ANYI: 一个以个人信息单元为中心的社交网络系统

德辉(dehui_jp@yahoo.co.jp)

传尚（songjlx@gmail.com）

摘要

ANYI网络系统是一个辅助个人社交生活的网络系统。自然人/法人个体和个体间的联系构成了整个网络；无中心平台。

设计原则：个人基本信息、社交关系等没有实体存在的数据同实体物品一样属于个人财产，应该由所有者全权管理。

目标：构建一个遵从现实生活模式的社交网络，以辅助用户的日常生活和提高交互效率。

主要特点：

· 用户数据各自保存，用户间直接交互，无需依赖任何平台，即去中心化。

· 采用非对称加密技术，保证数据存储和网络传输的安全性。

· 以新的合理的信息管理模式为基础，提高信息交互效率。

· 实现信誉的信息化流通，净化虚假消息，促进社交环境良性发展。

· 实现资源性信息的合理流通，结合信誉，使社交资源效益最大化。

1.当今社交课题

得益于互联网等信息技术的高速发展，我们在日常生活中享受着空前的便利。但由技术高速发展衍生的和固有的课题也正在困扰着我们：

· 用户信息安全事故频发。用户信息安全课题已经被全世界关注，人们不放心用社交软件来管理重要信息，甚至放弃使用主流社交软件，这使当前的社交软件重心还只停留在娱乐层面，难以进一步辅助人们的社会生活。

· 互联网上虚假信息和模糊信息泛滥。严重影响了人们对信息的有效利用；不良信息的传播也严重威胁着青少年的成长，影响着社会风气。

· 人们各自为战地甄别信息，难以对应海量信息。判断能力有限的个体的客观存在，缺乏有效的认知共有机制，使得虚假消息有了生存和滋长的空间。

· 信息获取方式原始。在传输速度和范围上我们取得了质的改变，但人们从社交环境中获取有效信息的方式，仍然靠个体的问询或偶然交流。

· 信誉信息缺位。在网络时代里，人们的社交范围更广泛，却没有相应的信誉体系支撑，人们无法得知一个新朋友的信誉状况，既可能遭受损失又可能失去机会。

· 个人敏感信息被习惯性滥用。姓名、住址、电话、邮箱等个人敏感信息，作为标识个人的关键字使用，已经是常态，信息泄露风险也被无可奈何地接受。

· 个人信息交互方式落后。提交个人信息表单的生活场景比比皆是，赶时间 + 人多 + 提交内容繁杂 + 忙中出错的令人慌乱的事情相信每天都在发生着。反复填写纸质或电子的表单的落后低效方式宏观上耗费了我们大量的时间和精力。

· 个人自主信息管理缺位。在普遍的中心化模式下，个人“碎片化”地存在着：存在于社交软件平台的个人社交信息碎片、分散于金融机构的个人资产信息碎片、产生于医院和诊所的个人健康信息碎片、在学校或教育机构或学习网站的个人学习信息碎片……个人难以综合管理自己的信息，个人自主信息管理的必要性被忽视。

试图解决上述问题，我们提出这个ANIY网络系统方案。

2.ANYI网络系统简介

个人信息单元是ANYI网络系统的基本构成单元（后文我们称这个基本单元为结点），结点间通过对等网络技术(Peer To Peer)相互连接形成ANYI社交网络。

结点主要分为数据和软件（对数据的处理）两部分，为确保数据安全，软件部分又细分为中间软件层和应用软件层。

利用非对称加密技术保证数据存储和信息传输的安全性，并将非对称加密的公钥作为能唯一代表个人的ID在ANYI网络中使用。

利用对等网络技术，通过统一的信息交互规则实现结点间的信息交互，从而形成不需要中心服务器的社交网络。

用户自主管理个人信息，ANYI社区定制和维护信息交互规则。基于接口标准的软件部分可以由软件供应商自由提供。软件部分不得超越用户意愿使用用户信息和密钥。

2.1 数据

数据的存储和访问由个人全权管理。

数据独立于应用程序，用户可以自由选择应用程序管理数据。

数据分为个人信息（个人基本信息、资源信息、社交信息、权限管理信息等）和ANYI网络系统设定信息。个人信息以加密形态存储，数据统一以键-值方式存储，并且统一键定义，以确保结点与软件应用的独立性。用户可以自主决定在结点上存储的内容，可以备份感兴趣的来自网络的信息。

