# 用可关联环签名设计去中心化邮箱注册半固定账号匿名社交平台

## 1. 简介

现有的研究成果及其缺陷:

去中心化的理念已经崛起。区块链作为一种数据库,使用该链的无数设备组成去中心化网络,共享该数据库,重现了自由、开放、互助的互联网精神。以太坊是区块链技术的里程碑,它的数据库中存储的是一段段程序,被称为"智能合约"。利用以太坊的智能合约,我们可以设计去中心化匿名平台,即用户调用智能合约,将其言论发布到智能合约的存储中,使得其他用户能通过去中心化网络看到该言论。对比普通的部署在服务器上的社交平台,这种去中心化平台能够加快加载速度,降低运营成本,避免服务器崩溃造成的单点故障,保证用户的匿名性,保障言论自由。

通过上述智能合约,以及非对称加密技术,我们确实能实现点对点的即时通讯平台(即时通讯平台例如微信、QQ)。但若要利用这种技术构建去中心化的公共平台(公共平台例如微博、知乎、豆瓣、虎扑),则会面临用户身份不确定、水军攻击、刷屏、内容质量低下等问题。为此,我们需要进行改进,通过密码学技术来实现该平台账号通过邮箱注册,但又保护用户的匿名性。

本文成果:

本文所提出的平台是一种不需要服务器的,去中心化的匿名社交平台,设计目标是:
1)(邮箱注册、邮箱混淆)用户通过邮箱注册获得账号,但其他人无法确切得知某一邮箱是否注册过该平台;
2)(匿名性)只有注册用户可以在平台上发言,但无人知晓平台上的任一内容是从哪一个账号发出的;
3)(半固定账号)无人知晓不同帖子中的内容是否来自同一账号,但同一账号在同一个帖子中发言时,所有用户都知道这些内容来自同一个账号;
4)(防止重复注册)无人知晓某一邮箱注册的账号是否发表过言论,但若该邮箱使用者重新注册,则原账号不可再发言。

主要技术手段:

这些目标,主要通过一种密码学技术来实现:环签名,是一种用来保证数字货币转出账号匿名的技术,现有门罗币等数字货币使用该技术。它被认为有助于普及数字货币,因为在非匿名的比特币或以太坊中,转账记录是完全公开的,但现实生活中,人们的银行转账记录和现金转账记录明显不可能公开,特别是现金转账记录,没有任何第三方可以查询。匿名数字货币应当被理解为一种数字现金。

为什么要使用环签名呢?因为我们要做的是半固定账号匿名平台,它具有如下性质:
帖内可关联性:同一个人在同一个帖子下的发言可以被关联起来,即其他用户知道这是同一个人的发言。

帖间不可关联性：同一个人在不同帖子下的发言不可被关联起来。（当然，通过语言风格来分析除外）
匿名性：没有任何人知道发言者的真实身份。
（事实上这就是现在复旦树洞的面向用户的设计，然而树洞只是面向用户匿名，在服务器上是实名的）

利用环签名来设计匿名平台，保证无人知晓平台上的任一内容是从哪一个账号发出的，非常容易实现；但为保证半固定账号，需要改造可关联环签名中可关联性的设计，通过精巧的方式实现帖内关联。

同时，由于该平台具有强大的抗审查特性，为了防止对平台资源的恶意破坏，可以部署区块链技术，发行代币、运行智能合约及建立闪电网络来避免 DDoS 攻击。对于善意使用者，在使用平台时，其设备会自动“做种”，为他人同步平台资源，从而不需要支付代币来获取资源；但恶意破坏平台的行为需要付出极高成本。因此，部署区块链能强行实现“人人为我，我为人人”的互联网精神。但是，部署区块链不是必须的，可以采用其他数据库，尽管本文会采用这一技术模型进行阐述。

## 2. 预备知识

哈希函数：将不定长输入转换为定长输出的混沌函数。具有混沌性：对相同输入，输出相同，若输入稍有差别，则输出大相径庭。不可逆性：无法从输出倒推出输入。在下文中，用到两种哈希函数，其中一种把一个数映射为另一个数，另一种把椭圆曲线上的点映射为另一个点，它们都记为 H(x)。这些哈希函数是公开的。

数字签名：一种密码学手段，签名者拥有一对密钥：公钥私钥各一。他用私钥对一段文本进行签名，然后将{自己的公钥，文本，签名}一起发布。旁人可以通过公钥来验证这个签名确实是通过该公钥对应的私钥签发的，从而确认这段文本是签名者写下的。

利用椭圆曲线实现的密钥对：设 G 为椭圆曲线上的基点，k 为一个足够大的整数（取值范围为 2 的 128 次方）。椭圆曲线上可以定义一种加法，两个点相加得到另一个点。k 个 G 相加，记为 kG。则 K = kG 为一个公钥（它是椭圆曲线上的一个点），k 是其对应的私钥（它是一个整数）。它具有哈希函数的性质，即混沌性和不可逆性：要从 K=kG 推断出 k，是著名的离散对数难题，只能通过暴力破解，由于 k 足够大，这需要无数劫的时间；如前所述，它是一对密钥，可以用来数字签名；它还可以验明正身：把公钥 K 看成账号，私钥 k 看成密码，这个账号的主人可以在不泄露密码的情况下，证明自己拥有密码。

