去中心化交易所设计

设计原则采用的是链下订单薄，链下撮合，链上交易。用户在链下发布订单，链上负责审核交易能否成交，并记录订单信息和完成情况。

链上指的是操作执行发生在区块链系统上，并将数据记录在区块链系统上。

链下指的是数据存取和操作发生在区块链系统之外，可独立运行。

链下订单薄：

订单薄存储用户的订单数据以及订单状态，对外提供检索功能。订单薄存储在链下数据库中，订单薄数据通常不上链。

基础订单数据为<tokenGive, tokenGet, amountGive, amountGet, Signature>等，分别记录了<卖出资产类型，买入资产类型，卖出资产额度，买入资产额度，订单拥有者(Maker)签名>等数据。买卖双方自行交换订单数据进行撮合匹配，或从第三方数据提供商获取订单数据撮合匹配。

订单 ID 为订单数据的 hash 值。签名为订单数据 hash 的数字签名。

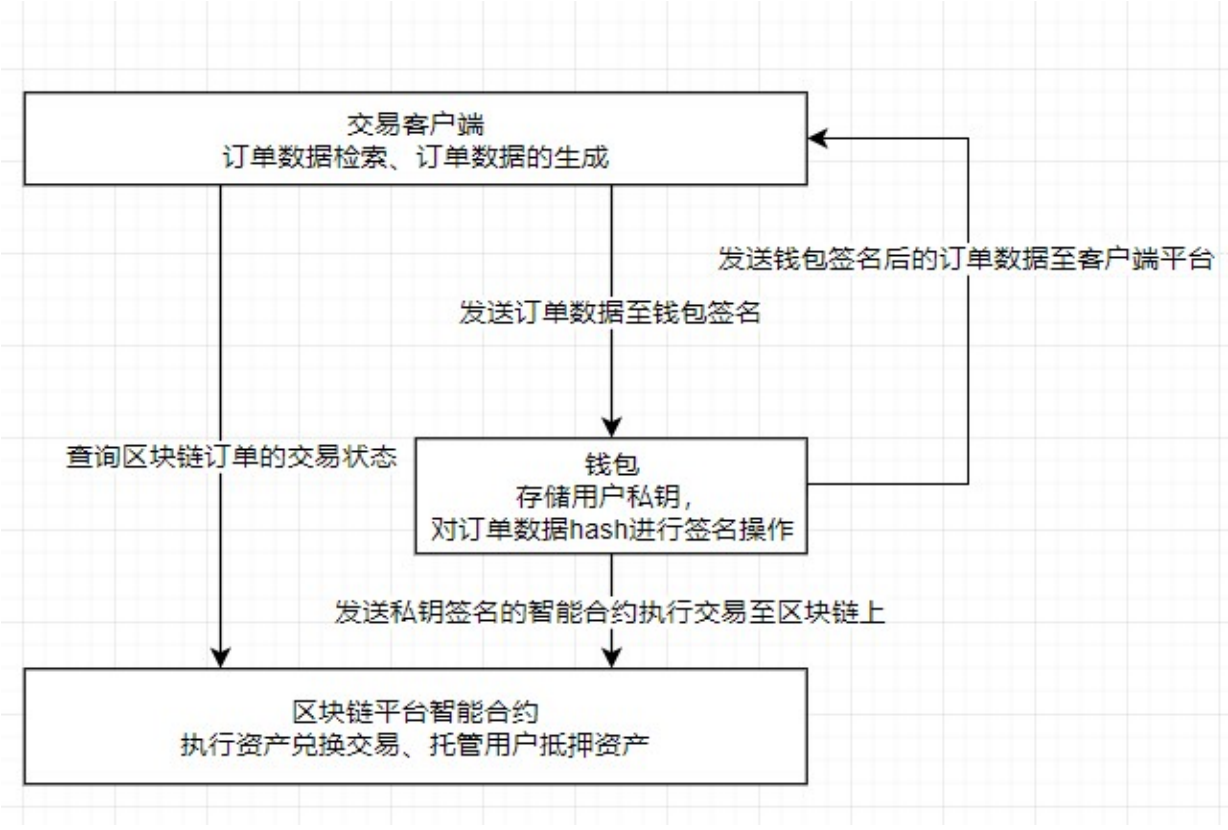
链下撮合：

撮合过程发生在链下，撮合过程主要是判断买一价大于卖一价交易是否匹配，买家寻找合适订单等这一过程。撮合操作一般在订单薄的后台程序中进行或个人指定订单进行。

订单数据由用户提供生成，用户需要在显示历史数据等交易平台上进行决策，撮合过程发生在链下。平台提供最新订单交易情况与订单薄数据，供用户作为信息参考。撮合过程发生在链下，降低链上智能合约复杂度并提高合约执行速度。