ANYI结点统一使用非对称加密方式管理数据，并且以公钥作为能唯一标识用户的ID，在关系建立、定向信息交互/加密、权限控制等共通交互规则中使用。而且可以从公钥衍生出多个ID来对应不同场景，也能满足有匿名性需求的场景。

2.2 中间软件层

中间层负责处理数据、实现网络接口和应用软件层接口。

中间软件层在数据方面，通过读取和使用密钥，实现对数据的加密/解密，以及对数据的访问和存储；在与网络交互方面，使用共通交互接口来实现与ANYI网络的交互；在用户操作界面方面，封装好数据和密钥，向应用软件层提供基本功能接口。

2.4 个人结点的基本规则

ANYI网络系统运行在对等网络协议上，结点遵守以下规则以确保网络运转：

· 结点主动声明登入网络。

· 结点在网络中承担共同信息传输义务：转送目标结点不是自结点的信息。

3.ANYI网络系统的应用场景

3.1 社交

ANYI结点通过共通的交互规则实现社交功能。通过ID管理实现对各种社交关系的合理权限管理：定义权限组合、关系分组。

3.1.1 建立关系和发送信息

双方通过交换ID完成关系的建立，并通过ID进行权限、分组等管理。

双方利用非对称加密技术安全地发送消息：

发送方使用接收方的公钥（ID）加密，附以由自己的私钥生成的签名；接收方用私钥解密信息，用发送方的公钥验证签名确认信息发送者。

3.1.2 建立群组

群组建立和管理自由，群组人数上限由管理员决定。

群组的管理也基于群组成员的ID，可以有多位管理员，可以自由地定制群组管理规则，不必局限于人数上限等平台规则限制。

发送方使用群组内所有成员的公钥哈希加密，使用阈值为1的多重签名规则（1-N），包含在哈希内的任何一个成员都可以解密信息。

3.1.3 不同种类信息的管理和利用

个人日常生活信息通常可分为以下几类：

- 本人利用的信息，如个人备忘录。
- 小范围内分享的即时信息，如漂亮的风景，偶然的感悟。
- 有商业性质等的资源性信息，如工作机会、商品优惠信息等

上述信息的对象、目的等各不相同。ANYI个人结点可以通过分类和权限指定来实现针对每一条信息的自由管理。对于资源性信息，需要以他人能判断有效的时间、空间、对象等为原则，按照合适的规则生成，使其能被准确检索。（具体规则及规则完善由ANYI社区维护）

在符合权限的范围内，用户既能实时地获取信息更新，又可以必要时主动检索取得资源信息。资源信息的可检索性，可以改善刷屏式宣传的现状，避免了收、发信息双方的干扰和时间精力投入。

3.1.4 信誉体系的建立和分享

信誉特点：源于被评价者的言行，受控于评价者；信誉观点可分享。

信誉是人类社交活动中极其重要的一环，商业中的信用管理早就被广泛重视，金融业的个人信用管理更是几乎涉及到每一个社会个体。

然而在普通人的日常生活中，我们尚没有能管理信誉信息的主流社交产品，连人们线下的信誉交流方式也依然是原始的偶然性的交流。人们经常因为得不到及时有效的信誉信息参考，而错过了机会或者遭受了损失。这也给了诈骗和不良商业活动等提供了持续猖獗的空间。

ANYI网络系统力图实现信誉信息的网络交互和管理：

· 让信誉信息也能在社交网络中存在和分享。

· 让人们的日常言行和社交网络系统中的信誉关联起来。

信誉信息的可参考能让社交网络中的人们更自律，能使人们通过参考信誉信息更好地鉴别良莠。相信信誉信息的交互能净化/边缘化互联网上的虚假消息，也能放大信誉的影响力从而促进现实社会的良性发展。

3.1.5 权限管理

人们在当今时代愈加广泛的社交关系和海量信息面前，有效地管理社交关系和资源已经越来越有必要。可以说能有效管理和利用社交资源的人，才能游刃有余地应对日新月异的现代社会生活。

