, or getting into the LPN's on the Platform from any other browsers.

[324] Even though the Binary Modular Platform system 100 relies on links between ULPs within distinct strings, tables, 3-D grids and LPN's, it has no link between the name or code of an ULP and its content and no link between separate strings, tables, 3-D grids and LPN's. A Binary Lock of one version or another is in place with respect of every individual ULP in an LPN as a default aspect of the Binary Modular construction of the system **100** as a whole.

[325] The binary modular systems disclosed herein is the Giant Host (discussed above) for all the ULPs but, similar to a safe deposit box repository the platform has no interest in knowing and no regular way of accessing the content once it's deposited (although the ability for access may be provided where the content is the subject of a Court order or warrant from a law enforcement agency). The platform has no link between the name or code of a ULP and its content, no link between separate Networks and a Binary password on every ULP. Transparency of a ULP with thumbnails is possible but only to a logged-in user viewing their own ULPs, or if they give permission, to members of the network or to the public on the platform as a whole. The platform may also be adapted to use thumbnails as part of the 'vernacular' self-search function in further arrangements of the platform and may also be adapted to create publicly viewable content in selected ULPs in line with the social media needs of networks.

[326] The preferred arrangements of the binary modular systems disclosed herein are provided with a secure foyer in the software that recognises shadow IP addresses in the background of member's attachments at content loading of ULPs. This is intended to deny access for proxy servers with potentially malicious intent. This secure foyer keeps pending ULPs separate from any network before closing and attachment occurs. Because of the containment of the ULPs the main database is inaccessible from anywhere but the platform's own servers. Malware scrubbers may additionally be provided to prevent incursions into the notification system via network members and the continuously rearranging and changing barrier of the Binary passwords has monumental resistance to cracking.

Example 5 – Content Collation

[327] The Binary Modular Platform system **100** described herein is basic and versatile enough to collect and collate any content that may be relevant only to a single person or business for only a limited time.

[328] Content from many sources and formats can be channelled into the Binary Modular Platform system **100** and located onto a single content repository opened by a link from tab history or device. All social media, home maintenance, banking, shopping, and calendars etc., can be collated by personal priority. Distinct friends from social media sites can be filtered out from all other discussions in one string. Individual page links from relevant merchant sites can be isolated into another and pending contracts and meetings in a diary onto another string. Dragging and dropping the strings into preference order has the effect of sorting the individual user's priorities. As well as sorting out priorities more easily, the Binary Modular Platform system **100** allows for a continual refreshment of those priorities by simply adding a new ULP to an existing string and hiding an old ULP allowing for new friends, new products, new contacts and new contracts with the whole string shuffling up to reflect the current situation.

Example 6 – Marketplace Solution

[329] Whole marketplaces for individual items where anyone joining the LPN marketplace can sell the same thing but in any way they want to.

[330] A virtual market place need only sell a single type of item relevant to all buyers and sellers of that item based only on the name used as a link to join the parties. In the non-hierarchical virtual world there is no actual need to base 'selling' per se in one place because the Interface is not an entity fixed by the content. The Binary Modular Platform system **100** therefore eliminates the third party market-place host where many different things are sold with commissions and within limited definitions and terms of sale, and replaces it with absolutely no limit on how and what can be sold other than the statutory limits of each country and a miniscule financial transaction licence. More than just selling and buying anything in a platform market place dedicated to a particular item only, anyone can add forums, blogs, YouTube links, chat and photo swaps. Anything of relevance to the items being sold, or simply of relevance to the buyers and sellers in their unique community, can be added to the string. Because the Binary Modular Platform system **100** enables a genuine online version of the traditional village market place the information being exchanged

between buyers and sellers becomes a crucial reason for joining. A new market could spring up every single day exchanging similar items but the 'Search Similar' function will allow for many different people to quickly join together in special interest markets free from external third party exploitation or compulsion and formed in a way that suits their aesthetic ideals and their entrepreneurial limits.

[331] Every market string thereafter exists and grows according to the amount of sellers joining and leaving the 'market place' LPN without third parties determining how and where they will categorise or sell their products or gouging them for the 'convenience' of auctioning or selling at traditional hosted sites. All buyers and sellers are free to participate in the social aspect of belonging to a market place by joining in discussions or developing marketing pitches or morphing entirely into other areas of interest with new circles of interest. Arrangements of the Binary Modular Platform system **100** will be configured to be able to take a small weekly transaction fee for activating a chosen banking licence with respect to content ULPs within the system **100** but otherwise removes itself entirely from the LNP member transactions and how they are conducted.

Example 7 – Job Board Solution

[332] The Binary Modular Platform system **100** described herein may in some arrangements be configured to provide user controlled job board sites that do away with third party control of information exchange.

