# PDU协议：去中心化社交网络服务


- email: liupeng@pdu.pub


**摘要：** 现有的社交网络服务，如Facebook、Twitter和微信，都是基于中心化的第三方平台。用户在享受便捷服务的同时，也受到了平台的限制。去中心化的数据分享方式，如Bittorrent和IPFS，虽然能够实现信息的自由传播，但其主要目的是存储和分享已知信息，缺乏筛选未知信息的能力。在去中心化的社交网络中，虽然数字签名可以证明信息的来源，但如果缺乏第三方验证提供的适当用户创建成本，就难以基于用户身份有效地筛选信息。

在本文中，我们介绍了PDU协议，这一想法源自人类社会结构。基于PDU协议，由相同私钥签名的消息形成一个全序列来定义用户身份。消息之间的引用关系建立了用户之间的联系。通过这些联系，用户可以扩展自己的可见用户群体，并以此为基础有效地筛选信息。

## 1 简介

### 1.1 现状

现今互联网上的信息传播和交互大多依赖于强大且可信的第三方中心化服务，如Facebook、Twitter、微信和微博等社交网络服务。这些平台的存在毋庸置疑地给用户带来了极大的便利，使得用户可以方便地发布信息，同时平台也会根据自身规则对信息进行过滤，防止垃圾信息泛滥。

然而，随着这些平台的发展，中心化社交服务的问题也逐渐显现。无论是有意还是无意，第三方服务都有可能滥用用户信息或导致数据泄露。出于商业考量，中心化的服务商可能会利用其强大的用户基础来打压竞争对手，如限制竞争产品信息在其平台上的传播，以维护其垄断地位。此外，中心化服务容易受到政府的监管和封锁，因为它们是可识别和可控的实体。

尽管存在这些问题，大多数用户仍然由于对第三方中心化服务的依赖，不得不继续使用这些存在问题的服务。对于大多数用户而言，更换平台可能不会导致数据丢失，但会失去在该平台上长期积累的用户关系，从而大大降低他们的影响力。由于这些关系是绑定在平台上的，用户实际上被平台锁定。

### 1.2 问题

为了防止用户被平台锁定，不但需要用户独立维护用户间的关系，还需要在去中心化的环境中完全实现平台提供的功能。在去中心化的网络中，无法进行类似中心化平台上用户注册时的验证过程，因此无法将用户身份与其真实身份关联，以增加用户创建成本。

现有的去中心化社交平台通常通过私钥签名确认用户身份。由于创建密钥对几乎不需要任何成本，可以无限制地创建。因此，在这种情况下，无法惩罚恶意行为，如发布垃圾信息。即使屏蔽了恶意用户，他们仍然可以创建任意多个新用户继续发布垃圾信息。因此，在去中心化的环境中，如何在无法进行任何现实关联验证的情况下有效过滤信息，成为系统面临的根本问题。

### 1.3 目标

本文提出了一种新的去中心化社交网络协议——PDU协议。该协议在没有第三方平台参与的情况下，通过用户之间交互固定格式的消息，实现信息的自由发布和传递，同时能够有效过滤信息。

首先，系统中的每条消息必须附加数字签名以确认信息来源。要求同一私钥签名的所有消息通过引用形成全序关系。我们将同源且具备全序关系的消息序列视为单一账户，其身份通过签名验证。同时，系统中的所有

消息根据其引用关系可以构建一个或多个偏序关系。根据这些关系，签名所代表的用户身份可以形成有向图。用户可以从任何已知的用户开始，根据这些关系按照指定层次遍历，以扩大其可见用户范围。在使用过程中，用户也可以从发生交互的用户开始扩展自身可见用户范围。在其可见的用户范围内，用户可以根据自身判断，对发布垃圾信息的用户进行屏蔽，从而实现信息的有效过滤。

### 1.4 前提

我们提出的PDU协议的基本前提是：系统的参与者都以信息传播的程度为唯一的利益衡量标准。用户希望发布的信息在更短的时间内能被更多的受众获取。这一前提的灵感来源于人类社会，在人类社会中，影响力是衡量利益或权利的最基本标准。在政治、经济和文化领域，一个人的影响力决定了其在社会中的地位和权利分配。信息传播的程度是社交系统中社会影响力的简化映射。