ANYI结点通过管理ID实现自由灵活的权限管理,来满足各种权限控制需求。

1）预先设置权限，应用程序根据权限处理信息。适用于社交关系。

· 可以对结点上的关系分组。

· 可以对结点上的信息分组。

· 可以对任意信息（或信息分组）作访问权限设置。

2) 临时授权。适用于政府、银行等非好友关系场合下的个人信息表单提交。

3.2 以个人为中心的新应用场景

3.2.1 一键式信息提交

通过纸质或电子表单提交个人信息是常见的交互场景，这个环节必要而又繁琐低效，也很容易成为机场等繁忙场所的瓶颈环节，如果忙中出错更是令人沮丧。

ANYI网络系统可以改变这个低效、易出错的落后方式：

· 机构方面像准备申请表单一样准备好面向ANYI结点的请求码，请求码内包含了具体请求内容和关联信息。

· 用户用结点软件读取请求码，软件自动提取结点内的信息并生成确认内容。

· 用户确认要提交的内容后通过结点软件即时授权，机构方即时得到用户信息，然后由机构方面处理后续业务。

优点：

（1）高效（快速、准确）：把人们从繁琐易错的交互方式和相应的等待中解放出来。

（2）个人结点上的交互记录，使得个人开始能够掌握自己的信息交互历史。

（3）机构方面也相应地节约了成本。

规范化：用户有权了解机构收集信息的理由；针对当前超越服务范围地获取用户信息的不良企业行为，可以由权威机构从法律层面规范。

3.2.2 减少敏感信息的使用场景 & 去实体会员卡片

每一个人拥有了结点的同时就拥有了至少一个能唯一标识自己的ID，在日常生活中需要与机构建立联系时，结点向机构提供ID作为会员标识；验证会员信息时，结点再次提供ID，机构方验证ID即可。不必再使用姓名、地址、电话、邮件等敏感信息作为联系关键字。减少了个人敏感信息泄露的渠道。相应的，联系对象的机构方面也可以减轻保护收集到的敏感信息的负担。

使用结点ID，不再需要机构向个人发放证明会员等关系的实体卡片。

既免除了个人的卡片管理的繁琐，也节约了机构方面卡片发行相关的成本。

当在联系关键字用途之外需要个人敏感信息时，使用3.2.1的方式提交。

3.2.3 以个人为中心的基本信息利用

日常生活中人们的基本信息经常会发生变化。目前我们的信息分散于各种社会机构，当基本信息变化时，我们需要花费相当的时间精力成本去同步变化的信息。或者因为放弃/忘记与部分机构间的信息同步，从而影响我们继使用相应的服务，关联机构也会产生无效数据导致的损耗。

ANYI网络系统基于个人的信息结点，以机构不再存储管理用户信息、必要时实时向个人结点请求信息的方案来解决这个课题：

· 建立联系时，机构向用户请求指定项目信息的使用许可（不必即时收集信息）。

· 用户信息变化时，及时更新结点信息。

· 机构在必要时通过ANYI网络系统取得用户的有效信息。

（个人结点作为数据源头，成为参考基准）

优点：

（1）用户只需要更新作为参考基准的个人结点，不再需要分散对应关联对象。

（2）用户开始能以个人为中心管理与外部的关系。当不再需要某些商业服务时，只需要关闭相应的许可，对应的商家就不能再获取到相关信息。

（3） 机构可以减少用户信息的持有期间或者避免持有用户信息，降低风险。

（4） 机构可以避免无效信息带来的损耗。

3.2.4 合理化信息资产运用

我们已经习惯了越来越多的没有物理实体存在的信息服务：在线音乐、电子书、在线教育、保险等等。这些服务可以视为我们的资产的一部分。然而即使在合理的情况下，我们仍普遍难以像处理实体资产一样处理信息资产，如转让所有权。