[333] In a similar way to a goods market outlined above a jobs market can be something much more like a local community noticeboard and much less like an international or national job search website. In the Binary Modular Platform, people seeking and offering the same type of job would end up on a single LPN with self-moderation clearing out redundant jobs using the Consensus Based Self-Moderation system and continually updated with new jobs, with no third party controlling the clearing out, the conversations or contact information. Thousands of individual job specific market place LPN's would form similar to the Market Place application where everything of relevance to that specific job type in any format of content could be posted free of charge, unless a banking or advertising licence is required.

[334] To maintain privacy a job provider could use a template for posting that has a job description and general contact details guide for both job applicants and job advertisers loading to the string to initiate more detailed job invitations. There would be nothing stopping

alternative templates being posted and as such whole recommendation strings with blogs and links available would form alongside all the job market strings, including resume sellers, clothes and deportment advice, extra-curricular training, etc.

[335] Searching by job type, remuneration levels, location or any other standard and non-standard parameter would be possible in a market string because job providers just use the naming function of the ULPs to focus their postings and those who receive them.

[336] The Binary Modular Platform system **100** described herein would also allow for far more of the personal and localised 'word of mouth' elements of job and employee hunting that can be found in semi-rural areas or village type situations where external competition or publicity may not be desired or useful and the parties can be protected by being in an LPN. Instead of using a job title for search-ability such posters could use job title, location and local dialect to immediately focus themselves away from standard large job sites or large job market strings in the Binary Modular Platform system and therefore maintain a level of privacy in a small community.

Example 8 – Services Noticeboard

[337] The Binary Modular Platform system **100** described herein in alternate arrangements can be configured to form a services market noticeboard, similar to the construction of a goods market and a jobs market.

[338] A traditional 'Yellow Pages' type service-listing host is restricted by the amount of content that can be stored versus the profit from advertising and the cost of hierarchically administering a massive common database including keeping content up to date and accurate. Compared to the near total lack of labour costs of an LPN 'database' that is being self-administered and kept up to date by the LPN participants for free.

[339] The Binary Modular Platform system **100** allows a service provider to join with other similar providers in their area, or their entire nation, to create informal and formal 'associations' that can correct and augment their own posts with video tutorials, advice strings, whatever! Strings can still have google earth and website links, phone numbers etc. but can be anything else the providers feel like adding to their advertised services. As soon as a group is formed the Consensus Based Self-Moderation system ensures that each association maintains relevance and accuracy to itself with everyone acting as administrator and moderator of the string. Any members of an 'association' hidden off an LPN can simply set up a new LPN relevant to their followers but any true professional associations would

disassociate as usual, and in any case they and their customers looking for those services will be equal definers of the search parameters they can use, making 'false associations' extremely difficult to maintain.

Example 9 – Live Chat Solution

[340] Direct text-editing option in a single ULP creates a live 'Chat' application where the ULP becomes a secure channel between designated users.

[341] In this arrangement of the Binary Modular Platform system **100**, the ULP's update notification functionality together with Update ULP Content and Allow ULP Transparency to enable continuously deleted archive-less chat forums with the option to create a permanent record in hard copy off-site and add different content formats in Related ULPs if necessary. Similar to SnapChat™, it allows for a user to copy or preserve their own content but not the reply of the recipient unless permission to do so in recipient ULPs is enabled. Once a body of text has been sealed in the ULP it becomes open-able and readable by permitted recipients, but once the reply is received an acknowledgement requires the Update ULP Content to be activated. This automatically deletes the content making the ULP ready for new content, hence the Transparency option to allow authors to read their own initial words before continuing.

[342] The Binary Modular Platform system **100** allows groups of 'friends' to exchange content free of the restrictions found on social media networks Facebook™ (prudishness, censorship and generalized friendship categories) or Twitter™ (size restrictions) and excludes the possibility to continuously enrage or obfuscate others with permanently preserved reams of irrelevant text and the inability to permanently remove antagonists. The ability to set and block recipients and the consensus deletion system will keep it relevant and courteous for all users in a friendship group.

Example 10 – Multiple Intranets

[343] The binary modular systems disclosed herein may be configured to provide multiple intranets within existing intranets, for example, tailored to the requirements and needs of either Government or Corporate organisations.

[344] The notification system, vernacular switching functions and binary modular settings (discussed above) enabled by the binary modular systems disclosed herein provide a limitless number of layers of access within the one system. For example, a multi layered intranet that

doesn't need to store its separated recipient groups on separate secure servers because each ULP is twice as secure as the platform itself and can be as distinctly addressed as required.

