**如何用区块链构建一个价值流通网络**

[**区块链**](http://blockchaindev.org/tags/区块链/)

作者：文浩  
链接：http://zhuanlan.zhihu.com/p/20766024  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

我的博客中有一篇译文《[货币的一种互联网体系架构--blockchaindev.org](https://link.zhihu.com/?target=http%3A//blockchaindev.org/article/An_architecture_for_the_Internet_of_Money2.html" \t "_blank)》，深入分析了在多种金融活动中如何建立一个分层的价值流通网络，今天我打算来谈谈这件事情。

本文打算探讨六个问题：

1. 区块链的简化模型是什么？
2. 区块链解决了什么问题以及没有解决什么问题？
3. 区块链应用场景的分布问题。
4. 区块链交易所是什么？
5. 什么是数字资产以及数字资产为什么重要。
6. 谈谈可能的技术架构。

**1. 区块链的简化模型是是什么？**

之所以要谈这个问题，是因为还有很多人对区块链是一个模糊的概念，所以想让更多的人有更直观的理解。现在考虑一下情形：

想象有一个100台的分布式数据库集群：  
场景一：这100个节点实际上的拥有者是一个机构，并且所有节点处在该机构的**内网**当中，所以这个机构想让这100个数据库节点干嘛就干嘛，换句话说这**100个节点之间**是处于一个**可信任**的环境，并且受控于一个实体，这个实体具有**绝对仲裁分配权**。  
场景二：想象这100个节点分别归不同的人所有，且每个人的节点数据都是一样的，即完全冗余，并且所有的节点是处在**广域网**当中，换句话说就是这100个**节点之间是不信任**的，且不存在一个实体，它拥有绝对仲裁权。  
现在考虑场景二，采用什么样的算法（**共识模型**）能够提供一个可信任的环境，使：  
每个节点交换数据过程不被篡改；  
交换历史记录不可被篡改；  
每个节点的数据会同步到最新数据，且承认经过共识的最新数据；  
基于少数服从多数的原则，整体节点维护的数据本身客观反映了交换历史。  
  
以上为背景，  
现在来谈谈区块链，区块链本质上就是要解决以上场景二的一种技术方案，更确切的说应该叫分布式的冗余的链式总帐本方案。  
只要包含了以：  
一种P2P的角度，链式的，只维护一本总帐的，能解决以上问题的技术方案，称之为区块链技术方案。

以上情况可以理解为区块链的一种简化模型。

现在我们来总结一下区块链的核心要素有3个：

1. **数据**
2. **数据认证**
3. **共识模型**

数据是广义的，泛指任何数据，也就是说区块链不仅仅可以用作金融活动上，只要任意场景需要强共识、强认证，则都是适用的。

数据认证，这个是指数据的所有权认证，对应到比特币上就是指公私钥验证这块，当然任何可以达成这种有效认证的方案，我们都是认可的。

在以上，数据和数据认证结合在一起，就可以变成一个终端数据库，即上面所述的场景二下的数据库。那么这个终端对应到金融活动中，表达了一种普适的概念，即资产数字化的概念，这个我们留在后文讨论。

共识模型，这是很有意思的一个东西，也是比较复杂的一块，对于刚刚接触区块链或者比特币的人会一直转到挖矿这些概念里出不来。其实抽象一下还是很好理解的，**泛指任何将无序的混乱数据变成可信任的共享数据（账本）的过程**，挖矿是针对完全开放场景的一种解决方案。有时候我们也会称共识模型为共识协议。

**2. 区块链解决了什么问题以及没有解决什么问题？**

区块链只解决了记账的问题，并没有解决供需信息配对的问题。

即区块链只解决了资产有效交割的问题，可以理解为保证交易发生后的情形，可是你要和谁交易呢？供需关系没有展现出来。

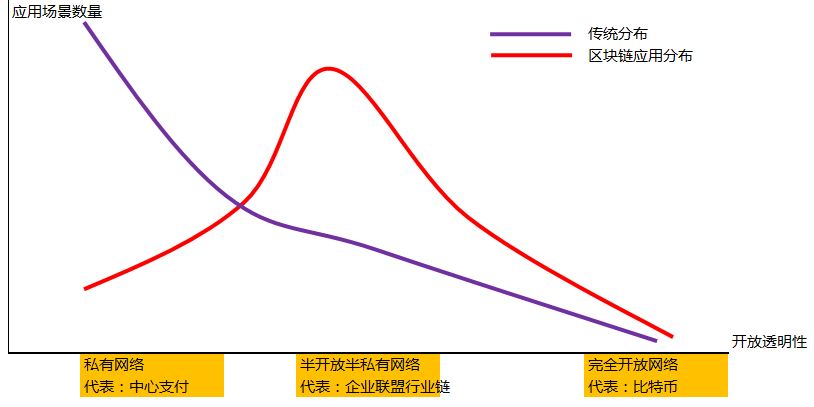
所以单纯依赖区块链并不能构建一个高效率的价值流通网络，那么这就轮到交易所出场了。