ANYI网络系统通过结点ID声明信息资产的所有权，通过所有人ID的变更能实现信息资产的转让。

我们以Kindle电子书服务为例说明：

亚马逊在向购买者A交付产品时，用A的公钥声明电子书属于A，并且用A的公钥加密电子书。这样只有A能用私钥解密电子书。

当A要将电子书转让给B时，由A向亚马逊申请将电子主人变更为B，亚马逊方面验证A的所有权后，将B声明为些电子书的主人并且重新用B的公钥加密电子书。

这样，电子书开始对新所有人有效的同时，关闭了电子书的旧主人的使用可能，完成了电子资产的转移。

类似的，实体物理资产也可以在ANYI模式下实现信息化管理，因为没有易拷贝的特性，物理资产的转让信息声明更简单。甚至实体物品的使用手册、质量保证书等也可以在ANYI网络系统中以电子信息的形态存在，用户不必再为保存管理各种产品的相关资料烦恼。

3.3 个体信息管理的未来

除了上述案例，当前的信息世界还有个人“碎片化”的课题：

· 在电子商务领域，大小商家各自为营，人们难以以个人角度跨商家系统地管理自己的交易信息。

· 医疗方面，医疗机构掌握着个人的病历信息，个人难以跨医疗机构管理和使用自己的病历信息。

· 社交软件方面，同类但不同商业团体的社交平台的存在，以及个体的使用偏好，使社交信息的流通受限于软件平台，个体用户只能进行无奈地取舍。

ANYI网络系统的个人结点模式使个人角度优先的管理成为可能：在与机构交互时在个人结点上记录下必要的信息，从而使我们可以跨越机构地管理交易信息和点数状况；可以全面系统地了解和使用自己的健康信息；可以不受限于第三方平台自然地管理社交关系。

在信息世界里拥有与机构对等的存在，使人们能轻松地实现自我管理。以此为基础，相信我们可以在更多领域里进行更多的合理化变革。

4.中心化

4.1 去商业中心化

个人用户不能自由地在不同社交软件之间迁移数据；不能将已经购买的信息资源（如音乐、电子书籍）自由转让；用户面临着信息被滥用、泄露的风险；商业公司合法的决策变更影响到普通用户（如雅虎中国邮箱服务终止，FB规则被恶用导致的大量用户信息被获取）… 种种不利于用户的限制和风险，是商业中心化模式的必然产物。

这些是利益优先的商业模式发展至今的现状，没有跨机构范围的全面变革，现状不可能改变，甚至不能阻止其恶化。

欧盟出台的GDPR（一般数据保护条例）针对上述课从法律层面定义了对企业的约束，但是GDPR只是通过事后惩罚来制约企业，没有有效的损害挽回措施。

ANYI网络系统使个人数据独立于企业的方案弱化个人对商业机构的依赖，降低商业公司变化对普通用户的影响程度。

脱离商业中心化，个人信息资产的产权关系也变得明朗简单。

4.2 行政中心化

如3.2.1提及的，对于商业机构向用户索取的信息的合理性，我们需要相应的法规保护；信息资产在必要的情形下作为继承、代理、冻结、强制限制等处理的对象时，我们需要合法的执行机构；密钥丢失或被盗时，我们需要有可依靠的机构能够帮助“找回”对自己结点的控制权；ANYI网络系统同样也需要实名认证机制，以满足相应的社会生活场景。

综上，我们需要合法的、对全民负责的信息规则立法者和执法者来保护和管理信息资产的世界。除了政府，没有更值得依赖的组织来担负这个职责。

5.结语

由于硬件和技术的发展限制，软件应用的中心化模式在到目前为止的很长期间内是最佳方案：商业公司提供信息存储、计算、安全等方面的服务；用户低门槛地利用互联网服务。

但也因此形成了当今互联网的用户信息碎片化地围绕着商业机构主体、商业机构“霸权”式地定制规则已是常态的现状，产生了前文所提及的种种课题，也限制了人们日常生活的进一步改善和发展。

当前我们具备了去商业中心化的条件：

· 智能手机等移动设备的普及使人们有了自主存储、计算、管理和网络交互的能力。

· P2P网络技术使得网络上的个体直接交流成为可能。

· 非对称加密技术从理论和实际应用上证明了信息存储和传输的安全性。

ANYI网络系统希望以一个明确信息所有、以人为主体的网络为基础，和大家一起建立起合理的规则体系，共同营造美好未来。

2018年11月6日