[345] Instead of separate levels of hierarchy in a typical bureaucratic system having to exist on separate servers, all the levels can exist in one system with many times more levels of security that a usual layered gatekeeper type system. This frees governments and corporations from the need to have separate secure servers filling up the basement or having tech staff to keep internal systems running. The binary modular systems disclosed herein also allows a government or corporation to conduct notification, survey and information functions all in the same system with the same recipients list much like the supply chain system mentioned above.

[346] In addition, the Ultra-secure version of the Ghost Security systems enabled by the binary modular systems disclosed herein, i.e. incorporating a 6 part Binary password and encryption regime exclusive to each subscription of purchase may additionally be configured to provided fractured file and encrypted cloud storage as users simply won't need separate secure servers anymore as the security of the networks and configurations formed using the binary modular systems disclosed herein is many orders of magnitude greater than existing password-protected systems.

Example 10 – Mass Content Dump Feature (BMDocument).

[347] Uses the prefix/suffix attribute of the Binary ULP system to create interactive tables from static content tables such as parts lists, product inventory lists, contracted task lists etc. A Origin ULP followed by the required number of Related ULPs forms the first line of any table with their content being the first row of every column in an original table.

[348] The user setting a designated line of ULPs to replicate itself and automatically fill itself from the subsequent rows of the columns, reforms the new table Document in the Binary Modular Platform system **100**. Each line in the Document then becomes an interactive string that can be added to by users to whom the table is sent by the original author and all subsequent recipients. All subsequent users form the community around the Document with various additional attributes provided and accessed by all the users with their own preference settings in the Binary ULPs being able to join the LPN that has that Document as its core raison d'être.

Example 11 – Binary ULP Computation.

[349] Another potential major application of the principals of the Binary Modular Platform would require a distinct and separate design of the ULPs. Particular arrangements of such a ULP would not include Binary Locks or separate account holders in an LPN and therefore would be incompatible and unusable on the normal Binary Modular Platform with LPN's as described in the rest of this Specification. The new design would be ULPs capable of running 'Bipolar titles', 'Bipolar titles' here means an adjustment of the binary module system to create a 'title' relevant to both the input and the output part of a calculation on the same ULP such that is can be assembled in a modular fashion to other bi-polar ULPs but only in a head to toe means in direct correlation to the sequence of calculations.

[350] In terms of speeding the process of massive calculations such as DNA sequencing many-fold, both parts of the computer must inform the other of correct and incorrect paths of calculation and must package the calculations so that only the input and the output relevant to that sequence of calculations is available as bipolar titles on the content ULPs.

[351] This separate design would have the ability to condense a large amount of calculations into bi-polar ULPs of results that can be used to speed up the calculations being carried out in a concomitant computer. This is not the same as two computers carrying on a similar quest. It is two parts of a computer or many computers acting in binary unison enabling one part to inform the other part of results before either part has wasted time on the same calculations. Either part of the computer can use these completed calculation in further stages of calculation, without having to run those parts of the calculations again.

[352] The self-searching ability of the bi-polar ULP platform enables these calculations to be used in similar or vaguely similar applications without having to repeat the calculations or with various assumptions garnered and used to focus calculations between many different computers engaged in any number of processes where a package of results might have application. The title searching abilities of the bi-polar ULPs can be automated in this system above a level of assumption and set and tested by a human user below it.

[353] Basically, a series of calculations can be separated into sequential order by precedent or prior knowledge and stored for use in later calculations. In terms of DNA sequencing for instance, an amount of the calculations may already have been performed for a similar species and can be stored as calculated parts for accelerated future calculations within the

Binary ULP system. The system can then self-search for the fastest way through a new calculation using previous calculations to accelerate the process.

COMPUTING DEVICE

[354] **Figure 3** shows a computing device **300** adapted for methods and systems for a binary modular, self-searching platform for non-hierarchical electronic content organisation in a program application adapted for use on the computing device. In particular arrangements, computing device **300** is adapted to comprise functionality for communication with the network **320** (for example, the internet), storage capability (such as a content-base) for storing user account content and the like.

[355] As is described above, the system **100** provides a system for methods and systems for a binary modular, self-searching platform for non-hierarchical content organisation. The system **100** depicted in **Figures 1, 2A**, **2B**, **4A** and **4B** may be implemented using a computing device / computer system **300**, such as that shown in **Figure 3** wherein the system **100** may be implemented as software, such as one or more application programs executable within the computing device **300**. Accordingly, it will be appreciated by the skilled addressee that computing system **300** is inextricably linked to the provision of non-hierarchical system **100** for organisation of content. In particular, the functions and operations of system **100** are affected by instructions in the software that are carried out within the computer system **300**. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The software may also be divided into two separate parts, in which a first part and the corresponding code modules performs the described methods and a second part and the corresponding code modules manage a user interface between the first part and the user. The software may be stored in a computer readable medium, including the storage devices described below, for example. The software is loaded into the computer system **300** from the computer readable medium, and then executed by the computer system **300**. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer system **300** preferably effects an advantageous apparatus for methods and systems for a binary modular, self-searching platform for non-hierarchical content organisation based on the binary construction.

