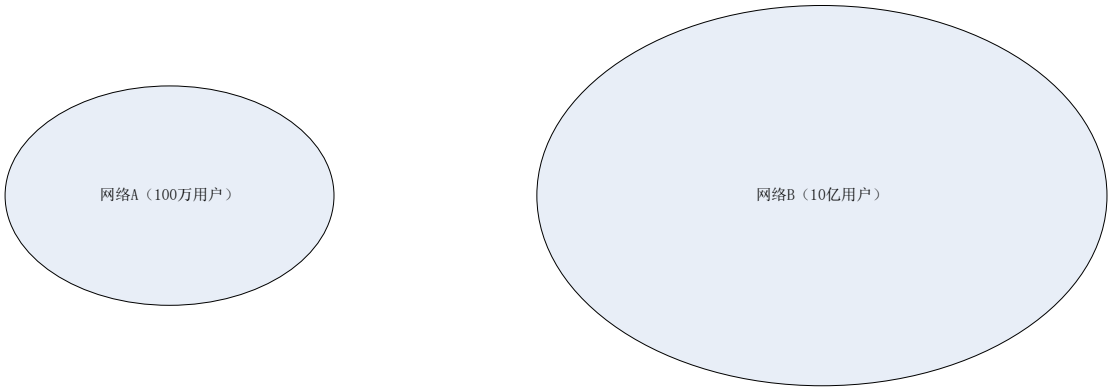
开放式社交公共网络白皮书

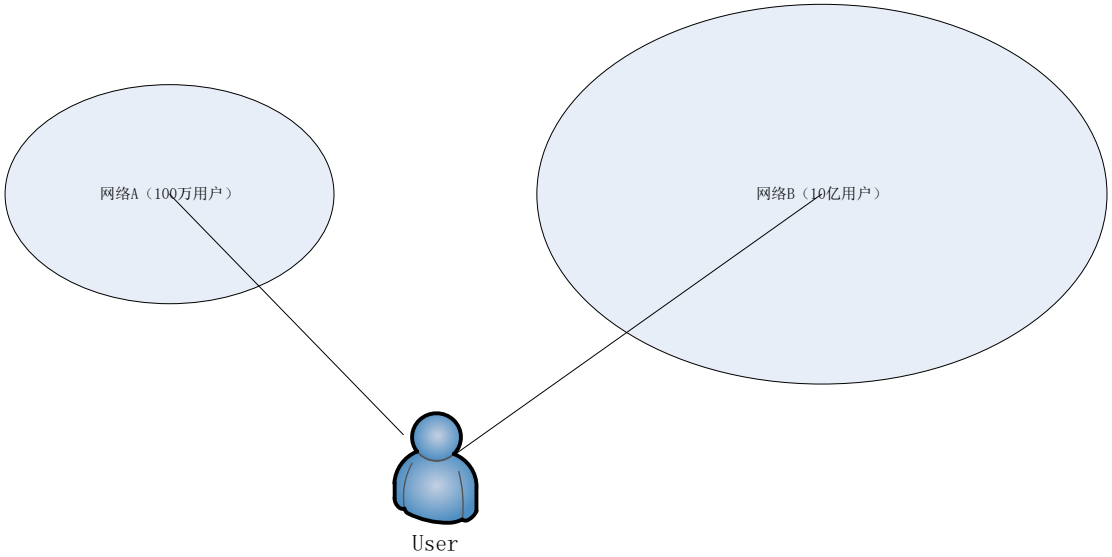
深圳市加农炮网络技术有限公司编写

前言

我们看到了一批又一批的勇士冲进社交领域，然后败北。分析其败北原因，用户不使用你们产品的原因是因为**社交关系网不在你的 APP 上**，即使你的产品做得再好，也很难让用户留下来。关系网存在大鱼吃小鱼的问题，大的关系网会把小的关系网吞并掉。