UTXO：比特币和门罗币这一类数字货币使用的模型。可以把 UTXO 理解为一种纸币。在这类数字货币中，一个公钥就是一个账户，每一个 UTXO 都是某个账户所有。一个账户的拥有者在这个账户拥有的一个 UTXO 上敲上戳（数字签名），来证明这张纸币被转让给另一账户；下一账户使用时，再进行签名。这种纸币可以分割，一般来说，一个 UTXO，可以被分割成一百亿亿份。使用者可以在这张纸币上写上：将这张纸币的多少份额转让给某某，其他份额

转让给某某，然后再签名。如果需要找零，可以把一部分份额转让给自己。

环签名：签名者知道其他若干人的公钥 K1, …, Kn，以及自己的公私钥 Ki, ki，其中 i 属于 1, …, n。在表达式中输入 ki，然后通过把这些公钥排成一个环形，迭代地输入 Ki, K(i+1), …, Kn, K1, …, K(i-1)来对一段文本签名，这个过程中需要用到的私钥有且仅有 ki。签名者发布{n 个公钥，文本，签名}后，验证者可以知道这些公钥里，有某一个公钥 Ki 对应的私钥 ki 拥有者对文本进行了签名，但不知道 i 具体是多少，即，不知道这 n 个人里具体是谁发布了签名。

可关联环签名：在这种环签名中，签名者需要使用并发布他的“钥匙扣”（key image）。对于密钥 ki 及对应公钥 Ki = kiG，钥匙扣为 kiH(Ki)（它是椭圆曲线上一个点 H(ki)自相加 ki 次）。钥匙扣具有如下性质：

1）在公布环签名时必须要公布正确计算的钥匙扣 kiH(Ki)，因为旁人需要通过它们，来验证这个签名确实是该签名者签发的；
2）旁人知道钥匙扣 kiH(Ki)，以及 H(K1), …, H(Kn)（因为哈希函数是 H 公开的，旁人可以对 K1, …, Kn 自行计算得出所有 H(Ki)），却无从推导 ki。如前所述，这是个离散对数难题，要破解只能通过不停地把 H(Ki)自相加，来看结果是否是 kiH(Ki)。等找到 ki，宇宙已毁灭。
3）对于同一个公钥，它的私钥是唯一确定的，因此钥匙扣也是唯一确定的。如果同一个公钥发布了两次可关联环签名，不论其他用来混淆的公钥 K1, …, Kn 一不一样，不论被签名的数据是什么，只要公钥 Ki 一样，这两次环签名都可以被关联起来。即，旁人都知道这个公钥 Ki 被使用了两次。

在可关联环签名中，签名者需要发布{n 个公钥，自己的钥匙扣，文本，签名}。

匿名数字货币的具体运行逻辑：

区块链是一种按时间排序的数据库，这个数据库中存储的都是（由转出方签名的）转账记录，它们就是上述可关联环签名。在非匿名货币中，转账的转出方和付款方都明确，因此个人财富可通过这些转账记录计算出来。但在匿名币中，转出方签名的转账记录有 n 个可能的转出账户，旁人包括收款方都不知道到底是哪个账户转出的钱。所以，旁人不知道一个账户里有多少钱。那么我们怎么知道转出方签发的转账是不是空头支票呢？靠的就是可关联环签名中必须使用的钥匙扣。

一对密钥，就是一个临时账户的卡号（公钥）和密码（私钥）。当户主想花掉这个账户里的钱时，就把其他人的卡号和自己的卡号混在一起，用这些公钥（其中包括自己的公钥 Ka），以及私钥 ka，对收款方的卡号 Kb 签名。这个签名的意思是：将 Ka 中的钱都转到账户 Kb 中。随后他试图把这个签名发布到区块链上以完成转账。合法的转账需要满足两个条件：

1）付款方账户 Ka 里收到过钱。旁人可以翻出之前那笔转账的签名信息来确认这一点，即，区块链上有一条转账记录，它是一条对公钥 Ka 的签名。这表示之前有一笔收款方是 Ka 的成功转账。
2）付款方账户 Ka 没有向外转过钱。大家可以检查之前所有在区块链上的转账记录来确认这一点。即，区块链上没有这样一条转账记录，它的签名使用了和这次付款方是 Ka 的转账签名一样的钥匙扣。

若转账合法，它就会被发布到区块链上，大家就知道那些账户中的一个，把所有钱转到了收款方账户 Kb 中。随后 Kb 的持有人就可以使用这笔钱了，因为它的账户满足了条件 1 和 2。但 Ka 的持有人就不能再使用这个账户了，尽管没有人确切知道他是否使用过这个账户，但如果他胆敢再次使用，第二次发布的{n 个公钥，自己的钥匙扣，文本，签名}中的钥匙扣就

会和第一次相同，从而不满足条件 2，从而无法被记录到区块链中。这就是使用可关联环签名的目的，防止双重花费。

注：这意味着每个账户只能使用一次，必须把所有钱一次性转出。不过每次转账的收款账户可以有很多个，付款方可以将一部分钱转入目的账户，另一部分钱转到自己的其他账户，作为“找零”。