这里交易所的功能与传统交易所类似，只做一件事情：构建一个撮合市场，提供流通性。

**3. 区块链应用场景的分布问题。**

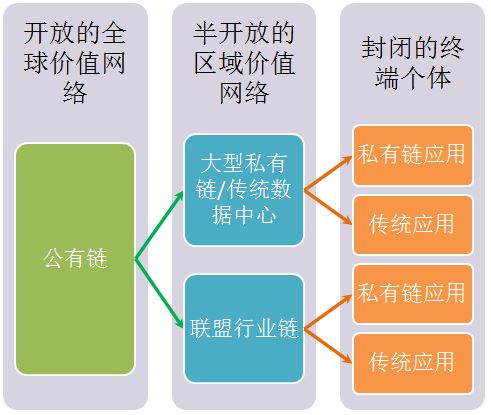
价值流通网络分为私有网络，半开放半私有网络，完全开放网络，对应到区块链上正好是私有/联盟/公有区块链，

我这有一个概览图，未做调研，可能不准，后期会做一些数据调研作为补充。

  
紫色线表示当前互联网中价值流通网络的应用数量，典型如X付宝，X信支付，X联。

红色表示了区块链在未来可能达到的应用场景分布状况，即价值流通网络的开放透明性整体前移。

下图是我早期构想的一张组织关系图：

  
即，在未来的价值流通网络中，我们可选的方案是有很多种的，如传统的中心化支付，企业之间的联盟支付，个人的公有链钱包等等。在终端应用方面，可以根据个人的能力和喜好选择对应的网络，即终端应用应当是可移植的，兼容型应用。

**4.区块链交易所是什么？**

区块链交易所是这样一个撮合交易平台：

a.兼容了传统撮合规则撮合引擎

b.资金托管和交割方式替换为区块链

这样一个区块链交易所可以解决区块链没有解决的问题，即供需信息发布和流动性的问题。

**5. 什么是数字资产以及数字资产为什么重要。**

在《[当我们在谈论区块链的时候，我们到底在谈论什么？](http://zhuanlan.zhihu.com/p/20716891)》文章里，我谈到了区块链世界的三个必要元素：

* 数字资产
* 智能合约
* 共识模型

数字资产类比数据结构，智能合约类比软件算法，共识模型类比软件架构，有了这三个要素，最终生产区块链的实体：**可信共享的总账本**。（智能合约可能是非必须的，但这样的区块链也是弱化的）。

学过编程的人，应该都了解数据结构的重要性，数字资产也是类似的概念：

在区块链的世界里，数字资产是被操作的实体，是有效的被认证的实体，如果没有资产的概念，那么区块链只能做公证服务了，并不能传递价值。

比特币采取了“挖矿”方式定义了数字化货币。

那么比特币也好，以太坊也好，还是其他区块链服务，本质上都可以看成是一种资产，既然是资产，为什么不可以数字化，听说过资产证券化的概念么？

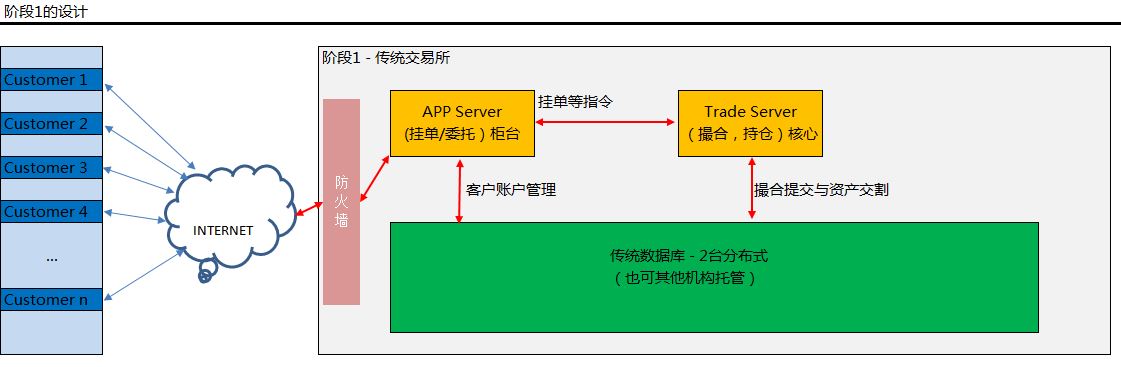
无论R3 CEV，还是Hyperledger，他们无论用什么样的分布式账本，终究都要定义分布式账本所存储的有效实体——数据+认证——**数字化资产**。

