PDU：基于点对点的社交网络系统

A peer-to-peer social networking service

- iOS App: https://apps.apple.com/us/app/p-d-u/id6443928730
- github: github.com/pdupub
- email: pdupub@gmail.com
- wechat: pengpengt00
- telegram: @PDUPUB
- telegram group: @PDUGroup
- twitter: @PDUPUB

摘要： 本文提出了一种在点对点的网络环境中可实现的社交网络系统，它使得任何使用者都可以自由发布信息，同时在不需要第三方认证的情况下实现信息发布者数量的有限可控。数字签名可以保证信息的真实、完整及不可否认，但由于密钥本身无创建成本，当没有第三方机构来验证及关联数字签名和其背后的用户身份时，系统中便会充斥大量机器人账户，使以账户为对象的惩罚机制失去作用。我们提出一种新的解决方案，基于点对点的方式构建社交网络服务，并帮助使用者能够在不依赖第三方认证的情况下，实现对信息发布者的有效筛选。系统中所有消息通过相互的引用确定有序关系，再由签名确定其来源。同源的全序消息序列被视为一个信息发布者身份，而所有的消息在系统中可构成一个或者多个有偏序关系的消息集合。任何信息发布者都可以自由的创建新族群或对其他身份做出属于某族群的认定。使用者根据已获取的族群认定消息来构建族群范围，并依据认定关系进一步过滤可疑的信息发布者。此过程将中心化服务中统一验证和一致的用户范围，变为基于可扩展的族群，由使用者自行决定的身份范围。

简介

信息传播系统应当让使用者能够自由地发布、传播信息，同时也能够有效的获取信息。由于信息通常根据其来源进行组织，所以对信息的有效获取必然基于两个条件，即来源的可确定与来源的有限性。

在信息的口耳相传过程中，面对面交谈时便可知信息来自何人，而生活中实际接触的范围便限制了信息源的数量。文字的发明在时间和空间两个维度上拓展了信息传播的边界，但并未打破上述两个条件的限制。

时至今日，众多社交服务平台为信息传播的效率与使用的便捷性提供了前所未有的帮助。通过手机号、邮箱等身份认证方式，平台可以有效的限制虚拟身份的创建，以维护信息源的有限性。但在提供服务的同时，平台本身对于信息传播的影响也越发严重。如限制用户权限、屏蔽言论或利用推荐机制扩大特定话题的传播范围。我们并不否定舆论的引导在某些特定事件上存在的积极意义，但更希望相信信息传播过程中的每一位参与者，将是非对错的判断交给所有人，而非单一的中心。

在本文中，我们提出一种点对点的社交网络系统，它基于特定的信息组织形式，使得系统使用者能够自由的发布、传播信息，也能够在不需要第三方认证的介入下实现信息来源的有限，从而保证使用者能够通过对信息来源的过滤而达到有效获取信息的目的。方案并不对系统中的身份创建过程附加统一成本或限制系统中的身份总量，而是将身份的组织方式交由系统中的所有使用者。使用者依据自我身份认同来扩展自身所属的族群，并按照意愿挑选系统中的一个或多个族群来作为自己可见的信息源范围。

消息

在本文所述的系统中，消息是点对点之间信息传递内容的最小单位，也是唯一的形式。我们定义每条信息均必须包含三个部分，引用列表、内容及签名。

引用列表

引用列表中包含其他消息的签名，用来建立消息之间的关系。因为签名出现碰撞的可能性很低，所以我们可以认为，引用列表中签名对应的消息创建于当前消息之前。

如果签名的私钥此前已经对其他消息进行过签名，系统要求当前消息引用列表的第一位必须是此前由同一私钥签名的最后一条消息的签名，称为自引用。如果私钥没有在系统中使用过，则当前消息引用列表的第一位则为空值。如此，所有同源的所有消息之间都有明确可证的前后关系，可构成一个全序的队列。

引用列表中除自引用之外还可以包含其他的任何签名，在实际使用过程中，推荐在列表中至少包含一条比较新的消息签名，目的是给当前的消息在系统整体时序上一个相对精确的可验证范围。

信息获取者没义务获知系统中的所有消息，所以也不会因为引用列表中存在未知的签名而对消息发布者进行惩罚。但如果其获取到具有相同自引用的不同消息，则说明发布者已经破坏了自身消息的全序限制，此发布者便不再应被视为一个合法身份，会蔽其后续的所有消息。

