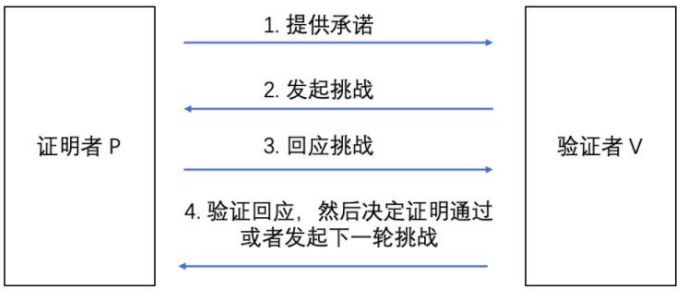
去中心化红包

1 概述

红包是中国特有的一种传统文化，已经演变成日常交际中不可缺少的一环，并随着文化输出，在国外也受到了越来越多的欢迎。传统的红包生成方法通常是基于确定的随机性算法，如微信红包，但是其无法在根本上实现令人真正公开可信的随机；在去中心化的区块链中应用红包，也可以促进用户进行交易，达到增加平台活跃度的效果。在此，我们提出了一种基于可验证随机函数的去中心化红包的生成方法。

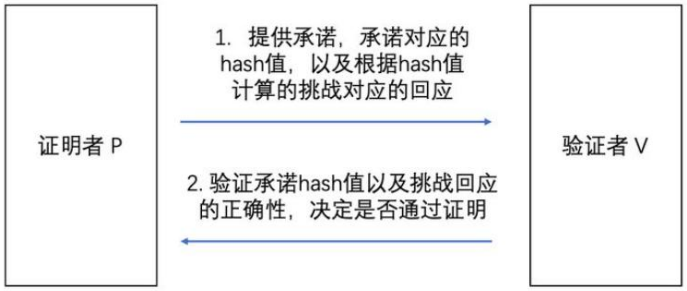
2 零知识证明

零知识证明(Zero-Knowledge Prove)指证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的，它具有正确性、完备性、零知识性。零知识证明根据其交互性可以分为交互式和非交互式，其中在交互式零知识证明中，证明者 P 需要提前提供承诺等待验证者 V 发起挑战，然后根据挑战中的随机值回应挑战验证者 V， 通过进行多轮挑战，直到认为证明者 P 证明正确的概率达到足够大的时候认可该证明。这种交互性的零知识证明需要双方建立通信，并要进行多轮交互，因此通讯效率较低，也无法满足双方无法通讯的情况。



非交互式零知识证明能够很好的解决交互式中存在的问题，通过 Fiat-Shamir 变换可将交互式证明转化为非交互式证明，其中利用了哈希函数结果的随机性，证明者 P 可以将承诺数据的哈希计算结果作为随机数列用于生成挑战及挑战对应的回应，对比交互式证明，非交互式减少了重复的挑战和回应过程，证明者只需要发送一次数据，验证者便可自行验证而无需再进行通信。

在可验证随机函数中，一个重要的特点就是应用了非交互式的零知识证明使得最终生成的结果拥有可验证性。



3 可验证随机函数

可验证随机函数（Verifiable Random Function,VRF）是一种将输入映射为可验证的伪随机输出的加密方案，它的最终输出结果是一个随机数，由于函数执行过程中产生了生成者对应的非交互式零知识证明，验证者可以通过公钥确定随机数的合法性。可验证随机函数具有可验证性、唯一性和随机性。

一个基本的可验证随机函数应该包括 VRF_HASH,VRF_Proof,VRF_P2H,VRF_Verfiy 四个子函数，其中证明者通过 VRF_HAS，VRF_Proof 使用私钥 SK 对信息进行加密生成加密结果 result 和证明 proof，并将 result 和 proof 发送给验证者，验证者可以通过 VRF_P2H 对 Proof 进行验证，检验 Proof 是否是根据 result 生成的，若能够通过此函数推出 result 则证明者需要将其公钥 PK 和加密前的原文发送给验证者，验证者通过 VRF_Verify 验证所有参数是否正确。

具体协议流程如下：

- 1.证明者生成一对秘钥，PK 和 SK；
- 2.证明者计算 result = VRF_HASH(SK,info)；
- 3.证明者计算 proof = VRF_Proof(SK,info);
- 4.证明者把 result 和 proof 递交给验证者;
- 5.验证者计算 result = VRF_P2H(proof)是否成立，若成立，继续，否则中止；
- 6.证明者把 PK，info 递交给验证者；

  7.验证者计算 True/False = VRF_Verify(PK,info,proof),True 表示验证通过，False 表示验证未通过。

4 基于可验证随机函数的去中心化红包生成方案

为了提供公开可验证的红包生成，我们提出了基于可验证随机函数的红包生成方案。该方案能够通过可验证随机函数使得最终生成的红包金额是公开可信的，人们可以通过存放在链上的数据进行验证，解决的传统红包的非中心化问题。

在该方案中，用户在领取红包时，需要事先生成自身的公钥、私钥以及初始随机数，初始随机数可通过一些伪随机生成方法在链下生成，如把领取的时间进行哈希运算等，用户将该初始随机数运行可验证随机函数生成用户的子份额发送给链上智能合约，所有用户需要在规定时间内将自身的子份额发送至合约，合约会根据 VRF 的机制对份额进行验证，验证不通过的用户会被踢出红包生成过程；当所有用户将子份额均上传成功，智能合约会对所有份额再次进行 VRF 运算，这样可以保证智能合约的执行也是公开可验证的；将最终 VRF 运算的结果进行哈希运算即可得到红包生成的随机种子，可以通过规定的逻辑对随机种子进行分配。

具体的方案流程如下：