Multilateral Token Trade Protocol (MTTP)
多边代币交易协议非技术简介

daniel@mttp.io

2017 年 6 月 17 日

1 区块链和代币

自中本聪发明比特币到现在，区块链技术得到越拉越多的关注和投入。很多企业在大力布局区块链生态，资本和人才不断进入这个生态，监管部门和学术机构也逐渐对区块链技术产生兴趣。从形式上人们将区块链分为私有链，联盟链，和公有链。至少目前看来，私有链得到的关注很少，而联盟链也依旧处在早期试验阶段。包括 Hyperledger 和 R3 在内的很多项目都还没有成功的应用，也许联盟链还需要三两年的时间才能真正产生价值。

目前区块链最成功的应用依然是在公有链上的价值网络，这种网络包括简单的虚拟货币，如比特币，莱特币，也包括以数字货币驱动的智能合约平台，如以太坊。价值网络的共有特点是数据中承载了有共识的价值，而不仅仅是业务数据。如果我们将数字货币从广义的区块链生态中去掉，这个生态就会支离破碎，没有任何生机。

根据 coinmarketcap.com 的统计，截止 2017 年 6 月 17 日，公有链的总价值超过 1090 亿美金，每天的交易额也超过了 42 亿美金，同比分别增长了 830% 和 1250%。我们相信这中增长的势头还会延续一段时间，毕竟对于整个生态，从排斥到认可和投入，现在还只是刚刚开始

2 中心化交易所的固有风险

对于任何价值网络，流动性都非常重要：低流动性会增加金融成本，反之则降低金融成本。目前每天 40 多亿美金的虚拟货币交易，绝大部分是通过现有的，中心化技术实现的交易所完成的（我们后续简称为“中心化交易所”）。

中心化交易所的模式大同小异：用户通过充值，将法币和虚拟货币（后续我们统称为代币）发送给交易所控制的银行账号或区块链地址；确认资金到账后，交易所会在内部，中心化技术支撑的虚拟账户系统中更改用户相应币种的余额；每次交易的结果是这些余额的变化，而非真正做了法币或虚拟货币的交换。用户如果想完成真正的兑换，要对交易所发起提现请求，提现成功后，真正的交易才算完成。

中心化交易所有着固有的局限性和风险。这些问题都是系统性的，是再好的 IT 技术也无法消除的。包括：

2.1 资金托管

为了在撮合之后能够保证交易双方按照指定价格交换不同类型的代币，交易所只好要求用户先将代币交给自己托管，否则就无法建立对用户订单的信任。资金托管对于用户的风险主要来源于两个方面。一是交易所经营者的商业道德；二是交易所的资金保管能力。

由于多数国家缺少甚至没有对交易所的监管，交易所经营者有可能在用户不知情的情况下，挪用用户托管的资产进行高风险投资。一旦投资失败，交易所可能根本没有能力偿还用户的损失；或者只好通过不断吸纳新用户的托管资金完成老用户的提现请求。

对于不愿挪用用户资产的交易所经营者，资产保管就成了一个没有任何收益，而且要有相当投入的苦差事。交易所不仅要有完善的冷热钱包机制，还要对系统中各种服务器做适当的隔离，同时要严谨制定和维护充值提现的相关工作流和不同人员的角色和权限。这些工作的投入，甚至要远高于交易所的撮合系统。很少有交易所能够遇见到资金托管系统和流程中的全部问题并将其及时解决，往往是资金丢失或被盗后才采取补救措施。

总的来说，用户把资产托管给交易所对中心化交易所模式是必要的，但风险对于用户和交易所都是巨大的。

2.2 内幕交易

由于交易所对交易撮合过程的完全控制，交易所可以比用户看到更多、更全面的数据，也可以对某些数据和指令采取特殊的处理，比如使用更高的优先级。这些内幕消息和内幕操作对于多数的用户都是非常不公平的。特别当交易所本身也参与交易的时候，还可能进一步操纵价格，造成普通用户的巨大损失 — 这种损失在有杠杆的时候尤其显著。

2.3 流动性分散

中心化交易所依然有较明确的地域定位，目前几乎还没有国际化特别好的平台，这其中包含语言，用户习惯，监管等多方面原因。现有的一百多家交易所每家都有自己的行情和深度，彼此没有办法实现共享或者联合撮合。交易所越多，买卖价差也就越大，订单深度也就越浅。换言之，如果全球只有一家交易所，那么深度和价差都会是最优的 — 因为这样一家交易所将汇集所有的流动性，而不像现在这样，流动性是分散的。但是，中心化交易所理论上无法共享订单，也就无法汇集流动性。而真正全球只剩下一家交易显然也不切实际。

3 MTTP 的目标和特点

MTTP 是去中心化交易所的协议层，目标是解决中心化交易所固有的风险和局限性，即上述的资金托管风险，内幕交易风险，和流动性分散的局限。具体来说:

- **MTTP 交易没有充值提现过程，用户和交易所都是零风险**。

- **MTTP 消除内幕交易，所有交易数据需要提交到区块链验证**。
- **MTTP 订单可共享给多个交易所做竞争式联合撮合，市场深度更大，价差更小，费用更少，迁移成本为零**。

我们称 MTTP 的撮合模式为 "**链外撮合，链上清算**"。具体技术细节请参考我们的技术白皮书。

我们一方面将研发 MTTP 协议，将其开源给社区，努力帮助现有的交易所转型；另一方面我们也会研发自己的交易所，其主要目的是验证 MTTP 协议可以落地应用。如果现有的中心化交易所不愿意转型到 MTTP 协议上做去中心化撮合，我们将寻求伙伴一起商业化运作一个 MTTP 交易所，与现有交易所形成竞争关系，逼迫它们转型。

4 MTTP 代币的价值和投资潜力

5 团队、研发计划

由于这部分信息更新频繁，请参考我们的网站 http://mttp.io。