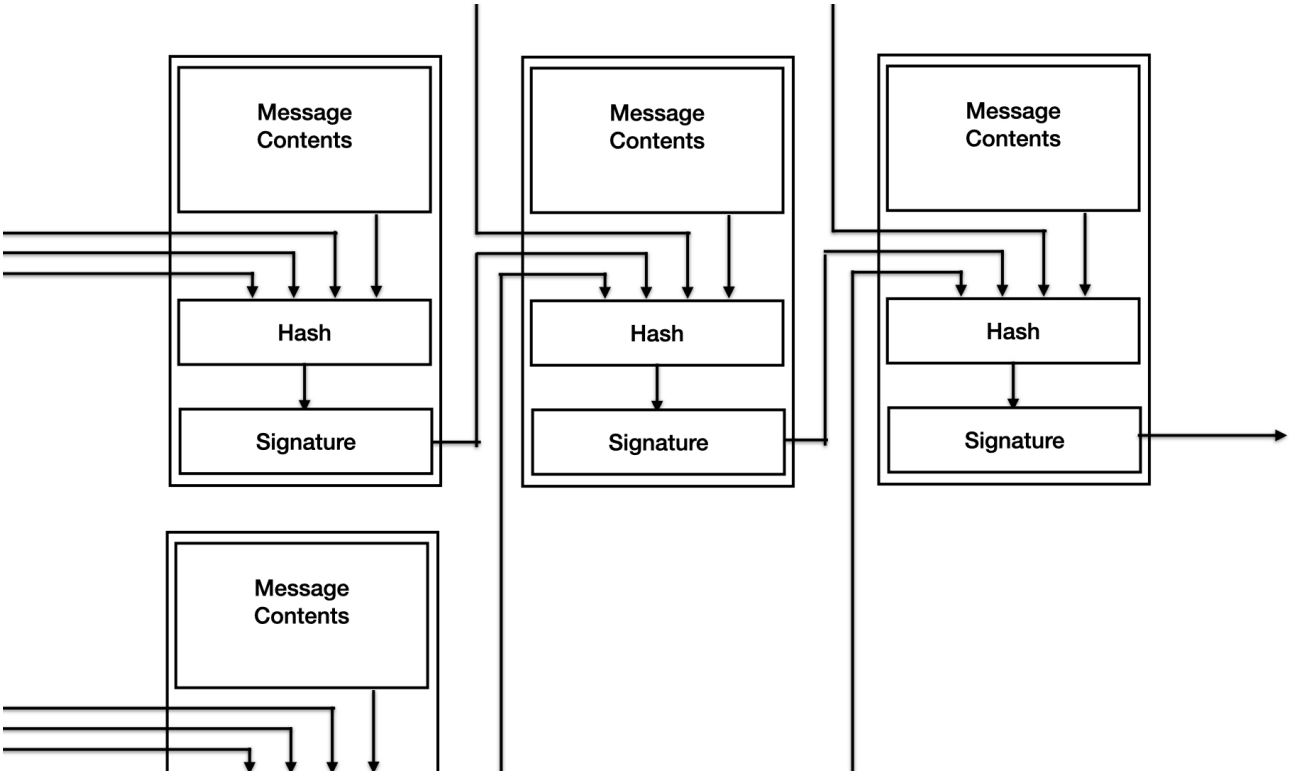
消息内容

消息内容是消息的主体部分，由消息类型和多个内容片段构成。目前系统中包含以下5种类型：

信息消息 「Information」: 最主要的消息类型，用于发布信息。内容可以包含文字、图片、音频及视频等不同格式的内容片段。 叠加消息 「Integration」： 此种消息主要用于新增或更改身份的属性或用户账本记录等需要简单呈现最终状态的场景。 族群定义 「Speciation」： 用于创建族群。 族群认定 「Identification」： 用对表达对其他发布者属于族群的认可。 终结身份 「Termination」： 用于因私钥泄露或其他原因主动希望被忽略后续消息的情况。

消息签名

系统中的所有消息必须包含签名以对其来源进行身份认定，确保消息内容的完整性。签名还将被放入后续的其他消息中，来表达消息之间的有序关系。



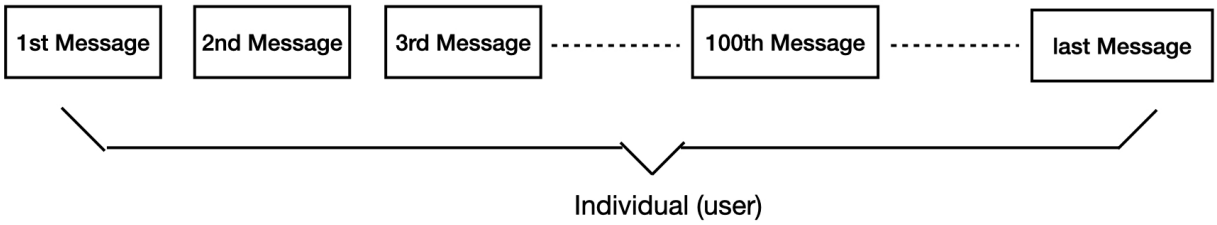
上图展示每个消息的构建及引用关系。

发布者身份

在常见的中心化社交网络服务中，用户身份通常即代表信息发布者身份，也代表了信息获取者的身份。依赖这一身份定义，使用者既可以屏蔽此用户发出的消息，也可以对其屏蔽自身消息，任何一条消息的传播方向都是由收发双方共同确定的。与此不同，在本文所述的点对点系统中，由于所有消息均为公开内容，所以传播的过程只由信息获取方决定。系统中的身份也被明确为一个对于他人完全可见的信息发布者身份，剥离了其中与信息获取相关的逻辑属性。