[356] With reference to **Figure 3**, an exemplary computing device **300** is illustrated. The exemplary computing device **300** can include, but is not limited to, one or more arithmetic

logic unit or central processing units (CPUs) **301** comprising one or more processors **302**, a system memory **303**, and a system bus **304** that couples various system components including the system memory **303** to the processing unit **301**. The processor(s) **302** may each be a reduced instruction set computer (RISC) or complex instruction set computer (CISC) processor or the like. The system bus **304** may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The bus subsystem **304** may offer parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like.

[357] Computer program code instructions may be loaded into the device memory **303** from the HDD **311** or from the network **320** using network interface **322**. During the bootstrap phase, an operating system **308** and one or more software applications or program modules **309** are loaded from the storage device into the memory **303**. During the fetch-decode-execute cycle, the CPU **301** fetches computer program code instructions from memory **303**, decodes the instructions into machine code, executes the instructions and stores one or more intermediate results in memory **303**.

[358] In this manner, the instructions stored in the memory **303**, when retrieved and executed by the CPU **301**, may configure the computing device **300** as a special-purpose machine that may perform the functions described herein.

[359] The computing device **300** also typically includes computer readable media, which can include any available media that can be accessed by computing device **300** and includes both volatile and non-volatile media and removable and non-removable media. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes media implemented in any method or technology for storage of information such as computer readable instructions, content structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by the computing device **300**. Communication media typically embodies computer readable instructions, content structures, program modules or other content in a modulated data signal

such as a carrier wave or other transport mechanism and includes any information delivery media. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[360] The system memory **303** includes computer storage media in the form of volatile and/or non-volatile memory such as read only memory (ROM) **305** and random access memory (RAM) **306**. A basic input/output system **307** (BIOS), containing the basic routines that help to transfer information between elements within computing device **300**, such as during Origin-up, is typically stored in ROM **305**. RAM **306**- typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit **301**. By way of example, and not limitation, **Figure 3** illustrates an operating system **308**, other program modules **309**, and program data **310**.

[361] The computing device **300** may also include other removable/non-removable, volatile/non-volatile computer storage media. By way of example only, **Figure 3** illustrates a hard disk drive **311** that reads from or writes to non-removable, non-volatile magnetic media. Other removable/non-removable, volatile/non-volatile computer storage media that can be used with the exemplary computing device include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive **311** is typically connected to the system bus **304** through a non-removable memory interface such as interface **312**.

[362] The drives and their associated computer storage media discussed above and illustrated in **Figure 3**, provide storage of computer readable instructions, content structures, program modules and other data for the computing device **300**. In **Figure 3**, for example, hard disk drive **311** is illustrated as storing an operating system **33**, other program modules **314**, and program data **315**. Note that these components can either be the same as or different from operating system **308**, other program modules **309** and program data **310**. Operating system **313**, other program modules **314** and program data **315** are given different numbers hereto illustrate that, at a minimum, they are different copies.

[363] The computing device also includes one or more input/output (I/O) interfaces **330** connected to the system bus **304** for communicating with one or more peripheral devices including an audio-video interface that couples to output devices including one or more of a

video display **334** and loudspeakers **335**. The I/O interface **330** may offer both serial and parallel interface connectivity. For example, the I/O interface **330** may comprise a Small Computer System Interface (SCSI), Universal Serial Bus (USB) or similar I/O interface for interfacing with computing device **300**. Input/output interface(s) **330** also couple(s) to one or more input devices including, for example a mouse **331**, keyboard **332** or touch sensitive device **333** such as for example a smartphone or tablet device. The I/O interface **330** may also comprise a computer to computer interface, such as a Recommended Standard 232 (RS-232) interface, for interfacing the device **300** with one or more personal computer (PC) devices. The I/O interface **330** may also comprise an audio interface for communicate audio signals to one or more audio devices **335**, such as a speaker or a buzzer.

[364] Of relevance to the descriptions below, the computing device **300** may operate in a networked environment using logical connections to one or more remote computers. For simplicity of illustration, the computing device **300** is shown in **Figure 3** to be connected to a network **320** that is not limited to any particular network or networking protocols, but which may include, for example Ethernet, Bluetooth or IEEE 802.X wireless protocols. The network **320** may be a wired network, such as a wired Ethernet™ network or a wireless network, such as a Bluetooth™ network, IEEE 802.11 network, or cellular network (e.g. a 3G or 4G telecommunications network). The network **320** may be a local area network (LAN), such as a home or office computer network, or a wide area network (WAN), such as the Internet or private WAN.