**6. 谈谈可能的技术架构**

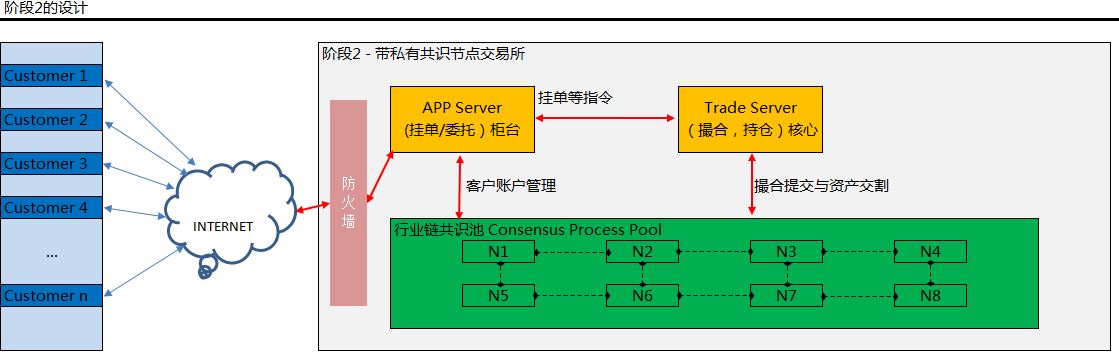
接下来我们谈谈如何架构一个区块链价值流通网络：

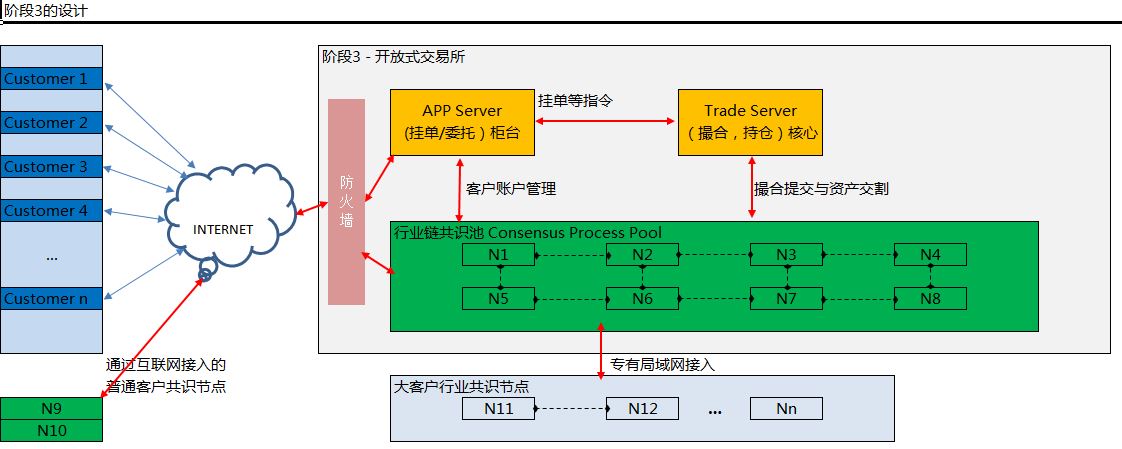
一共分3个阶段进行：

第一阶段：构建一个传统交易所。



第二阶段：使用私有区块链替换传统中心数据库。

  
第三阶段：开放区块链，让其他节点参与共识过程（监督与透明性），形成价值局域流通网络，如应用到供应链金融上。



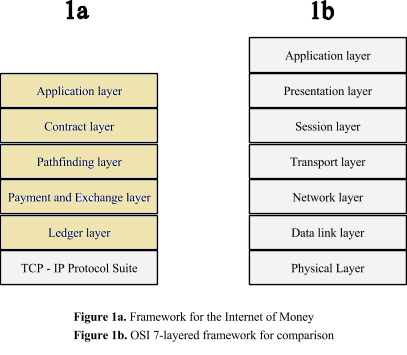
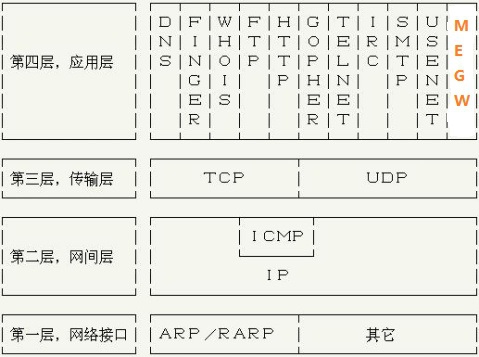
在第三阶段我们其实已经完成了如何构建一个**局域的**价值流通网络，那么我们还差一步。

还差什么？**像信息互联网一样的价值互联网！**

不过关于如何构建一个价值互联网，让价值像信息一样在互联网上高速流通，是一个很宏观的很伟大的命题，意义不亚于互联网的诞生，笔者这里这里只能展望一番：

1. 首先一定要构建一个**稳定强壮、低成本**的局域价值网络；
2. 其次要让局域价值网络渗透到完整的企业生命周期；
3. 再者推动企业形成自治联盟，通过这个企业联盟制定**价值交换网关协议**，可以是基于TCP/IP网际协议的，如在IP层的上面一层**。**

下图是HyperLedger设计者Meher Roy提出的一种方案，即在TCP/IP协议的上面构建一个基础协议。

  
笔者认为如果要构建一个价值交换网关，可以直接在TCP/IP协议的应用层增加一个交换协议，与HTTP/FTP等基础协议平行的协议，如下图：  


MEGW = Money Exchange Gateway = 价值交换网关协议。

至此所有局域网可以基于该协议进行互联，连接形成的价值互联网。