**去中心化短信验证协议**

**（三无验证协议）**

## 介绍

去中心化短信验证协议的设计目的主要在于解决去中心化应用中用户账户身份认证的难题。是去中心化短信验证程序设计的协议框架。

如果在去中心化应用中仍采用传统的电子邮件或短信验证方式，那么其去中心化程度和服务的持续性将受到严重质疑。这是因为邮箱认证需要一个专门的发件箱地址，短信验证则需要一个在电信公司申请的短信接入号码或发送端口。这些资源不仅需要持续维护、还需要付费；那么，这些工作也是需要一个中心化的人为操作执行的。因此，这种程序会严重引发用户的不信任感，与去中心化应用的核心理念相悖。

在比特币诞生的背景下，非对称私钥被用作于权限认证手段。这种方式是完全去中心化的认证方案。后来为了便于用户记忆和管理，开发者们衍生出了助记词的解决方案并在去中心化应用中广泛使用。但是这些方案都存在私钥或助记词丢失、忘记、被盗用等风险，并且让用户产生一定的焦虑情绪。

去中心化短信验证协议的验证办法可以将系统设计为，用户无需密码、无需私钥、无需助记词的方式进行身份验证，因此我们也称为“三无验证”。

## 角色与名词

* 服务端

服务端是网络应用中提供服务的一方，一般是指区块链中的智能合约应用，主要负责处理客户端的请求和提供相应的服务，并通过身份识别为用户提供私有专属数据和资源。

* 客户端

网络应用中接受服务的一方，主要负责向服务端发送请求和接收响应数据，与用户进行交互和展示结果。并代表用户专属身份访问其私有专属数据和资源。

* 用户

一个真实的个人，服务的使用者和专属资源的拥有者，通过客服端与服务端交互，这里指该应用程序最主要的服务对象。

* 验证终端

指为用户提供身份验证的接入终端，终端由移动设备并安装对应的验证终端程序和一个承载MSISDN的SIM卡构成。负责接收用户SMS验证信息、和获取用户发送号码并转发到服务端。

* 验证终端池

由多个验证者提供的验证终端构成验证终端池。

* 验证者

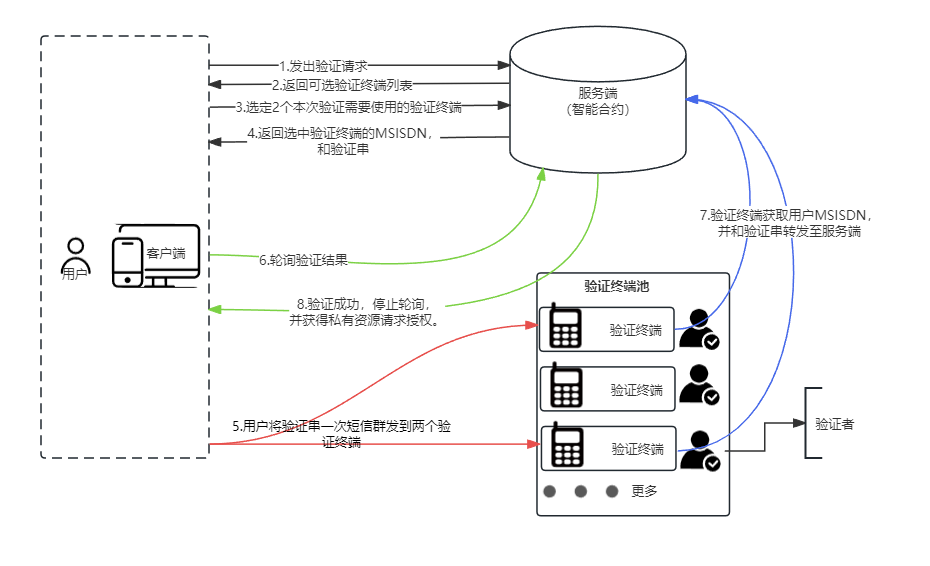
在系统中取得验证权限的个人，负责启动和维护验证终端。

## 方法

首先，系统允许不特定用户申请成为验证者，并为验证者提供一个验证终端应用程序，该程序在用户授权下具备访问手机短信的权限，验证者利用一台闲置的智能手机和一个专用的MSISDN，并安装和启动该验证终端程序。这样，当有用户需要身份验证的时候，就可以通过短信发送验证字符串到这个MSISDN接入号，验证终端程序就可以检测和读取短信中的验证串和发送者号码，并将转发回传到服务器或智能合约，通过服务器程序或智能合约进行比对相关信息，就可以完成用户身份验证。

为了提高可靠性和可用性，系统需要建立一个验证终端池，允许更多的用户成为验证者。这样，系统在用户在需要身份验证时，就可以通过轮选机制为用户提供身份验证接入服务。一般系统需要设计一定的奖励策略来鼓励验证者提供长期和可靠的服务。

## 协议流程



## 验证者激励机制

作为一个去中心化的开放应用，我们需要吸引不特定的用户成为验证者，并为他们提供适当的奖励机制，以激励他们为系统提供可靠和持续的验证服务。根据具体的业务情况，我们还可以设置必要的验证者门槛和退出机制，以确保长期有验证者为用户提供验证服务，保证系统可靠运行。

## 防止验证者欺诈

验证者欺诈是指验证者通过技术手段伪造他人的MSISDN转发至服务端，骗取其身份的行为。

为了防止验证者欺诈，一般采取以下措施：

1. 当在验证终端池返回用户可选的验证终端列表时，应该以非明文或半明文的形式显示验证终端的接入的MSISDN。这样，验证者将无法在可选验证列表中选中自己控制的验证终端，从而防止验证者通过技术手段伪造他人的MSISDN进行欺诈。
2. 保持多个验证终端同步验证，这样做，不诚信的验证者很难与素不相识的其它验证者共谋。这种机制可以进一步增加不诚信验证者的操作难度。

通过以上措施，可以有效地防止验证者欺诈行为的发生，保护系统的安全和可靠性。

## 可靠性评分

为了确保验证的可用性和可靠性，我们可以建立一种适当的评分机制，以激励验证者为验证终端保持高质量的网络和电力。通过实时收集终端的移动信号质量和网络延迟的信息，我们可以形成一个实时的评分。用户可以根据这个评分选择质量更高的验证终端，从而进一步促进验证者更好地维护验证终端的可用性和可靠性。这样既能保障用户验证的流畅性，也能激励验证者提供更优质的服务。

## 流程自激措施

当系统刚开始运行的早期还没有用户加入成为验证者的时候，系统需要一个中心化的接入号为早期用户提供验证接入服务。之后，当验证者达到一定数量后可设置自动移除该接入号码。

Delta Core Developer

2023年11月