[365] The logical connection depicted in **Figure 3** is a general network connection **321** that can be a local area network (LAN), a wide area network (WAN) or other network, for example, the internet. The computing device **300** is connected to the general network connection **321** through a network interface or adapter **322** which is, in turn, connected to the system bus **304**. In a networked environment, program modules depicted relative to the computing device **300**, or portions or peripherals thereof, may be stored in the memory of one or more other computing devices that are communicatively coupled to the computing device **300** through the general network connection **321**. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between computing devices may be used.

[366] The above-described arrangements/embodiments of the present disclosure can be implemented in hardware, firmware or via the execution of software or computer code that can be stored in a recording medium such as a CD ROM, a Digital Versatile Disc (DVD), a

magnetic tape, a RAM, a floppy disk, a hard disk, or a magneto-optical disk or computer code downloaded over a network originally stored on a remote recording medium or a non-transitory machine readable medium and to be stored on a local recording medium, so that the methods described herein can be rendered via such software that is stored on the recording medium using a general purpose computer, or a special processor or in programmable or dedicated hardware, such as an ASIC or FPGA. As would be understood in the art, the computer, the processor, microprocessor controller or the programmable hardware include memory components, e.g., RAM, ROM, Flash, etc. that may store or receive software or computer code that when accessed and executed by the computer, processor or hardware implement the processing methods described herein. In addition, it would be recognized that when a general purpose computer accesses code for implementing the processing shown herein, the execution of the code transforms the general purpose computer into a special purpose computer for executing the processing shown herein and integrally linked therewith. Any of the functions and steps provided in the Figures may be implemented in hardware, software or a combination of both and may be performed in whole or in part within the programmed instructions of a computer. Interpretation

Bus

[367] In the context of this document, the term "bus" and its derivatives, while being described in a preferred embodiment/arrangement as being a communication bus subsystem for interconnecting various devices including by way of parallel connectivity such as Industry Standard Architecture (ISA), conventional Peripheral Component Interconnect (PCI) and the like or serial connectivity such as PCI Express (PCIe), Serial Advanced Technology Attachment (Serial ATA) and the like, should be construed broadly herein as any system for communicating content.

In accordance with

[368] As described herein, 'in accordance with' may also mean 'as a function of' and is not necessarily limited to the integers specified in relation thereto.

Composite items

[369] As described herein, 'a computer implemented method' should not necessarily be inferred as being performed by a single computing device such that the steps of the method may be performed by more than one cooperating computing devices.

[370] Similarly objects as used herein such as 'web server', 'server', 'client computing device', 'computer readable medium' and the like should not necessarily be construed as being a single object, and may be implemented as a two or more objects in cooperation, such as, for example, a web server being construed as two or more web servers in a server farm cooperating to achieve a desired goal or a computer readable medium being distributed in a composite manner, such as program code being provided on a compact disk activated by a license key downloadable from a computer network.

Content-base

[371] In the context of this document, the term "content-base" and its derivatives may be used to describe a database comprising user content, such as for example, a single not commonly accessible platform database, a set of separated user accessible LPN databases, a system of tagged interconnected databases or the like. The system of content-bases may comprise a set of databases wherein the set of databases may be stored on a single implementation or span across multiple implementations that by virtue of the binary modular security system are not commonly accessible from inside or outside the Platform. The terms "content-base" or "database" is also not limited to refer to a certain database format rather may refer to any database format. For example, database formats may include MySQL, MySQLi, XML or the like.

Wireless

[372] The invention may be embodied using devices conforming to other network standards and for other applications, including, for example other WLAN standards and other wireless standards. Applications that can be accommodated include IEEE 802.11 wireless LANs and links, and wireless Ethernet.

[373] In the context of this document, the term "wireless" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a non-solid medium. The term does not imply that the associated devices do not contain any wires, although in some embodiments/arrangements they might not. In the context of this document, the term "wired" and its derivatives may be used to describe circuits, devices, systems, methods, techniques, communications channels, etc., that may communicate data through the use of modulated electromagnetic radiation through a solid medium. The term does not imply that the associated devices are coupled by electrically conductive wires.

Processes

[374] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing", "computing", "calculating", "determining", "analysing" or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities into other data similarly represented as physical quantities.

Processor

[375] In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic content, e.g., from registers and/or memory to transform that electronic content into other electronic content that, e.g., may be stored in registers and/or memory. A "computer" or a "computing device" or a "computing machine" or a "computing platform" may include one or more processors.

[376] The methodologies described herein are, in one embodiment/arrangement, performable by one or more processors that accept computer-readable (also called machine-readable) code containing a set of instructions that when executed by one or more of the processors carry out at least one of the methods described herein. Any processor capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken are included. Thus, one example is a typical processing system that includes one or more processors. The processing system further may include a memory subsystem including main RAM and/or a static RAM, and/or ROM.