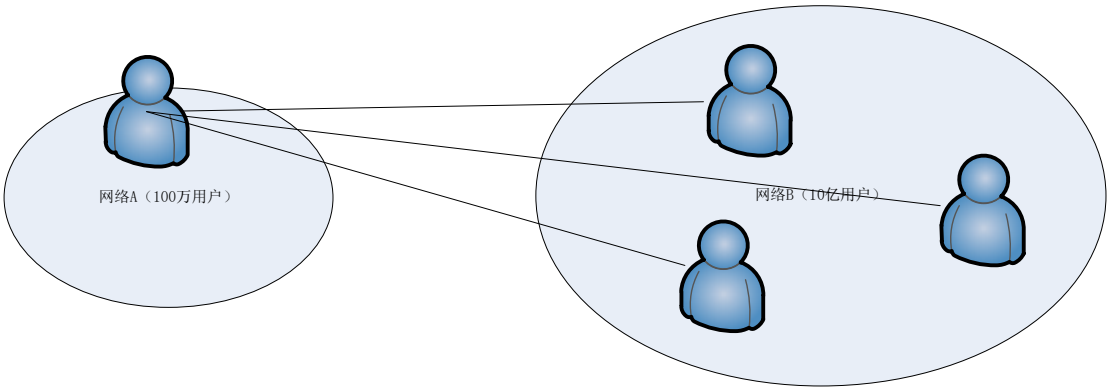


假设目前有两个社交网络，一个网络有 10 亿用户，一个网络有 100 万用户。

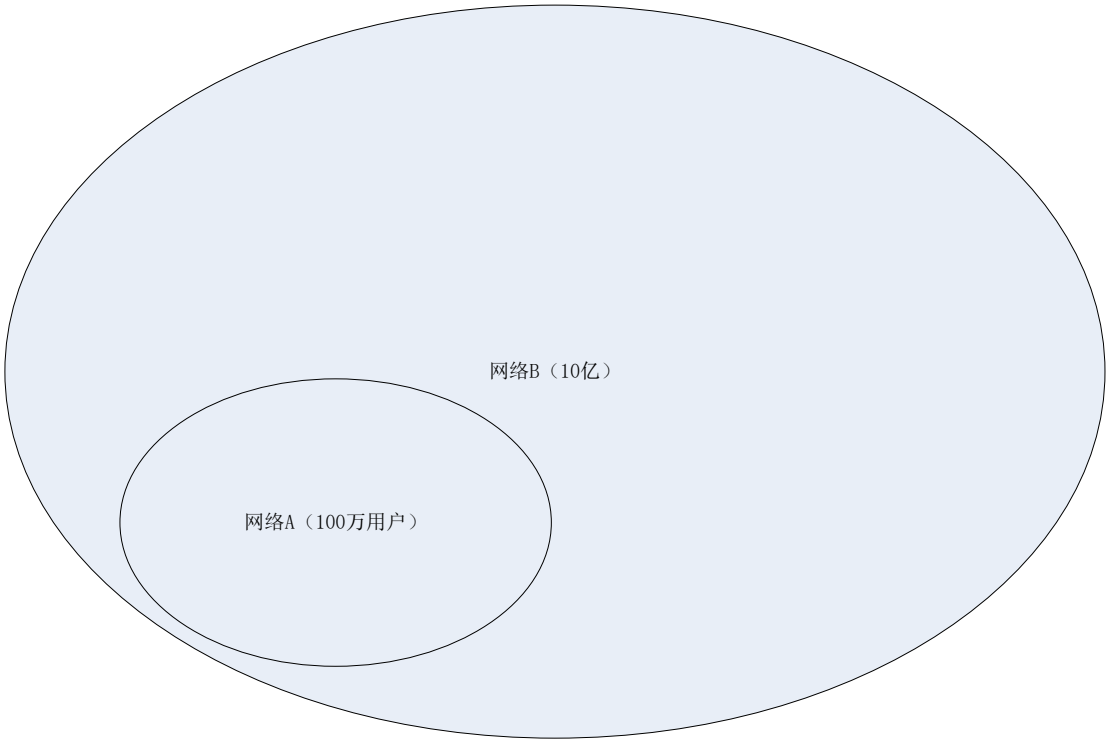


现在有一个用户，他在网络 B 中有 1000 个朋友，在网络 A 中有 10 个朋友。由于社交软件之间存在壁垒，使用两个社交软件进行切换很麻烦。因此这个用户就会推荐网络 A 中的 10 个朋友，使用网络 B 中的软件。