## 2 消息

在PDU协议中，消息是peer与peer之间唯一传递的形式。系统中的其他数据形式，如用户身份等，都是基于网络中的公开消息在节点中自行组合的。

消息是系统中最基础的数据结构，也是点对点之间唯一进行直接交互的数据类型。系统涉及的其他数据类型，如账户、社区等，均可在各个节点自行基于消息生成。消息包含三个组成部分：消息内容、引用列表及签名。

### 2.1 消息内容

消息内容是消息的主体，由消息类型和多个内容片段构成。

### 2.2 引用列表

引用列表中可包含多条消息的签名，用以确定消息之间的有序关系。

消息可以将任意已知的消息签名放入本消息的引用列表中，再计算hash后添加签名，用以证明本消息必然发生在被引用的消息之后。如果当前账户已经签发过消息，系统要求在引用列表中必须包含同一私钥签名的最后一条消息的签名。在使用过程中，推荐在引用列表中至少包含一条比较新的消息，以便给当前消息提供更精确的时序验证范围。

同一来源的所有消息可以通过引用的方式确保构成全序关系，即任意两条由同一账户签名的消息都有确定的先后顺序。不同来源的消息可以借助相互的引用，构成一个或多个偏序关系，可以用有向无环图（DAG）表示。

### 2.3 签名

签名的存在首先可以对消息来源进行身份认证，同时确保消息内容的完整性。消息签名还可以被放入后续消息的引用列表中，表示消息间的有序关系。

### 2.4 关于消息的说明

不存在单一的第三方来过滤消息。任何消息都可以发布到系统中。

系统中不存在类似于区块链的共识机制来保证每个节点都获取相同的消息。在PDU协议中，对于每个用户来说，其可见的用户范围可能不同。系统并不强调一致性或信息的完整性。PDU协议认为，通过用户对信息的传递，如转发和引用，即便仅有系统中少量用户可见，也可以满足用户对信息获取的需求。

此外，当同一个私钥签发的消息有多个后续消息时，系统会认为该私钥代表的发布者有故意作恶的嫌疑。其他用户可以根据自身意愿对其进行处理，可以屏蔽该私钥后续签发的消息，也可以在当前冲突的后续消息中随意选择一个。

需要强调的是，自我引用消息的全序关系，即同一私钥签名的相互引用，是PDU协议中构建发布者身份的基础，破坏这种关系会被认为是主观恶意行为。

另外，消息中通常不应包含加密内容，因为系统中的公开消息是定义用户身份的基础。正如前提中所述，每条消息的目的是最大化信息传播。而加密的信息对公众来说是无意义的，这会削弱信息传播效果，从而不利于身份的定义。

# 3 用户

在PDU协议中，传统中心化平台中的用户角色被分为信息发布者和信息获取者两个不同的身份。

需要注意，这并不是将一个用户分为两个身份，这两个身份之间也不具备一一对应的关系。并不是将传统平台的一个用户直接分割成两个部分。

对于信息发布者而言，其唯一目的就是最大化自身信息的传播。

由于所有信息都是公开的，信息获取者可见的信息仅限于他们基于自己定义的用户筛选方式所能看到的信息。

我们的设计方式使用户能够基于发布者身份及其关联关系进行信息过滤。信息获取者的身份只保留在本地，并不属于系统中的公开信息。

当信息发布者发布新消息，或进行转发、引用、点赞等行为时，这些行为都会以消息的形式在系统中公开。当然，信息发布者可以选择是否公开某些行为，如点赞或屏蔽用户。

信息获取者可以通过信息发布者之间的关联关系，扩展自己可见的用户范围。

当信息发布者与可见用户发生互动时，可以通过对方的关联用户进一步扩展网络。当然，信息获取者也可以主动从任何发布者的关联关系中进行扩展。

我们可以认为，即便同一用户控制的多个信息发布者在扩展可见用户范围时也与其他信息发布者没有区别，可以采用同样的规则进行。

所有用户之间的关联关系都可以用有向图表示，方便在维护时进行删除。

# 4 组织

多个发布者可以形成一个更高层级的组织，这需要构建一个更高层次的全序消息队列，以类似个体的形式对外展现。

通常的发布信息方式可以是：在引用列表中，第一个引用依然表示自引用，第二个引用表示特定的起始消息，第三个引用则构成组织的全序引用。

采用这种方式可以实现任何共识规则下的加密货币，但考虑到这些出块节点已经具有身份，所以更倾向于选择不需要强大算力支持的共识方式，如委托权益证明（DPoS）和权威证明（PoA）。

