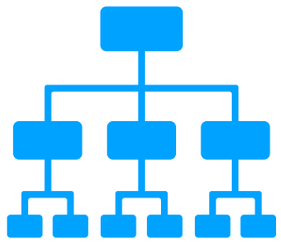
DAC技术白皮书

公链体系

共识体系

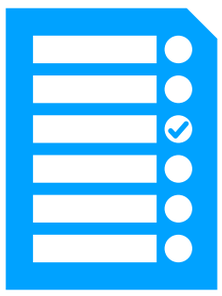
账户体系

公链体系



整体架构

- DAPP
- 交互/确权
- 侧链
- 公链



合约组构

- 主权合约
- 交互合约
- 逻辑合约

虚拟机

- 图灵完备
- 基于JS

公链体系-整体架构表述

整体架构由应用层、交互和确权、侧链和主链构成。其中应用层、侧链和主链是三个主体，交互和确权主要由通信协议和相关合约组成。这样应用层与侧链之间，侧链与主链之间通过协议和合约的形式进行关联，达到了模块化解耦的目的。各主体之间相对独立，保证了系统的安全性，兼容性和鲁棒性，是系统运行的更加稳健。创新的架构形式设计，既借鉴了经典互联网成熟的模式，又结合了区块链新技术的特点，使得侧链能够更好的作为一个桥梁或中转站，连接起应用和主链，发挥各自的优点特长。

应用通过URT形式的通信协议和侧链进行通信交互，暂且将协议称为合约，那么就有应用和侧链通过通信合约进行交互，通过通信合约可以调用逻辑合约，同时通过主权和约确立和侧链的权益关系。同理侧链也是通过以上机理与主链进行交互。

公链体系-整体架构-应用层与交互确权

应用层通过通信合约与侧链建立联系和交互，应用的一些共识逻辑通过逻辑合约实现，并存储在侧链上，最关键的一点也是创新点，应用通过主权和约确立自身与侧链的权益关系，从而应用自身变成数字价值。原则上为了减小主链的压力，应用是不能直接调用主链的逻辑合约的，但是应用可以通过侧链上的逻辑合约通过侧链与主链间的通信合约调用主链的合约，合约之间可以继承与实现，包括侧链合约与主链合约，侧链合约与侧链合约间不能直接通信，可以采用在主链建立侧链间通信合约的形式实现。

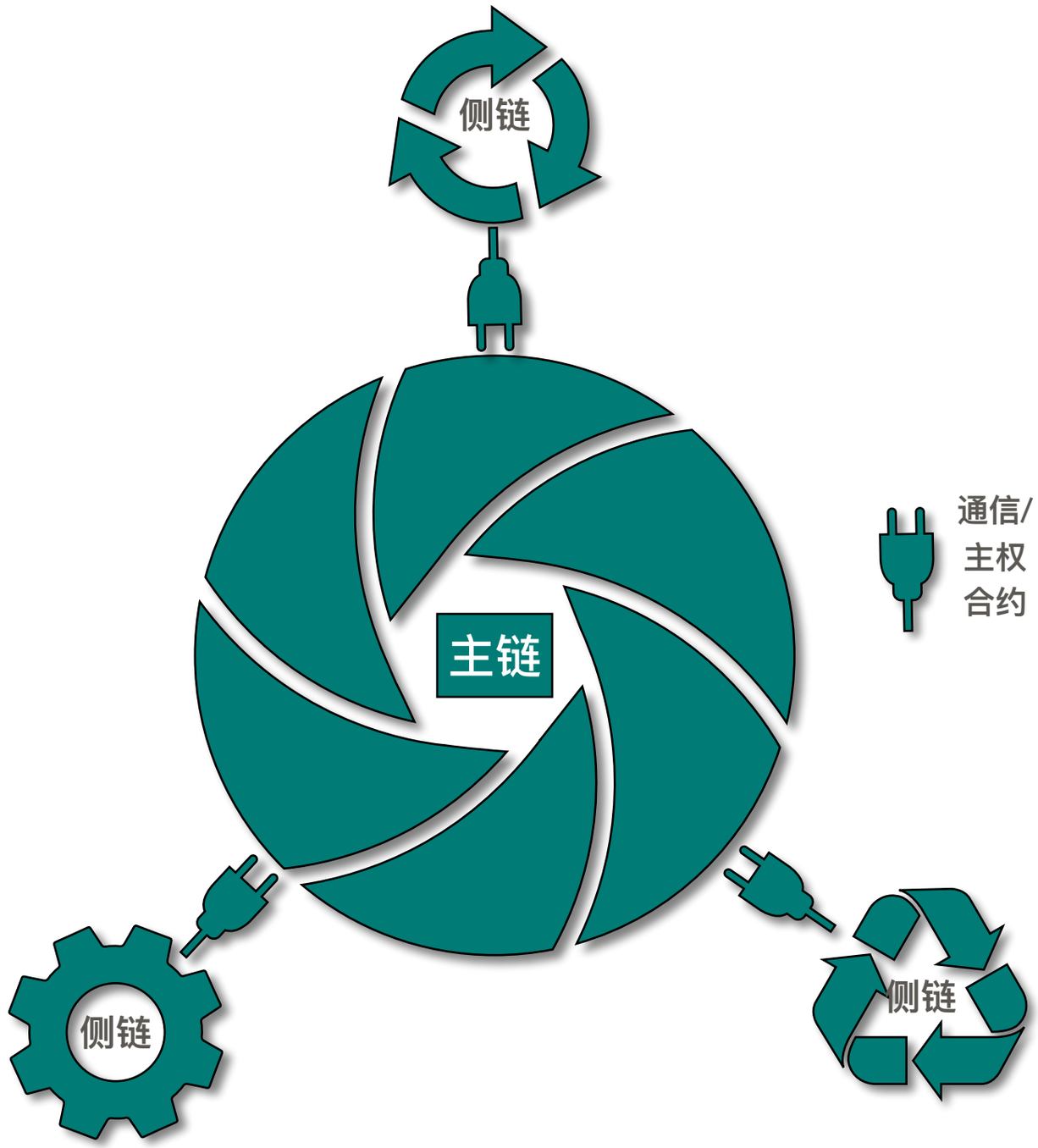
交互和确权是通过通信合约（协议）和主权合约的形式来体现的。通信合约本质是通信协议，由于应用和侧链可能是采用不同的语言可发，所以二者之间通信就需要采用一个合约形式的通信协议来规范双方的通信数据，每个应用一个通信合约，也可以共用一个通信合约合约。主权合约规定利益双方的利害关系和主体从属关系等方面的内容，以合约的形式展现和部署，防篡改。