在网络 A 的其中一个朋友，如果是因为该用户推荐他使用网络 B，可能他使用网络 B 的概率不大。但是真实的情况是，这个朋友会有很多的朋友，都推荐他使用网络 B。如下图所示。



这个人就有很大的概率投入网络 B 的怀抱，而他发现使用 2 款社交会很麻烦，就会推荐网络 A 中的其他朋友使用网络 B。



很快，网络 A 就会被网络 B 吞噬。

跨界社交的理念

如果你的 APP 可以和网络 B 的 APP 相互聊天，那么你的 APP 就有机会让用户留存。基于这种假设，我们提出了**“跨界社交”、“跨界通信”**的理念，**让所有的社交 APP 都可以相互的聊天**。比如，微信可以和陌陌聊天，陌陌可以和钉钉聊天等等。有了跨界社交，你的 APP 的生存概率才会增大。（**想想三大运营商移动、电信、联通如果不能相互打电话相互发短信会有怎样的结果？**三家存一家可能是最后的结果）

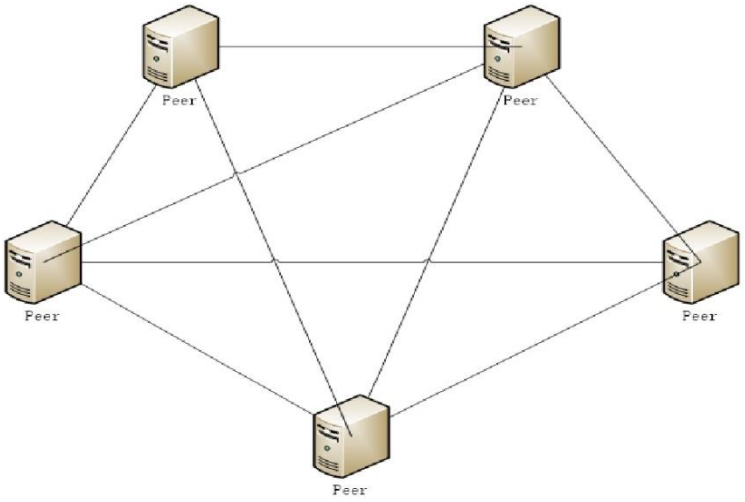
开放式社交公共网络介绍

开放式社交公共网络（Open social public network，简称 OSPN）是一个可以帮助企业的社交 APP 与其他社交 APP 建立“跨界社交”联系的项目。OSPN

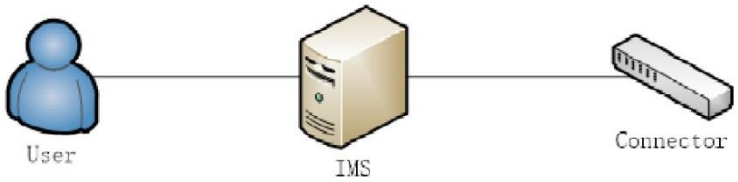
是一个**开源免费**的项目，它是**一种理念**，是**一套解决方案**，是**一套源代码**，需要企业将这套源代码植入到自己的服务器中去。