如前面提到的，在本系统中由同一私钥进行签名的全序消息队列被认为是一个信息发布身份。其与私钥是一一对应的关系，但二者并不等同。我们认为系统中的信息发布者身份代表一个独立的以信息传播最大化为唯一目的的主体，由一系列具有全序关系的消息所展现，能够感知外部奖惩影响而修正自身未来行为的最小单位。同一私钥使得这个身份可以被识别，而全序则使得其后续要的消息传播程度可以受之前消息的影响。

目前我们已经定义了系统中的消息这种点对点之间传输信息的基本单位及可以承担奖惩的发布者身份，但并没像中心化平台一样对身份进行统一验证。虽然系统中所有的消息根据签名均可确定其来源，但使用者依然会面对无限的发布者而无从筛选。



族群

我们已经定义了发布者身份，但在点对点的环境中，任何人都可以轻易创建任意数量的秘钥，并且按照前面所述的方式组织信息并添加签名。在没有三方认证的情况下，系统中依然会出现大量的机器人账户。我们无法在保证自由发布信息的同时阻止这种情况的发生。但需要明确的是，我们的目标并非保证系统整体的发布者有限，也无需让每位使用者具备同样的可见发布者范围，仅是提供给使用者一种方式使其所见的发布者数量有限。

为实现上述目标，我们提出了“族群”的概念。如同身份被作为消息的聚类方式，族群可被认为是身份的一种聚类方式。我们可将族群的归属简单理解成发布者是什么，而非发布者的爱好或者特征。比如我们既属于人类这个族群，也属于灵长类动物的族群，同时还属于地球生物这个族群。

族群的建立及扩展

每种群体的建立都是基于个体间的某种共性，而承认此共性的存在则源于个体的自我认同。加入群体的过程就是被群体接纳的过程，对于新进个体而言是一种被动的过。系统中每个发布者都可以通过族群定义消息来公开的成立族群，也可以通过族群认定消息来认定某个发布者属于特定的族群，以此来扩展族群的规模。

在点对点的系统中，我们希望使用者所接受处理的都是对自身有意义的信息，而非全量的信息。因而对于信息本身除了同源全序外，无其他任何的信息间逻辑判定的硬性要求，比如并不要求一个身份必须先属于某个族群才能对其他身份发出族群确认信息。我们将这种判定的自由留给系统使用者，使用者可依据可见信息自行决定判定规则。

族群内的筛选

如前所述，系统中的发布者身份已经剥离了信息获取的相关逻辑，但在系统的使用过程中，尤其是获取信息的过程中依然需要构建一个获取逻辑来保证信息源的有限。使用者可以通过已存在的关联关系，比如初始进入系统时所关联的几个发布者，找到他们所属的族群并任意的选取1个或者多个以此为当前可见范围。也可以通过族群内的发布者来探索更多的族群，并最终确定哪些族群来限制自身的可见范围。

在此族群内部使用者还可以根据用户间的认定关系来进行过滤。比如A被判定为可疑用户，并认为其目的就是向族群中引入更多的可疑用户，则可以设定其所有认定消息均对自身无效，从而过滤此族群中所有由A引入的后代。此过程并非直接过滤掉A认定的用户，因为A也可能认定被其他发布者同样认定的身份，所以仅需消除A在此族群扩展中的影响即可。在实际使用过程中，因为使用者本地信息量的限制，对于较大的族群而言，其范围也可以由使用者定义筛选规则，而让服务节点代为计算。

虽然族群的数量也是无限的，但随着系统的发展，少数族群由于良好的发展会产生聚集效应发展为较大的族群，此时使用者对于族群变动或增减的需求并不会太强烈，筛选的主要工作会变为对于族群内新进身份的过滤判定。

节点

节点是物理上的含义，通常对应某个设备或是网络服务，我们简单的将节点分为用户节点与服务节点。

用户节点

用户节点通常指使用者的手机，电脑等终端设备。使用者通常应在至少一个自有用户节点上保存完整的消息序列，以在有必要时提供给其他节点。而其他节点则没有义务完整的保存此类的信息。用户节点作为信息获取设备，通常也会保留自身设定的用户范围限定规则，比如选取的族群及族群内过滤规则，方便用户使用。此规则用户无义务提供给他人。

