

Zether

Fully-decentralized confidential payment mechanism

基于账户的方法作为交易机制的基础（公私钥作为一个账户的分辨依据）

隐藏了交易数额的信息，并以零知识证明（ Σ -Bulletproofs）实现数额在各个合约、账户之间实现流通——将账户对应资金在合约中进行锁定，结合相应零知识证明实现隐私

构成部分：

1. **Global Setup**：为后续所需要使用的密码学协议实施 **Trust Setup**；并初始化每个账户对应的参数
2. **Zether 合约**：
 - (1) 5 个公开方法：Fund、Burn、Transfer、Lock、Unlock
 - (2) 每个公开方法被调用时必须检查是否存在未处理的 Transaction，即调用合约内部私有方法 RollOver
3. **User Algorithm**：表明了用户如何与合约进行交互
4. （可选）匿名 Zether：实现了在一组用户中除了隐藏交易金额，还隐藏了交易的发送方和接收方的信息

零知识证明 Statement：

1. **Burn Transaction**：
 - (1) 将账户余额全部转移出
 - (2) **Statement**：证明用户确实拥有账户对应公钥 y 的私钥；证明账户余额 b 被正确的加密
 - (3) 使用 Σ -protocol 即可证明
2. **Transfer Transaction**：
 - (1) 从公钥 y 的账户转移数额 b^* 到公钥 y' 的账户
 - (2) 分别将 b^* 在公钥 y 与 y' 下加密得到 $(C, D), (C', D')$
 - (3) **Statement**：
 - ① 证明 2 组密文都是关于 b^* 的正确加密
 - ② 证明 b^* 是正数
 - ③ 证明公钥 y 对应的账户余额在转移 b^* 出去后仍是正数

拍卖应用：

是英格兰拍卖（低价开始出价，价高者得），竞拍成功者只需支付第二高出价的价格

流程：

1. **竞拍阶段**：竞拍者将对应拍卖价格的抵押资产转移到新账户并与拍卖合约（AUC）锁定
2. **揭露阶段**：只有竞拍者提供正确的竞拍价格和相应证明给 AUC，合约才会对锁定账户进行操作
 - (1) 若揭露价 < 最高价，AUC 解锁揭露用户对应的账户
 - (2) 若揭露价 > 最高价，AUC 解锁先前最高价对应账户并记录其出价，更新最高价格
3. **最后阶段**：AUC 会将第二稿价格与最高价的差价返回给竞拍成功者