1、 整体架构

开放式社交公共网络的底层通讯采用了基于 DHT 结构的 P2P 技术。每一家接入的企业都将以一个节点的形式接入到 OSPN 中。其结构图如下图所示



企业作为节点接入需要三个部分，connector，IM 服务（IMS），客户端（APP、小程序、或者 web 等等）。三者之间的关系如下图所示



connector 的作用是与其他企业的 connector 进行数据交换。

2、 账户系统

OSPN 的账户不再是由服务器生成，而是采用椭圆加密算法，由客户端随机生成。账户生成的具体方案请参见《开放式社交网络通信协议》。

3、 添加好友

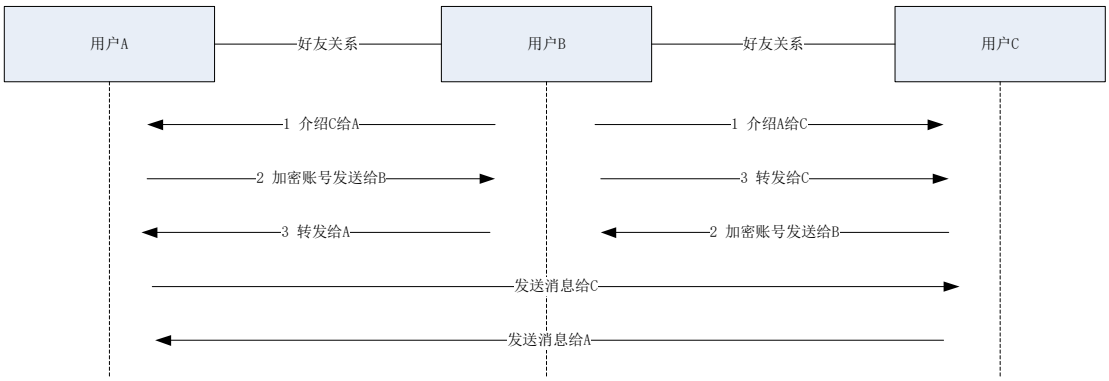
添加好友有几种方式：

3.1 双方互相交换账号

该方式就像是双方交换电话号码。

3.2 由好友推荐

用户 B 介绍用户 A 和用户 C 成为好友。

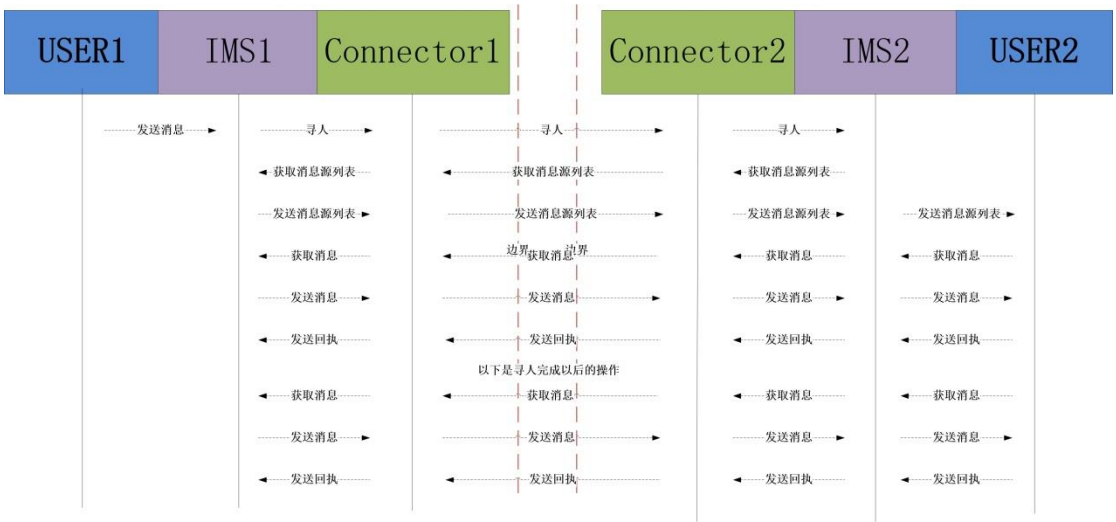


第一步，用户 B 将介绍信发送给双方
第二步，用户 A 和 C 同意，就会将自己的账号加密以后发送给 B
第三步，B 收到 A 和 C 发来的加密账号以后，转发给双方。
注：B 收到的信息是密文，并不知道里面具体的账号是什么。
双方将对方的加密账号在终端添加成好友以后，就可以相互发送消息了。