Computer-Readable Medium

[377] Furthermore, a computer-readable carrier medium may form, or be included in a computer program product. A computer program product can be stored on a computer usable carrier medium, the computer program product comprising a computer readable program means for causing a processor to perform a method as described herein.

Networked or Multiple Processors

[378] In alternative embodiments/arrangements, the one or more processors operate as a standalone device or may be connected, e.g., networked to other processor(s), in a networked deployment, the one or more processors may operate in the capacity of a server or a client machine in server-client network environment, or as a peer machine in a peer-to-peer or

distributed network environment. The one or more processors may form a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine.

[379] Note that while some diagram(s) only show(s) a single processor and a single memory that carries the computer-readable code, those in the art will understand that many of the components described above are included, but not explicitly shown or described in order not to obscure the inventive aspect. For example, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

Additional Embodiment/Arrangements

[380] Thus, one embodiment/arrangement of each of the methods described herein is in the form of a computer-readable carrier medium carrying a set of instructions, e.g., a computer program that are for execution on one or more processors. Thus, as will be appreciated by those skilled in the art, embodiments/arrangements of the present invention may be embodied as a method, an apparatus such as a special purpose apparatus, an apparatus such as a data processing system, or a computer-readable carrier medium. The computer-readable carrier medium carries computer readable code including a set of instructions that when executed on one or more processors cause a processor or processors to implement a method. Accordingly, aspects of the present invention may take the form of a method, an entirely hardware embodiment/arrangement, an entirely software embodiment/arrangement or an embodiment/arrangement combining software and hardware aspects. Furthermore, the present invention may take the form of carrier medium (e.g., a computer program product on a computer-readable storage medium) carrying computer-readable program code embodied in the medium.

Carrier Medium

[381] The software may further be transmitted or received over a network via a network interface device. While the carrier medium is shown in an example embodiment/arrangement to be a single medium, the term "carrier medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "carrier medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of

instructions for execution by one or more of the processors and that cause the one or more processors to perform any one or more of the methodologies of the present invention. A carrier medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media.

Implementation

[382] It will be understood that the steps of methods discussed are performed in one embodiment/arrangement by an appropriate processor (or processors) of a processing (i.e., computer) system executing instructions (computer-readable code) stored in storage. It will also be understood that the invention is not limited to any particular implementation or programming technique and that the invention may be implemented using any appropriate techniques for implementing the functionality described herein. The invention is not limited to any particular programming language or operating system.

Means For Carrying out a Method or Function

[383] Furthermore, some of the embodiments/arrangements are described herein as a method or combination of elements of a method that can be implemented by a processor or a processor device, computer system, or by other means of carrying out the function. Thus, a processor with the necessary instructions for carrying out such a method or element of a method forms a means for carrying out the method or element of a method. Furthermore, an element described herein of an apparatus embodiment/arrangement is an example of a means for carrying out the function performed by the element for the purpose of carrying out the invention.

Connected

[384] Similarly, it is to be noticed that the term connected, when used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression a device A connected to a device B should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means. "Connected" may mean that two or more elements are either in direct physical or electrical contact, or that two or more elements are not in direct contact with each other but yet still co-operate or interact with each other.

Embodiments/Arrangements

[385] Reference throughout this specification to "one embodiment" or "an embodiment" or "one arrangement" or "an arrangement" means that a particular feature, structure or characteristic described in connection with the embodiment/arrangement is included in at least one embodiment/arrangement of the present invention. Thus, appearances of the phrases "in one embodiment/arrangement" or "in an embodiment/arrangement" in various places throughout this specification are not necessarily all referring to the same embodiment/arrangement, but may. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner, as would be apparent to one of ordinary skill in the art from this disclosure, in one or more embodiments/arrangements.

[386] Similarly it should be appreciated that in the above description of example embodiments/arrangements of the invention, various features of the invention are sometimes grouped together in a single embodiment/arrangement, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment/arrangement. Thus, the claims following the Detailed Description are hereby expressly incorporated into this Detailed Description, with each claim standing on its own as a separate embodiment/arrangement of this invention.

Furthermore, while some embodiments/arrangements described herein include some but not other features included in other embodiments/arrangements, combinations of features of different embodiments/arrangements are meant to be within the scope of the invention, and form different embodiments/arrangements, as would be understood by those in the art. For example, in the following claims, any of the claimed embodiments/arrangements can be used in any combination.

Specific Details

[387] In the description provided herein, numerous specific details are set forth. However, it is understood that embodiments/arrangements of the invention may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description.

