数字货币的交易模式

现阶段数字货币更像一种投资产品，因为缺乏强有力的担保机构维护其价格的稳定，其作为[价值尺度](https://baike.baidu.com/item/%E4%BB%B7%E5%80%BC%E5%B0%BA%E5%BA%A6/9635023)的作用还未显现，无法充当[支付手段](https://baike.baidu.com/item/%E6%94%AF%E4%BB%98%E6%89%8B%E6%AE%B5/9634849)。数字货币作为投资产品，其发展离不开交易平台、运营公司和投资。

交易平台起到交易代理的作用，部分则充当[做市商](https://baike.baidu.com/item/%E5%81%9A%E5%B8%82%E5%95%86/268436)，这些交易平台的盈利来源于投资者交易或提现时的手续费用和持有数字货币带来的溢价收入。[交易量](https://baike.baidu.com/item/%E4%BA%A4%E6%98%93%E9%87%8F/4533839)较大的平台有 Bitstamp、Gathub、Ripple Singapore、SnapSwap 以及昔日[比特币](https://baike.baidu.com/item/%E6%AF%94%E7%89%B9%E5%B8%81/4143690)交易最大平台日本[Mt.Gox](https://baike.baidu.com/item/Mt.Gox/3611884)和中国新秀瑞狐等。

数字货币通过平台进行交易的流程如下:

(1) 投资者首先要注册账户，同时获得数字货币账户和[美元](https://baike.baidu.com/item/%E7%BE%8E%E5%85%83/484146)或者其他[外汇账户](https://baike.baidu.com/item/%E5%A4%96%E6%B1%87%E8%B4%A6%E6%88%B7/3045654)。

(2) 用户可以用[现金账户](https://baike.baidu.com/item/%E7%8E%B0%E9%87%91%E8%B4%A6%E6%88%B7/18219963)中的钱买卖数字货币，就像买卖股票和期货一样。

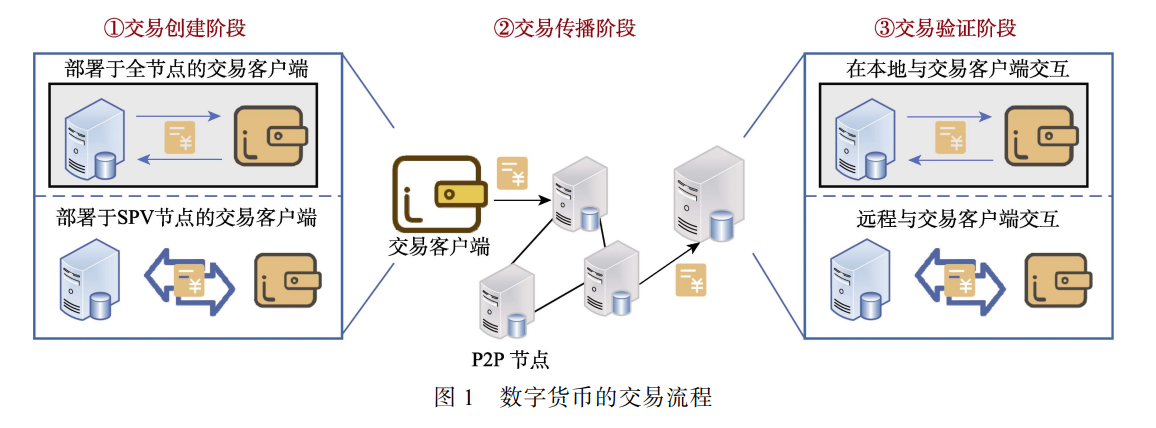
(3) 交易平台会将买入请求和卖出请求按照规则进行排序后开始匹配，如果符合要求即成交。

(4) 由于用户提交买入卖出量之间的差异，一个买入或卖出请求可能部分被执行。

数字货币通过运营公司交易的模式为: 以[瑞波币](https://baike.baidu.com/item/%E7%91%9E%E6%B3%A2%E5%B8%81/4956309)为例，瑞波币由专业运营公司OpenCoin 运营，[Ripple](https://baike.baidu.com/item/Ripple/6901044) 协议最初是基于支付手段设计的，设计思路是基于熟人关系网和信任链。要使用 Ripple 网络进行汇款或借贷，前提是在网络中收款人与付款人必须是朋友( 互相建立了[信任关系](https://baike.baidu.com/item/%E4%BF%A1%E4%BB%BB%E5%85%B3%E7%B3%BB/8757233)) ，或者有共同的朋友( 经过朋友的传递形成信任链) ，否则无法在该用户与其他用户之间建立信任链，转账无法进行。

例子：基于区块链的数字货币系统

与传统的中心化支付系统不同，基于区块链的数字货币系统是无中心的，它允许交易双方在没有第三方参与的前提下完成交易，而交易记录则会以区块的形式存储在所有参与者可见的公开账本中。这里我们将用户利用数字货币进行交易的过程分为三个阶段：交易创建阶段、网络传播阶段和交易验证阶段，交易流程如图 1所示。



交易创建阶段：

交易发送方通过交易客户端与P2P节点进行交互。通过交易客户端，用户可以管理个人的私/公钥和交易地址，还可以查看和花费个人钱包中的可用资金，并能 够进一步的生成数字货币的交易。当前市面上有许多数字货币的交易客户端，例如 BitcoinJ、imToken、Binance 等。当用户发起交易时，交易客户端创建密钥对，交易发送方在利用密钥对交易进行签名之后，会通过P2P节点广播至区块链网络。

交易传播阶段：

该阶段主要表现为交易在P2P节点之间进行传播。数字货币使用P2P网络来传播交易信息。交易信息在 P2P 网络中的传播主要包括两个过程：节点路由和交易传播。节点路由即一个新的P2P节点加入数字货币网络时，发现网络中的其他节点并建立连接的过程。交易传播即一条验证过的交易在区块链网络中按照一定的 规则进行传播的过程。

需要注意的是，当节点接收到一笔新交易时，会将该交易信息发送给所有的邻居节点，并保留消息转发记录，以保证交易信息仅向每个邻居节点转发一次。每个 P2P 节点将收到的所有交易保存在一 个内存池中，当接收到一笔新交易时，节点会将接收到的交易哈希与内存池或区块链账本中的哈希值进行比对，若哈希值相同，则拒绝接收该交易。

交易验证阶段：

该阶段主要表现为P2P节点与交易接收方之间的交互。区块链网络中的记账节点会收集所有尚未被记入账本的交易，并对交易进行排序打包生成区块。当记账节点创建一个区块并获得记账权，就会向区块链网络中的其他节点进行广播，这样具有记账功能的节点就会将其附在内部维护的区块链上。

此时，交易接收方便可确认自己的货币所有权，完成交易。具体而言，交易用户利用交易客户端访问P2P网络节点，通过存储于节点中的区块链账本中再通过识别他们的交易地址或假名来确认货币所有权。