3.3 通过发送添加好友请求命令

该方式需要你使用的 APP 所在企业是否支持跨界添加好友请求，如果该企业不支持跨界添加好友，则无法使用。

4、 发送消息



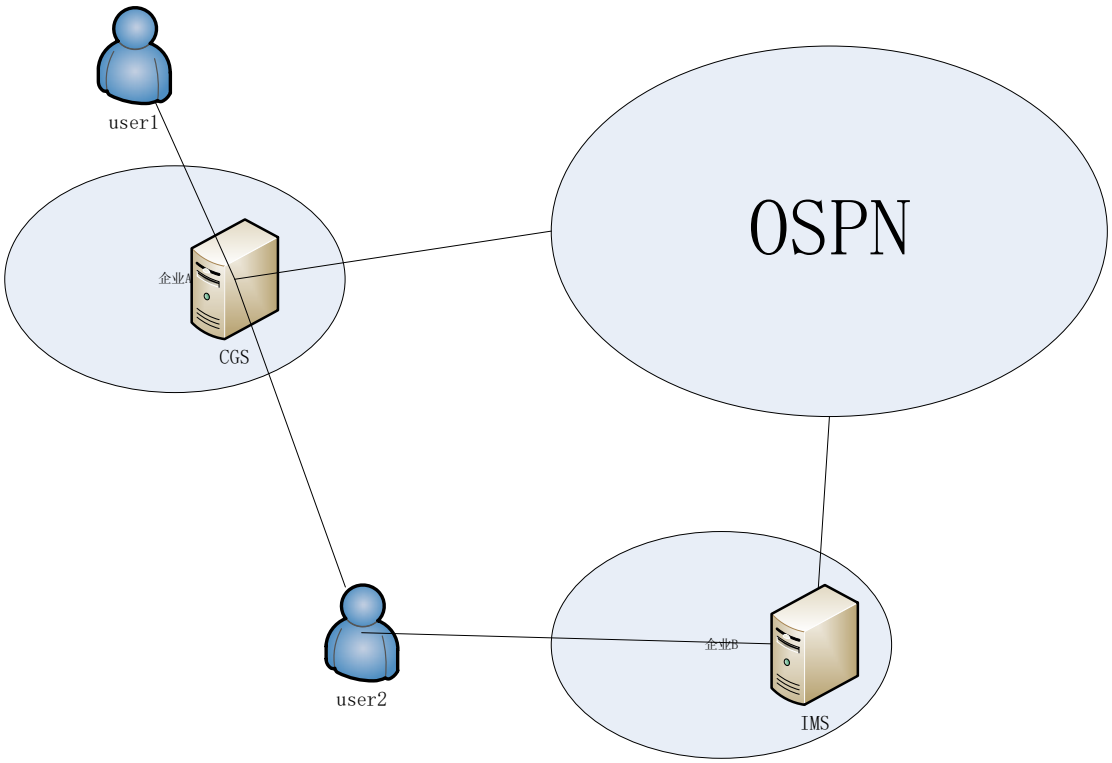
用户 1 给用户 2 发送消息的流程如图所示。
IMS1 代表 USER1 使用的 IM 服务。
connector1 代表与 IMS1 配套的服务。
IMS2 代表 USER2 使用的 IM 服务。
connector2 代表与 IMS2 配套的服务。

1. USER1 首次给 USER2 发送消息时会将消息发送给 IMS1，IMS1 发送寻人命令给 connector1，connector1 到 OSPN 网络里广播寻人。（发送的消息会使用 USER2 的公钥进行加密。）

2. connector2 收到广播找人消息以后会将命令发送给 IMS2,IMS2 判断 USER2 是否在自己的服务上。如果 user2 在线，IMS2 才会去获取用户源列表。
3. IMS1 接收到获取用户列表命令以后发送关于某一用户的列表。
4. USER2 收到列表以后根据自己的需求，筛选所需消息，发送获取消息命令。
5. IMS1 接收到获取消息命令以后发送消息。
6. USER2 接收到消息以后验证签名，并发送回执。
7. IMS1 接收到回执，删除滞留的消息。
8. 建立了首次通信以后，双方只需要发送获取消息的命令即可完成消息发送与接收。