Terminology

[388] In describing the preferred embodiment/arrangement of the invention illustrated in the drawings, specific terminology will be resorted to for the sake of clarity. However, the invention is not intended to be limited to the specific terms so selected, and it is to be understood that each specific term includes all technical equivalents which operate in a similar manner to accomplish a similar technical purpose. Terms such as "forward", "rearward", "radially", "peripherally", "upwardly", "downwardly", and the like are used as words of convenience to provide reference points and are not to be construed as limiting terms.

Different Instances of Objects

[389] As used herein, unless otherwise specified the use of the ordinal adjectives “first”, “second”, “third”, etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

Comprising and Including:

[390] In the claims which follow and in the preceding description of the invention, except where the context requires otherwise due to express language or necessary implication, the word “comprise” or variations such as “comprises” or “comprising” are used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments/arrangements of the invention.

[391] Any one of the terms: “including” or “which includes” or “that includes” as used herein is also an open term that also means “including at least” the elements/features that follow the term, but not excluding others. Thus, including is synonymous with and means comprising.

Scope of Invention

[392] Thus, while there has been described what are believed to be the preferred arrangements of the invention, those skilled in the art will recognize that other and further modifications may be made thereto without departing from the spirit of the invention, and it is intended to claim all such changes and modifications as fall within the scope of the invention. Functionality may be added or deleted from the block diagrams and operations

may be interchanged among functional blocks. Steps may be added or deleted to methods described within the scope of the present invention.

[393] Although the invention has been described with reference to specific examples, it will be appreciated by those skilled in the art that the invention may be embodied in many other forms. This is especially applicable to the fact that modularity allows for a limitless expansion into the future of possible interfaces in using the content contained in the underlying binary modular elements.

Industrial Applicability

[394] It is apparent from the above, that the arrangements described are applicable to the mobile device industries, specifically for methods and systems for distributing digital media via mobile devices.

[395] It is apparent from the above, that the arrangements described are applicable to the desk top device industries, specifically for the methods and systems for distributing digital media via the internet from and between fixed location devices.

[396] It will be appreciated that the systems described/illustrated herein at least substantially provide a non-hierarchical system for organisation, delivery, storage and management of content based on the binary modular application of just two distinct content packaging module types for the creation of Locatable Private Networks.

[397] In another design using principals of the system it will be appreciated that the systems described/illustrated herein at least substantially provide a non-hierarchical system for the computation of content based on the modular application of just one distinct content packaging module type being used in relay solution solving of complex mathematical problems.

The systems described herein, and/or shown in the drawings, are presented by way of example only and are not limiting as to the scope of the invention. Unless otherwise specifically stated, individual aspects and components of the systems may be modified, or may have been substituted therefore known equivalents, or as yet unknown substitutes such as may be developed in the future or such as may be found to be acceptable substitutes in the future. The systems disclosed herein may also be modified for a variety of applications while remaining within the scope and spirit of the claimed invention, since the range of potential applications is great, and since it is intended that the present systems be adaptable to many such variations.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A non-hierarchical binary modular system for the organisation, storage, delivery and management of content in multiple Locatable Private Networks on an overarching Platform, the system comprising:

at least two upload portals (ULPs) containing information of interest to at least one or a plurality of users, said at least two ULPs each being of a binary compatibility with distinct and inter-related control mechanisms enabling a modular construction, by one or a plurality of users;

connection means for said users to define a logical connection between said at least two modular ULPs being a binary modular platform based self-searching system;

contact means between said users in respect of information of interest being a binary modular platform based omni-directional and private notification system for maintaining real-time interaction;

moderation means for the maintenance of Locatable Private Networks formed on the Platform being a binary modular platform based consensual self-moderation system for maintaining a logical purpose within Locatable Private Networks without site administrators or third-party moderators;

security means for the continued existence of Locatable Private Networks formed by users activating at least one ULP containing information of interest on the Platform, being a binary modular platform based security system formed by binary locks attached to each individual ULP and activated by each individual user subscription to the Platform and each individual user activity on the Platform; and

filing means for the user only placement and retrieval of content by distinct hyperlink using a 3 dimensional point placement of all ULPs into a replicate-able multiple point n-dimensional 3D array, each multiple point 3D array having an ‘n’ reference that allows layering of said multiple point 3D arrays into each other, and each point position being designated by an n-dimensional nomenclature, to create a limitless, anonymous, non-administered, non-hierarchical, compartmentalised and uncommon data-base.

2. The system as claimed in claim 1 further comprising computer program code means for an infinite n-dimensional 3D filing system enabling ‘Locatable’ Private Networks to be visually represented for instant user only access, placement and retrieval purposes, anonymous filing

purposes, fractured encrypted filing purposes, visual interface purposes, all governed by the attachment of ULP to other relevant ULP in a logical user only controlled 3 dimensional sequence into an endlessly replicated (n-dimensional) multiple point 3D array file location.