链上交易：

买卖双方对各自交易数据签名，发送至区块链系统上，由区块链上智能合约验证交易签名、交易数据合法性，最终执行交易。由于交易数据经由买卖双方私钥数字签名后才可生效，因此用户具有唯一操作权力。



交易客户端：可以为 web 网页前端+服务器后台，也可以是移动手机 app 系统、或者 PC 客户端。具体功能为存储订单薄数据，实时监控链上合约订单成交情况，生成订单最新状态。提供链下订单薄和链下撮合功能。

钱包：功能为存储用户私钥，提供对订单数据的私钥签名操作，并发送调用链上的智能合约的交易。

可部署交易所智能合约的区块链平台：提供链上交易功能。

去中心化交易所的智能合约至少需要提供的功能如下：

1、 合约充值

a) 用户充值名下资产至合约。

2、 合约取现

a) 用户从合约取出名下资产，余额不足时，合约执行失败。

3、 执行订单的交易

a) 判断订单数据是否合法；如验证签名是否为创建者所签、所签名的订单数据各字段数据是否满足允许范围值、订单是否已经结束等；

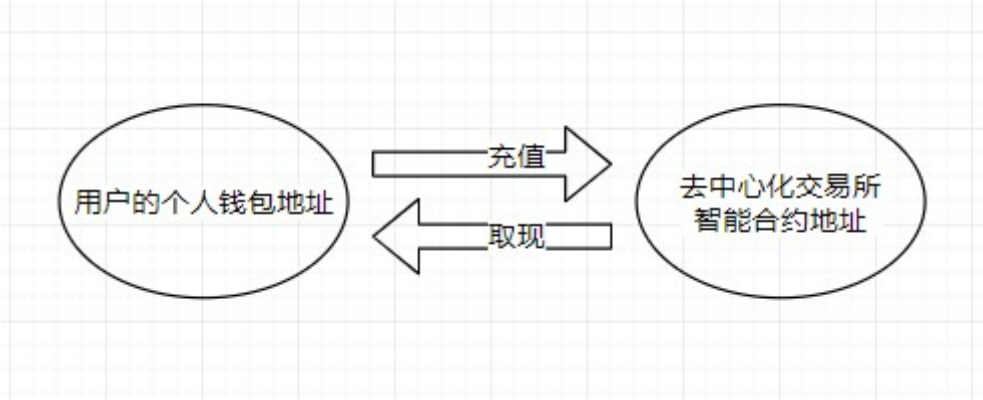
b) 判断买卖双方抵押至合约的金额是否满足订单成交的额度；

c) 按照额度与价格，交换双方抵押在合约的资产，达成交易；