5、 跨界群

跨界群，顾名思义，是要让不同应用（APP、小程序等）上的用户能够在同一个群里聊天。



跨界群示意图，CGS 代表跨界群服务，user1 是企业 A 的用户，user2 是企业 B 的用户。他们可以同时使用企业 A 提供的跨界群服务。

群的所有权

由于群是由群主创建，因此我们主张群的所有权归属于群主所有，同时群主具有选择服务商的权利。

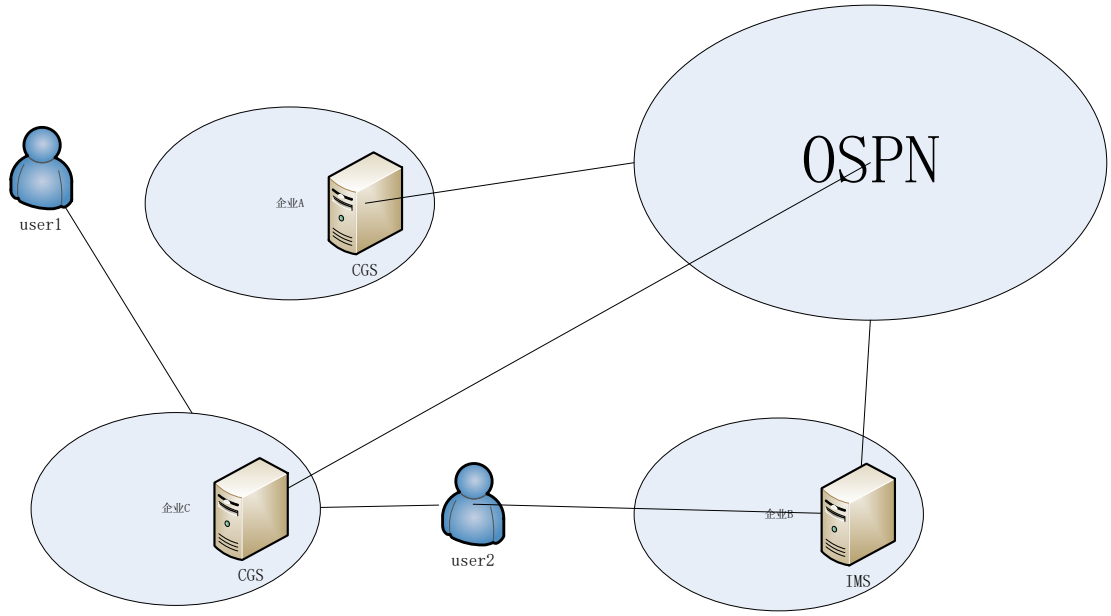
群的监控权

由于群属于是公共场合，因此企业作为群的服务提供商，群的监控权应该归属于企业所有。企业应具备对群言论的监控权，以及是否对群提供服务的权利。企业可以要求群主进行实名认证，我们主张群实行群主负责制，言论的管控由群

主负责，如果发生不当言论，应当直接找群主处理，群主可以对群成员进行禁言或者 T 出群。如果群主不作为，企业可代行处理。

群服务商的更换权

群主应具备对服务商的更换权。为了防止群服务提供商滥用手上的职权，为了坚持群的所有权归属群主所有。



群主更换跨界群运营商的示意图。User1 为群主，可以将跨界群的服务迁移到企业 C 上，从而保护住自己的群不丢失。

如何实现群的所有权归属群主，而监控权归属服务商？

OSPN 网络使用的账号包含了双密钥对，其中的暗密钥对掌控着对群的所有权，明密钥对则可以拥有监控权。群主在创建跨界群时，群账号由群主生成。选定服务提供商以后，群主需要将群账号和明密钥对交给服务商。这样归属权和监控权就分离开了，服务商具备了仅具备了群的运营权和监控权，不具备归属权。

群主如何对服务商进行更换？服务商拥有明密钥对，如果服务商不配合应该如何处理？

群主更换服务提供商，首先需要找到另外一家愿意提供服务的服务提供商。群主向新的服务提供商提供群账号和明私钥。此时旧服务商和新服务商都拥有运营群的权利。

群主向新服务商提供群成员名单。

群主向新服务商提出更换群账号的指令。新服务商通过 OSPN 网络广播告知所有群成员账户更换，旧服务商无法更换群账户。

群成员收到更换通知以后连接到新的群地址即可完成群的更换。

6、 治理方式

OSPN 网络采用了“完全去中心化”的设计。设计由深圳市加农炮网络技术有限公司（简称加农炮）完成，但是运营权不归属加农炮所有。现在我们假设加农炮要修改当前的规则，推或者要推出一些新的协议，如果目前网络中的大部分

企业表示不不支持，他们继续维护着原来的规则，那么这些新的改动是无法完成的。只有当有企业支持了这种新的规则，并且大部分的企业达成了共识支持这种规则，新规则才会被采纳。

