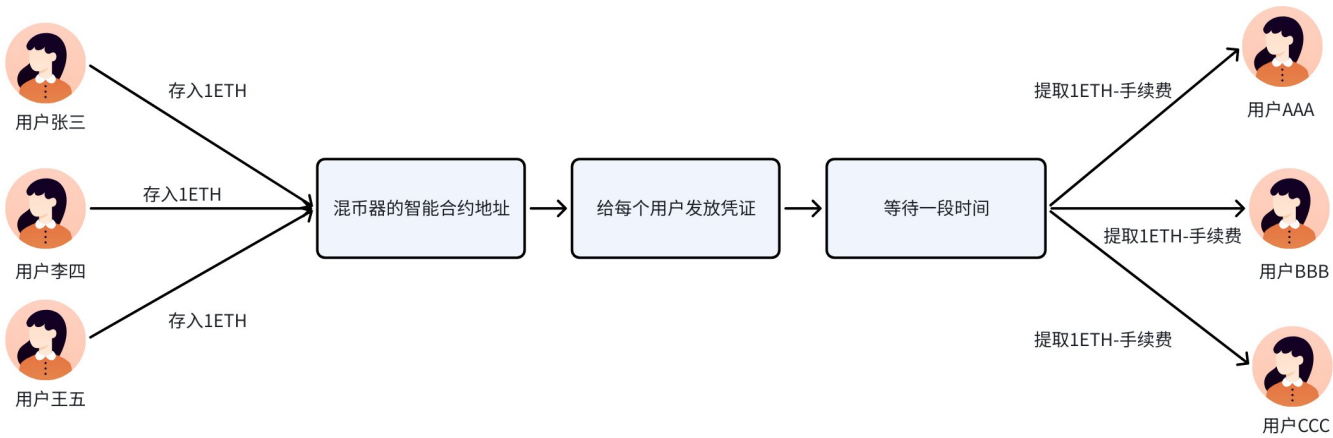
作业2:研究市场上的混币器及各自优势

一、混币器工作原理

市场上不同的混币器在原理上虽然采取的技术不同，但是底层逻辑都是打破资金流向的关联性，让监控追踪时候无法将流入资金与流出资金有效关联，从而失去追踪意义。



二、不同类型的混币器

混币器类型	代表项目	工作原理简介	优点	缺点与风险
中心化混币器	ChipMixer	用户信任一个中心化运营商来处理混合过程。	通常简单易用。	单点故障：运营商可能跑路、被黑客攻击或被执法部门查封；信任风险：运营商可能记录用户的入金和出金地址关联。
去中心化混币器	Tornado Cash	通过智能合约和零知识证明技术，无需信任运营商。	无需信任：合约代码即法律，运营商无法窃取资金或关联记录；抗审查性更强。	使用门槛稍高；协议风险：智能合约可能存在未被发现的漏洞。
隐私币	Monero, Zcash	在协议层通过加密技术默认隐藏交易信息。	隐私是默认的，无需额外步骤；隐私性极强。	需要持有另一种代币，而非增强比特币/以太坊的隐私。
CoinJoin	Wasabi Wallet, Samourai Wallet	将多笔交易合并为一笔大型交易，外部观	非托管式，用户始终掌控私钥；协作式混合。	需要在线寻找其他协作方；混合规模有限

		察者难以区分输入和输出的对应关系。		

三、关于Tornado Cash

1. 存入 & 获得“存单”：你存入资金时，会生成一个的 “凭据” ，就像一张不记名的存单。
2. 提取 & 出示“存单”：当你想要取款时，你向智能合约出示这个“凭据”（通过零知识证明，你不暴露“凭据”本身，只证明你拥有它）。合约验证通过后，就允许你将资金提到任何一个新地址。
3. 用一个游乐园的例子说明：

一个犯罪分子拿着200元赃款到游乐园去玩旋转木马，押金200元，给他一个凭条，玩完了需要用凭条取回押金；监管只能找到犯罪分子到了游乐园玩了旋转木马，但是取走赃款200元的不一定是他们要找的犯罪分子

游乐园示例	对应的Tornado Cash现实
游乐园 & 旋转木马	Tornado Cash 智能合约
存入200元押金	向合约地址存入固定额度的ETH
拿到一张凭条	获得一个链下的、秘密的“零知识证明凭据”
用凭条取回200元	使用零知识证明，从合约中提取等额资金
取回的可能不是原钞票	资金池模型，取出的是池中任意资金
监管追踪冠字号	区块链分析师追踪交易哈希和资金流向
追踪在游乐园中断	链上追踪在Tornado Cash合约处中断