# 系统组成：



# 大致流程：

1. 注册：

用户必须注册才能进行后续的购币和交易操作，用户注册的核心操作：监管者将用户的地址公钥哈希值存储到用户公钥池中。监管者维护一个公钥池。

1. 兑换：

假设用户是通过向发行者购买的方式获得初始数字货币的，然后才能进行转账交易。购币的核心操作：**发行者将用户购得的数字货币承诺的哈希值添加到系统的承诺池中。**

**其中cm形式为pederson承诺**。

1. 交易：

假设S要向R支付v\_r。S原本有v\_o，支付v\_r，给自己找零v\_s。

交易时，

* S生成对交易金额的承诺：CM\_s=v\_s\*G1+r\_s\*H，CM\_r=v\_r\*G1+r\_r\*H, 其中对原始金额v\_o的承诺是兑换时生成的，CM\_o=v\_o\*G1+r\_o\*H。
* S生成对交易双方身份的承诺：CM\_spk= S\_pk \*G1+r\_spk\*H，CM\_rpk= R\_pk \*G1+r\_rpk\*H,。
* S用接收者R的公钥加密v\_r，得到:

E(v\_r)= (v\_r\*G1+r\_r\*H, r\_r\*G2)

* S用监管者公钥加密v\_o，v\_s，v\_r，得到:

E(v\_o)= (v\_o\*G1+r\_o\*H, r\_o\*G2),

E(v\_s)= (v\_s\*G1+r\_s\*H, r\_s\*G2),

E(v\_r)= (v\_r\*G1+r\_r\*H, r\_r\*G2)

* S用监管者公钥加密交易双方地址公钥S\_pk，R\_pk，得到:E(S\_pk)，E(R\_pk)。
* 同时S生成零知识证明，证明：

1. CM格式正确：零知识格式正确证明。
2. 对CM\_o，CM\_s，CM\_r使用range proof，证明三个金额都是大于等于0的。
3. 对CM\_o，CM\_s，CM\_r使用会计平衡证明，证明交易满足会计平衡。
4. 证明3个承诺与3个接收者密文中的金额和地址公钥分别相等，即CM\_o与E(v\_o)中的v\_o是相同的，CM\_spk与E(S\_pk)中的S\_pk是相同的。
5. 证明3个承诺与3个监管者密文中的金额和地址公钥分别相等，即CM\_o与E(v\_o)中的v\_o是相同的，CM\_spk与E(S\_pk)中的S\_pk是相同的。

上述所有零知识证明统称为Π。

最终公布交易tx=( CM\_spk ，CM\_rpk ，CM\_o, CM\_s, CM\_r，E(v\_o)，E(v\_s)，E(v\_r)，E(S\_pk)，E(R\_pk)，sig，Π)。

1. 验证：

大众看到公布的交易，可以验证

1. CM\_o属于CM池：交易初始货币是否存在。
2. S\_pk，R\_pk属于PK池：交易双方身份是否合法。
3. 验证Π。
4. 监管：

监管者看到公布的交易，用自己私钥解密其中的密文，查看交易双方身份及金额，可验证：

1. S\_pk，R\_pk属于PK池：交易双方身份是否合法。
2. 明文金额是否会计平衡。