如果一部分企业采纳了这种规则，另一部分企业不采纳，可能会发生“分网”的情况。发生了此种事件以后，由市场决定其走向，假设现在形成了“分网”，那么未来由用户来决定未来走向。如果新规不能得到市场的认同和共识，那么新规将被市场淘汰掉。

7、 隐私保护

我们提倡的碎片化隐私保护。现在我们全部使用微信，以朋友关系网为例，我现在与 1000 个朋友的关系网全部在微信，一旦隐私泄露，就会把我的关系网，以及我的朋友全部暴露出来。

但是碎片化的隐私保护，提倡你与 1000 个朋友的关系网分散到多家企业，这样一家企业得到你的关系网将会是一个不全面的关系网，即使暴露了也仅仅是暴露了你自己的资料，而你朋友们的隐私得以保护，因为他们的隐私在另外一家企业。

而对于企业所保存的个人隐私资料，企业也不会共享给其他企业。用户使用谁的 APP，就会是谁的用户。

8、 最合理的通胀模型

开放式社交公共网络具备区块链的“去中心化”特征，但是没有区块，也没有链。同时也没有 token，却自带了隐藏 token 属性。全球 70 亿人是 OSPN 的总 token，企业运营自己的 IM 软件，等同于挖矿。获得了多少用户，等同于挖到了多少矿。

原来一个社交企业，如果只有 5 万的用户，达不到质变的效果是没有价值的。但是有了 OSPN 以后，拥有了 5 万的用户，就变得有价值了，因为如果持续购买 100 个有 5 万用户的 APP，就可以形成 5 百万的用户级数。因此小中企业会变得更有价值，也更容易活下来。

如果一家本就带有了一定的用户（20 万），这个时候加入到 OSPN 网络中，就等于挖到了 20 万的 token。

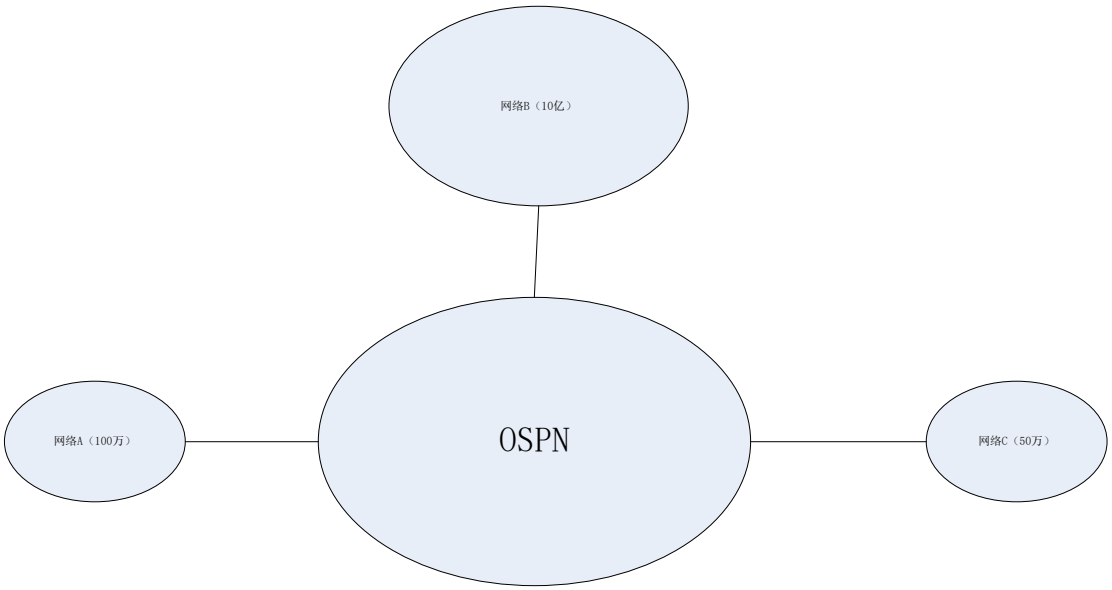
相对于其他的 token，OSPN 自带的隐藏 token 具备更多其他 token 不具备的优势。它的通胀模型非常合理，与比特币相比，由于比特币的上限总量恒定，且后期产量减半，会导致后来者不愿意入局。因为后入局者容易变成韭菜。而每年固定百分比增发和每年固定数量增发的模型也会导致在未来形成通胀。