d) 记录订单成交后的状态。

智能合约可以提供事件机制，外部系统通过订阅订单数据、用户充值等事件来获取链上操作执行的情况。

充值/交易流程



充值流程为普通转账或智能合约调用。

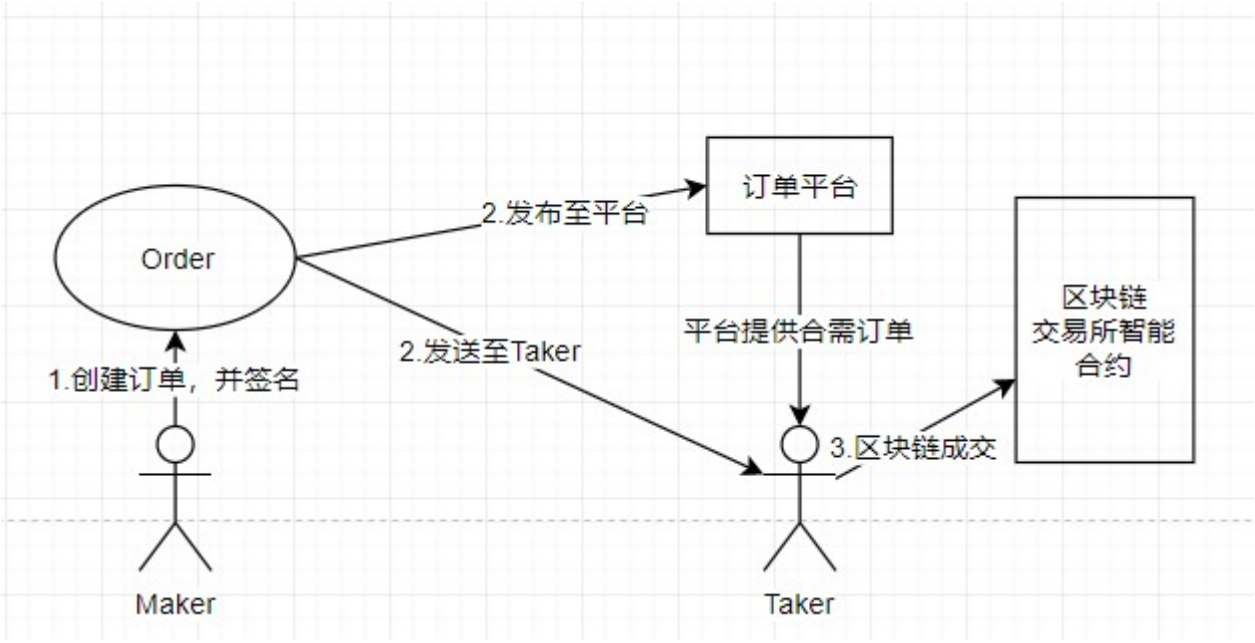
取现操作需合约执行获取用户的取现额度，为智能合约调用。

交易角色如下：

Maker 创建订单，并对订单数据数字签名，每个订单都有其交易额度。

Taker 为吃单人，每次交易会成交订单一定的额度。

交易流程如下：



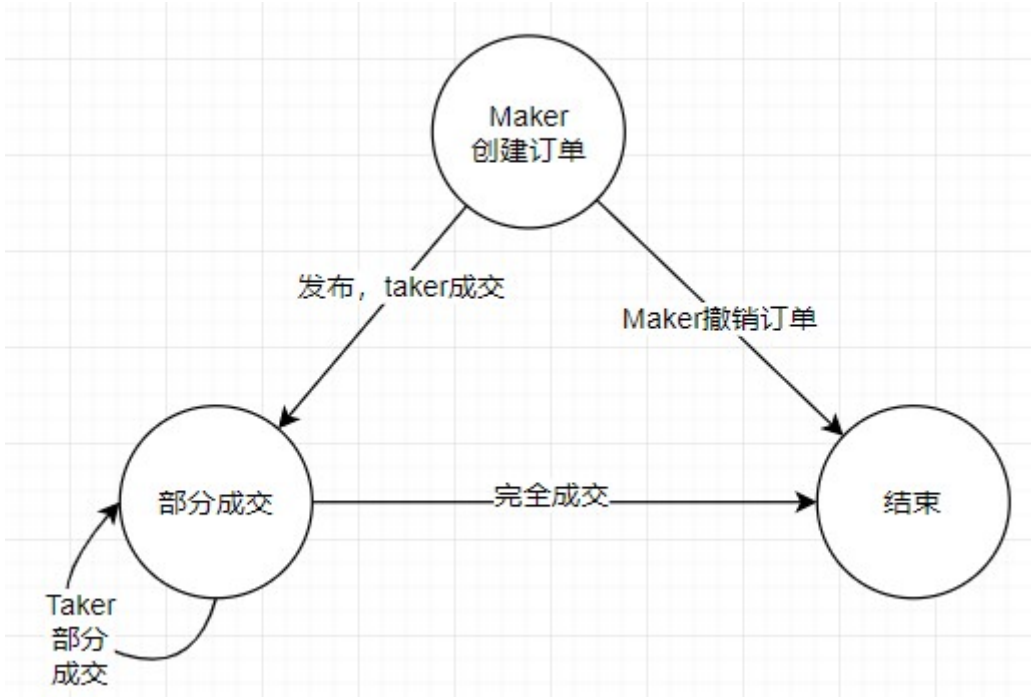
1、Maker 使用私钥对发布的订单 hash 进行签名，并将其发送给第三方平台或 Taker

2、Taker 从 Maker 或第三方平台获取订单

3、Taker 创建订单交易的合约调用操作请求，发送至区块链系统

链上执行 Taker 发送的操作，交换各自的资产，达成交易

订单状态迁移



1、Maker 创建订单，并对订单数据数字签名，每个订单有一定的额度。，Taker 为吃单人，每次交易会成交订单一定的额度。

2、Maker 发布订单，Taker 部分成交直到成交结束。

3、Maker 可撤销订单，直接结束订单。