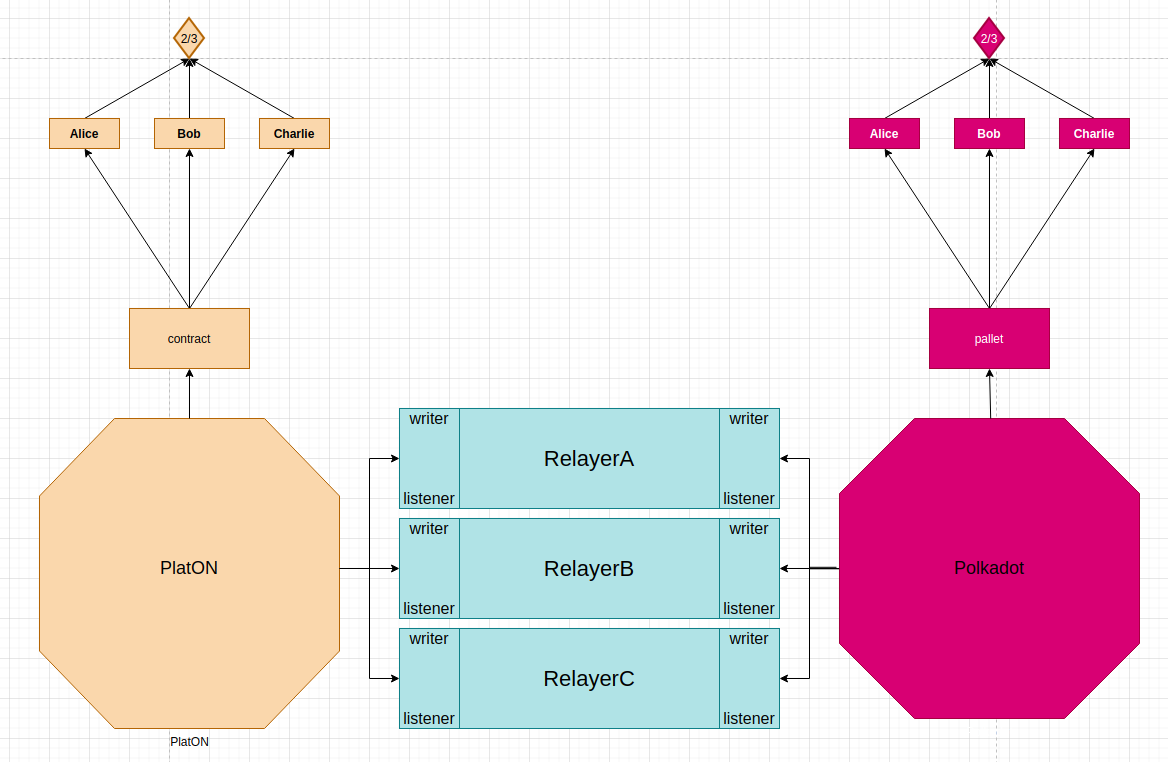
# Platdot开发设计

## 1，概览

PlatDot当前基于可信模型，依赖于受信任的见证人，但其多重签名的机制将确保任何Relayer都无法独自挪移资金。在多重签名方案下，Relayer可以创建转移资产的提案并对该提案进行投票，但在达到指定阈值之前无法执行转账，也就是说跨链交易被确认之前，必须获得足够多的Relayer投票，在超过某个阈值后才能执行。这种机制要求多方验证每笔跨链交易。



以Alaya网络和Kusama网络之间进行资产跨链为例，由多个Relayer组成的Platdot进程所连接，每个Relayer都绑定了两个网络上的见证人账户，以RelayerA为例，分别绑定了Alaya网络的见证人账户Alice和Kusama网络的见证人账户Alice，Platdot进程连接见证人账户，对交易进行签名并通过RPC传输到对应网络上。

在能够和网络进行交互后，还需要完成多重签名逻辑的设计，因此要求两个网络中都有能执行多签签名逻辑的脚本，Alaya网络中部署Bridge和Handle合约完成多重签名逻辑，而Kusama网络中的multisig模块支持多重签名，根据multisig模块的具体方法完成相应设计。