3. The system as claimed in claim 1 wherein said ULPs are adapted to retain electronic content in multiple formats.

4. The system as claimed in claim 1 wherein said connection means utilises a title associated with each ULP to enable a self-searching function to control the dual purposes of assembly of person into Locatable Private Networks and the collection of the content contained within said ULPs of interest to each individual user.

5. The system as claimed in claim 1 wherein said at least two ULPs are selected from a ULP type comprising either an Origin ULP or a Related ULP for the purpose of assembling Locatable Private Networks.

6 The system as claimed in claim 5 said Origin ULP is adapted for storing content.

7. The system as claimed in claim 6 wherein said Related ULP is adapted for storing content of relevance to said Origin ULP and linking together at least an Origin and a Related ULP in a binary modular way.

8. The system as claimed in claim 7 comprising a plurality of said Related ULPs each comprising a logical connection to at least one or more Related ULPs and to at least one associated Origin ULP and the ability to infinitely add upon said linked ULPs by a plurality of other parties in a Locatable Private Network.

9. The system as claimed in claim 1 further comprising a consensus based self-moderated system for removal of irrelevant content from an established Locatable Private Network.

10. A computer program product having a computer readable medium having a computer program recorded therein for providing non-hierarchical binary modular system for organisation, delivery and management of content in multiple Locatable Private Networks on an overarching Platform said computer program product comprising:

computer program code means for at least two ULPs containing information of interest to at least one or a plurality of users, said at least two ULPs each being of a binary compatibility with distinct and inter-related control mechanisms enabling a modular like construction, by one or a plurality of users;

computer program code means for connection means for said users to define a logical connection between said at least two modular ULPs being a binary modular based self-searching system;

computer program code means for contact means between said users in respect of information of interest being a binary modular based omni-directional and private notification system for maintaining real-time interaction;

computer program code means for moderation means for the maintenance of Locatable Private Networks formed on the Platform being a binary modular based consensual group self-moderation system for maintaining a logical purpose without site administrators or third-party moderators; and

computer program code means for security means for the continued relevant existence of Locatable Private Networks formed by users activating at least one ULP containing information of interest on the Platform being a binary modular based security system formed by binary locks attached to each individual ULP and activated by each individual user subscription to the Platform.

11. The computer program product as claimed in claim 10 further comprising computer program code means for an infinite n-dimensional 3D filing system enabling ‘Locatable’ Private Networks to be visually represented for instant user only access, placement and retrieval purposes, anonymous filing purposes, fractured encrypted filing purposes, visual interface purposes, all governed by the attachment of ULP to other relevant ULP in a logical user only controlled 3 dimensional sequence onto an infinitely replicatable n-dimensional multiple point 3D array file location (xyz@n).

12. The computer program product as claimed in claim 10 further comprising computer program code means for providing a consensus based group self-moderated system for removal of irrelevant data from said modular data packages in their binary constructed format.

13. The system as claimed in claim 1, wherein said security system is formed from the binary modular construction of a ULP shared between at least 2 users and comprising at least 4 unique content elements, at least 2 unique content elements being associated with each one of said at least 2 users and being sufficient for any one user to access their content.

14. The system as claimed in claim 13, wherein said security system is an at least 2 half, binary code system with various unique codes in at least 6 parts of 3 slip-paired format or, at least 7

parts of 3 slip-paired format and universal verification code or, at least 4 parts of 2 slip paired format or, 5 parts of 2 slip paired format and a universal verification code

15. The system as claimed in claim 13, wherein said security system is a code unique 4-part, 2 slip-paired, binary code system.

16. The system as claimed in any one of claims 13, 14, 15, wherein the said at least 2 content elements associated with each of said at least 2 users are selected from the group comprising: a user's password, a user's username plus a random auto generated 3 character extension to the username.

17. The system as claimed in claim 1, wherein said security system being formed from the binary construction of one or more binary upload portals (ULPs) shared between at least 2 users and comprising at least 4 unique content elements, at least 2 unique content elements being associated with each one of said at least 2 users, and a universal verification code.

18. The system as claimed in claim 16, wherein said security system is a code unique 5-part, 2 slip-paired, binary code system.

19. The system as claimed in either claim 16 or claim 18, wherein the said at least 2 content elements associated with each of said at least 2 users are selected from the group comprising: a user's own account access password, a user's username plus a random auto generated 3 character extension, a site-generated universal verification code.

20. A relay solution computational arrangement using a modification of the binary modular system as claimed in any one of claims 1 to 9 comprising a notification system; and a bi-polar ULP title system and a self-search system adapted to accelerate the solving of complex mathematical problems.