服务节点

服务节点通常类似于现在的第三方网络服务，区别在于其建立在公有的公开信息之上。可提供数据的存储，检索等基本服务。需要注意的是服务节点无义务，也并不可能包含系统的全量信息，其与用户节点无本质区别，也可根据自身定义的规则对用户可见范围进行筛选。区别仅在于其可见的族群范围可能更广，储存信息更加丰富和持久。

节点上存储的所有消息间可构成一个或多个有向无环图(DAG)。消息根据其互相之间的引用关系来确定图中的位置，多个DAG之间可能由于新的信息而产生合并，也可能由于某条信息被判定失效，而带来DAG的分割。

隐私

系统中所有的内容都是公开的。隐私的内容可利用发布者身份所对应的秘钥为基础进行，但隐私的内容可认为不属于本系统，这也不是系统尝试解决的问题。

任何传播过的消息都会以某种方式留下痕迹，可能被一些节点存储，或者被另一些消息所引用。而未留下丝毫痕迹的信息，因为其并未对系统产生任何影响也就等同于不存在。信息的传播速度和广度取决于信息本身，所谓隐私只是公开程度限于某个暂时的，且无法保证的臆想。其后果往往不是信息的保密，而是扭曲后的继续扩散。

保护隐私的偏好来源于思维惯性，但我们认为不公来源于并非所有的信息都被同等程度的完全公开，现实中只有部分的个体的信息能够被另一部分个体所知，反之则不然。然而真正的隐私只有个体心中从未表达过的信息，其不需要任何系统以任何形式进行保护。而公开的，有过传播的信息，都应该被准确的记录、公开。

组织，管理，货币

组织

系统中的组织是指建立在发布者为基础之上的更高形式的个体，通常按照一定规则对外呈现成全序的序列。这种全序可以根据使用的需求进行自定义。

比如几个发布者共同组成一个新闻组，他们可以利用其引用列表的第二位作为新闻组的有序关联位，他们之中的每个发布者依然可以自由的在系统中按照原先的规则发布其他内容，只是在发布新闻组相关内容时，可以在引用列表的第二位引用此新闻组的上一条新闻的签名。

与族群的概念不同，组织并非系统中必须的基础结构。组织像是现实中的家庭或公司，是一种社会组织结构，能够将个人以不同程度组织起来，并对外表现为一个整体。而族群是一种个体的集合。

在此完全去中心化的系统中，我们已经可复制真实社会中的绝大部分社会组织形态。

管理

系统实现了族群内发布者的有限性，因而族群可以用投票等常见方式进行管理。但需要注意，投票需要一个组织或身份来辅助进行，以确认可见的发布者范围。此过程类似于在选举之前要进行选民登记，以划定范围。

真实社会中的惩罚是由权力机关用物理隔离的方式减弱单一个体对大众的影响。在点对点的系统中没有中心化的权利机构，所以不存在强制力的惩罚，但服务节点可以由自身的规则来选择如何对某个发布者的信息进行处理，是否存储或中转。在开发特定的应用时，应用也可以根据自身平台、地区的法律法规来定义自身使用服务节点规则，从系统中选取适合的用户和他们的信息。

货币

我们可以在此去中心化的系统中实现中心化的货币，也可以基于已知的多种加密货币共识方式实现去中心化的货币。但在实际使用过程中，考虑到系统本身已经实现的族群内有限身份及工作效率，我们更倾向于利用投票相关机制而非纯粹的工作量证明方式来实现加密货币的共识，比如DPoS共识。

区块链可被视为一种系统内的组织，由多个身份共同组成，对外呈现为全序的消息队列，即更高层级的个体。各种共识规则决定了这个全序序列中后续消息的选择方式。

总结

我们提出不依赖中心化认证的身份构建方式。单纯的数字签名可以对身份进行标识，但却无法防止机器人账户创建对系统的影响。为解决这个问题，我们定义了消息的格式使消息间必然存在关联并以此将全序同源定义为身份。基于自我身份认同，每个发布者身份都可创建及扩展族群。以族群相关的消息为基础，使用者可以任意选择族群构成有限的发布者集合并根据发布者之间的认定关系进一步对可见的集合进行筛选。因为所有使用者都可以按照自身的意愿对消息进行传播，优质的内容会使得发布者身份得到更多的关注，从而利于其后续信息的更广泛传播，相反劣质的内容虽然依然可能会被大量创建，但因为其无法得到传播而失去了意义，也不会对系统使用者产生严重的影响。本文还明确了关于隐私的态度，其可以基于发布者身份而实现，但不能以之确定身份，也并不属于本系统。

附录

1. PDU之禅

- 事件通过有向关联确定偏序关系。
- 全序事件集合可被视为单一个体。
- 群体的构成源于个体的自我认知。

- 系统世界决定于个体的主观感知。

2. PDU的实现

- go-pdu
- iOS App beta

back