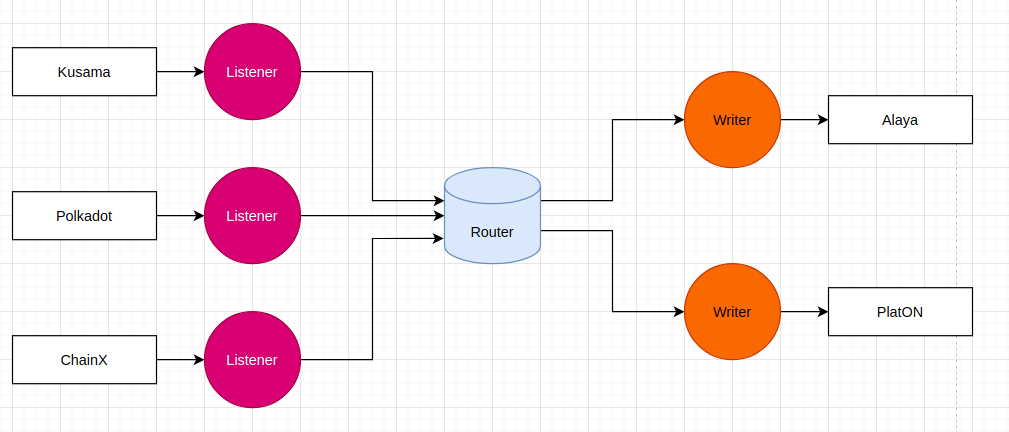


## 2，程序模块设计

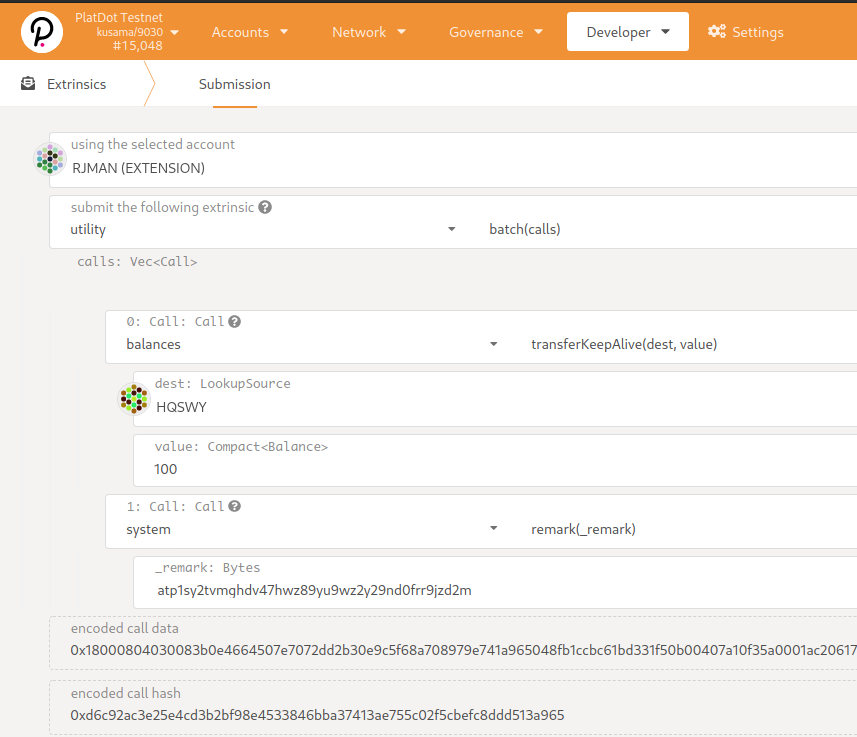
### 2.1，Solidity合约

PlatDot的solidity合约的多重签名逻辑主要由Bridge合约完成，并将特定的发行和销毁功能委托给相应的Handler合约，ERC20合约则负责执行具体Token的铸造和销毁，三者共同完成多重签名跨链方案的实现。

### 2.2，发行流程



#### 2.2.1，构造跨链充值交易

在Kusama网络上的账户，如果需要将KSM充值到Alaya网络获得AKSM时，要发送一笔携带Alaya接收账户地址的交易，在Kusama网络中Utility模块的batch方法能够很好地满足需求，交易参数如下。

Utility中有两个方法：

方法一：balances.transferkeepalive方法能够转移用户的KSM至多签地址HQSWY（五个见证人H、Q、S、W、Y共同维护的多签地址）。

方法二：system.remark方法能够携带自定义信息，例如另一个网络的接收地址。

#### 2.2.2，Listener监听Kusama网络的跨链交易

Listener即为和Kusama网络建立的连接，能够监听网络上每个块的交易和事件，并从区块信息中检索出跨链交易。一旦检索出跨链交易，就将跨链交易构造为Message，通过Router转发给Alaya网络的Writer进行处理。

#### 2.2.3，Writer解析Router转发的消息

Writer接收消息并解析出所需的参数，构造交易与Alaya的Bridge合约进行交互，在目标链的Bridge合约上创建一个提案。提案具有不同的状态：不活动、活动、最终确定和已转移，新创建的提案被标记为活动的。在创建多重签名提案后，若提案达到设定阈值，提案状态会被标记为最终确认，就能够执行提案的交易，将AKSM发行到接收者地址。

### 2.3，赎回流程

赎回流程类似于发行，只是处理操作不同。

#### 2.3.1，构造跨链赎回交易

用户通过调用Bridge合约上的Deposit方法发起赎回交易，该方法将调用代币合约上的“transferFrom”方法，并发出一个Deposit事件。

#### 2.3.2，Listener监听Kusama网络的跨链交易

Relayer的Listener模块通过建立和Alaya网络的连接，监听对应的Deposit事件并从区块中解析出交易参数。构造为Message，通过Router转发给Alaya网络的Writer进行处理。

2.3.3，Writer解析Router转发的消息

Writer接收消息并解析出所需的参数，构造Multisig.Asmulti交易，在Kusama网络上创建新的多重签名交易。Multisig的多重签名提案有三个阶段，新建、批准和执行，且必须依序完成。Writer对交易的三个阶段进行处理，构造不同的参数，最终完成一笔多签赎回交易，将KSM从见证人共同维护的多签地址转出到接收者地址。

### 2.4，转账

调用ERC20合约的transfer方法进行代币转移。