历年新生儿统计示意图

而 OSPN 自带的隐藏 token 的的通胀模型与人口挂钩具有去陈出新的特性，这是其他区块链所不具备的。假设目前一家企业处理垄断地位，但是每年都会有一部分 token 消失（人口减少），而每年的新增 token 则是众人去竞争，所以 OSPN 的隐藏 token 被集中的概率会更低，这是一种非常分散化的 token 模型。而对于入局者，任何时候入局都不会晚，即使是后来入局者，仍然会有优势。

未来社交网络

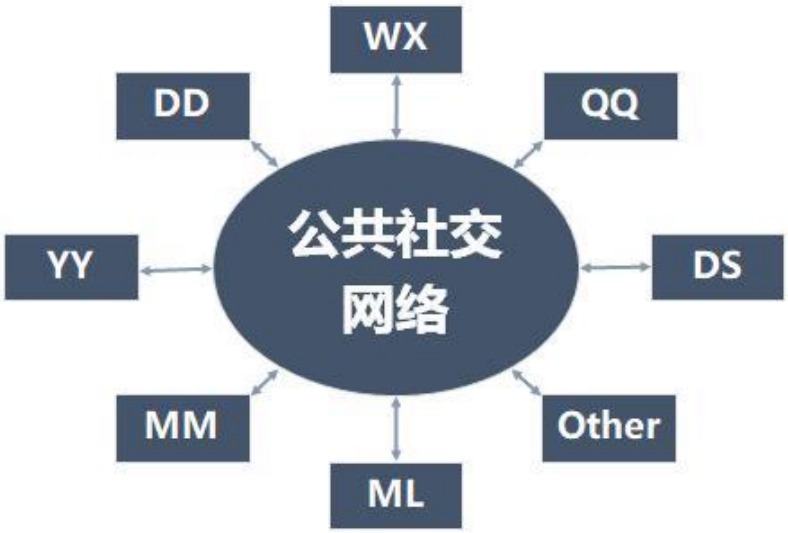
当有了 OSPN 网络以后，我们再来分析还会不会存在大鱼吃小鱼的情况。同样是两个网络，一个拥有 10 亿用户，一个拥有 100 万用户。



还是同样的情况，有一个用户，他在网络 B 中有 1000 个朋友，在网络 A 中有 10 个朋友。这个用户选择哪一个网络，都可以和所有的朋友交流，因此不再存在有人建议他使用哪个软件的情况，用户可以根据自己的喜好任意选择自己喜欢的 APP。没有了朋友的推荐，对于小型的网络来说，就保留住了自己的用户，而网络 B 由于前期是因为朋友关系被捆绑到网络 B 中的用户，则可以逃离出来，分散到其他的网络中。

既然用户可能逃离网络 B，网络 B 为什么又要加入 OSPN 呢？首先一个人的手机上不可能只装一款 APP，一般会装 12 款 APP。我们假设用户除了装网络 B 的软件，另外 11 款 APP 有 3 款是具备跨界社交功能的，只是目前这个用户没有使用这个功能而已。这时，这个用户遇到一个朋友，他不使用网络 B 的 app，而是 OSPN 上的某一款 APP。那么这个用户就会使用那 3 款软件中的其中一款 APP 与这个朋友添加好友。因为不用下载新的 APP，用已有 APP 就可以完成，对用户的接受程度会很高。久之，这个用户就会逃离网络 B，这种情况即使是网络 B 不加入 OSPN，也会发生用户逃离的情况，综合考虑，网络 B 为了保护自己的用户不流失，会加入 OSPN 网络。

其他 3 款 APP 又为什么会加入 OSPN 网络？目前除了头部的几家企业，其他 APP 大部分都没有足够的用户，而所有的 APP 都可以改造，内置跨界聊天。他们加入 OSPN 的成本很低，同时也可能帮助他们开拓出的新的业务和新的用户，因此他们会选择加入 OSPN 网络。



未来社交网络示意图

综上所述未来的社交网络是百家争鸣的盛世，所有的社交 APP 都可以相互通信相互聊天，甚至每一个 APP 都可能有这么一个跨界聊天的模块。当今这种大鱼吃小鱼的情况会得到改善。