# 5 网络

整个网络可以由观察者节点构成，每个节点的数据都依赖于其可见用户范围。节点有自定义的地址，可以自行选择，类似于以太坊的节点地址，这些地址与信息发布者的地址无关。

节点可以选择任意的维度对地址进行折叠，然后找到离自己最近的N个地址并尝试连接。随着维度的变化，目标地址也可能发生变化。

观察者本身不依赖于自己的地址。

# 6 第三方服务

PDU协议中的第三方节点，不同于Mastodon等提供社区的节点，它们是基于公开的信息为用户提供便利服务的。

## 6.1 账户信息节点

这些节点可以快速获取某个地址的所有信息，用户可以实时查询目标地址对其他地址的行为情况，并根据综合逻辑计算其可见用户范围。

## 6.2 消息查找节点

这些节点帮助检索最新消息，通过引用地址查询消息等。

## 6.3 隐私消息传递

此类信息不属于整个系统，但可以利用这些服务来辅助实现实时交互等功能。

## 6.4 广告平台

在去中心化的社交网络中，广告必须嵌入到用户主动发布的信息中。广告宣传的结果应该通过可见账户之间的互动行为来统计。

## 6.5 中心化银行

这可以作为在去中心化社交系统中区块链技术的替代方案。在去中心化社交系统中，从最去中心化的工作量证明到混合的DPoS，再到中心化的货币系统，都有共存的可能。

## 6.6 功能性服务平台

如投票、调查问卷、游戏等。

需要注意的是，第三方节点通常作为功能平台出现，它们通常不是信息发布者，所以从这些节点获取的数据往往是经过加工的系统中公开消息。

# 7 隐私

传统上，许多人认为社交网络需要保护用户隐私。然而，我提出一种不同的观点：去中心化的社交网络本质上是一个完全公开的网络。在这种网络结构中，隐私内容并不直接包含在社交网络本身中，而是通过社交网络建立的身份系统来实现和保护。

具体而言，去中心化的社交网络将用户的数据和身份信息分离，通过加密技术和区块链技术保障用户隐私。在这一框架下，用户的公开活动和内容可以在去中心化网络中自由流动和共享，而敏感的个人信息则通过独

立的身份系统来管理和保护。这种方式不仅维护了网络的开放性和透明性，还增强了用户对自身隐私的控制权。

## 8 新用户的启动

新的信息发布者身份，需要与已经被接受的用户发生互动行为，才能让其地址开始被系统中的其他用户可见。这可以通过现实中的关系完成，也可以在第三方信息查询节点上完成。

每个新的信息获取者身份都会有一个快速扩展期，过后新用户的接受度就会降低。

所有用户都会维护可见用户的身份列表及部分信息列表。对用户来说，传统平台的关注列表相当于可见用户列表，而用户的关注列表则是可见用户列表中发布者身份的子集。

在这个系统中没有互相关注的概念，因为一个用户的信息发布者和信息获取者本就可以是多个身份、多个无关联的身份。

Twitter用户的平均关注人数为707个地址，而关注最多的Justin Bieber也只关注了273.6k人。我们可以用这个规模来计算可见用户的极限。

我们需要理解的是，在一个信息能够自由流通的系统中，当我们可见的活跃地址达到一万个左右时，几乎所有有价值的信息都会被认为是可见的，通过转发或引用实现。

对于点赞和评论的地址，我们可能会选择性地加入可见用户列表，但不会通过这种方式扩展可见用户范围。

## 结论

具有相同私钥签名且具有全序关系的消息，构成信息发布者身份。传统中心化社交系统的用户身份被分割成信息发布者和信息获取者身份，且这两个身份之间没有逻辑上的绑定关系，这不应理解为一个发布者和一个获取者组合就等同于原来的用户。

在信息公开的基础上，用户建立的关系全部公开。用户按自身规则意愿形成可见用户范围。对于各个信息获取者而言，他们所看到的信息并没有一致性的保证，因可见性不同。

与传统的中心化社交网络服务不同，现在所有内容都公开，隐私通过用户身份实现，但不助于用户身份的定义，而不属于本系统。

在去中心化系统中，信息可以自由发布的前提下，我们依赖用户自身的选择来减少无意义信息的传播。对于其他过激言论，如暴力、色情、煽动仇恨等，违反地方法规的内容，应交由地方处理，而不是该系统的职责。这就像比特币系统解决了双重支付问题，但不能解决洗钱问题一样。