公链体系-整体架构-侧链与主链

侧链概念的提出是出于解决目前公链普遍存在的拥堵问题，其原理是分流主链的流量，然后集中零散信息与主链交互达到缓解主链拥堵的目的。

我们选取主侧链机制也有这方面的考虑，此外我们赋予侧链更大的自主机制，侧链只是通过通信合约和主权合约与主链建立联系和确立关系，其余的由侧链自主决定，包括但不限于存储的数据，部署逻辑合约等等。

从另个一个方面讲侧链剔除掉与主链建立的合约关系，他就是一条公链。这样的架构选择和设计，除了保证了整个系统的安全性，兼容性等特征，更主要的一点是促进了主链和侧链各自的健康发展。



公链体系-合约组构

主权合约

主权合约规定应用与侧链，侧链与主链之间的权益关系。就像现实世界的合同一样，确立各自的法律权益关系。其确立了权益双方的合作关系。

交互合约

交互合约是应用与侧链，侧链与主链之间通信交互的规范，此外侧链之间是双方通信数据格式等方面的约定，其本质就是通信协议，像HTTP。

逻辑合约

逻辑合约主要是部署在侧链和主链上实现程序逻辑的合约。其和目前其他公链上的合约功能基本一致。

我们的合约基于JS开发，后面逐渐支持其他的通用语言，像Java，go，C++。

公链体系-虚拟机

DAC虚拟机

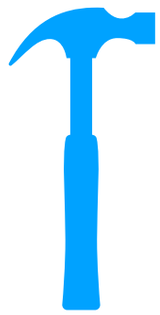
我们的虚拟机是基于JS开发，图灵完备。其可以在我们客户端运行，也可以像插件一样集成到相关的应用中，实现合约的相关逻辑。

共识体系

角色

机制原理

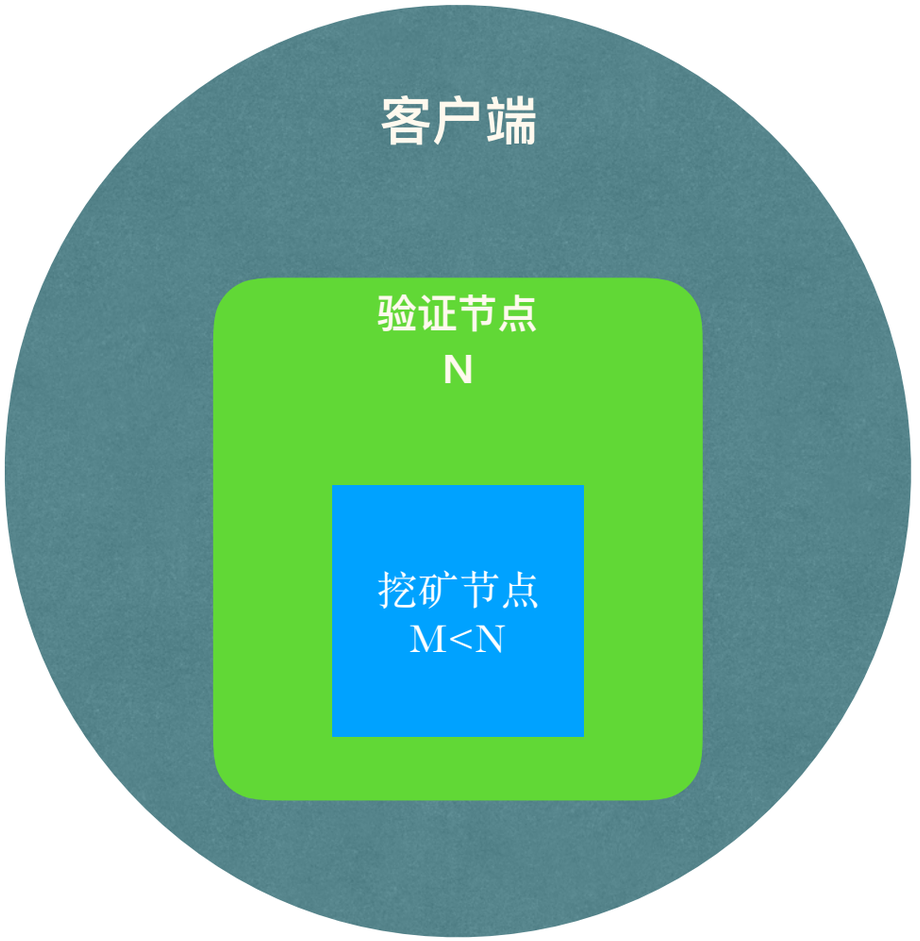
共识机制



挖矿规则

共识体系-角色

共识体系中主要由客户端、验证节点和挖矿节点三种角色组成。



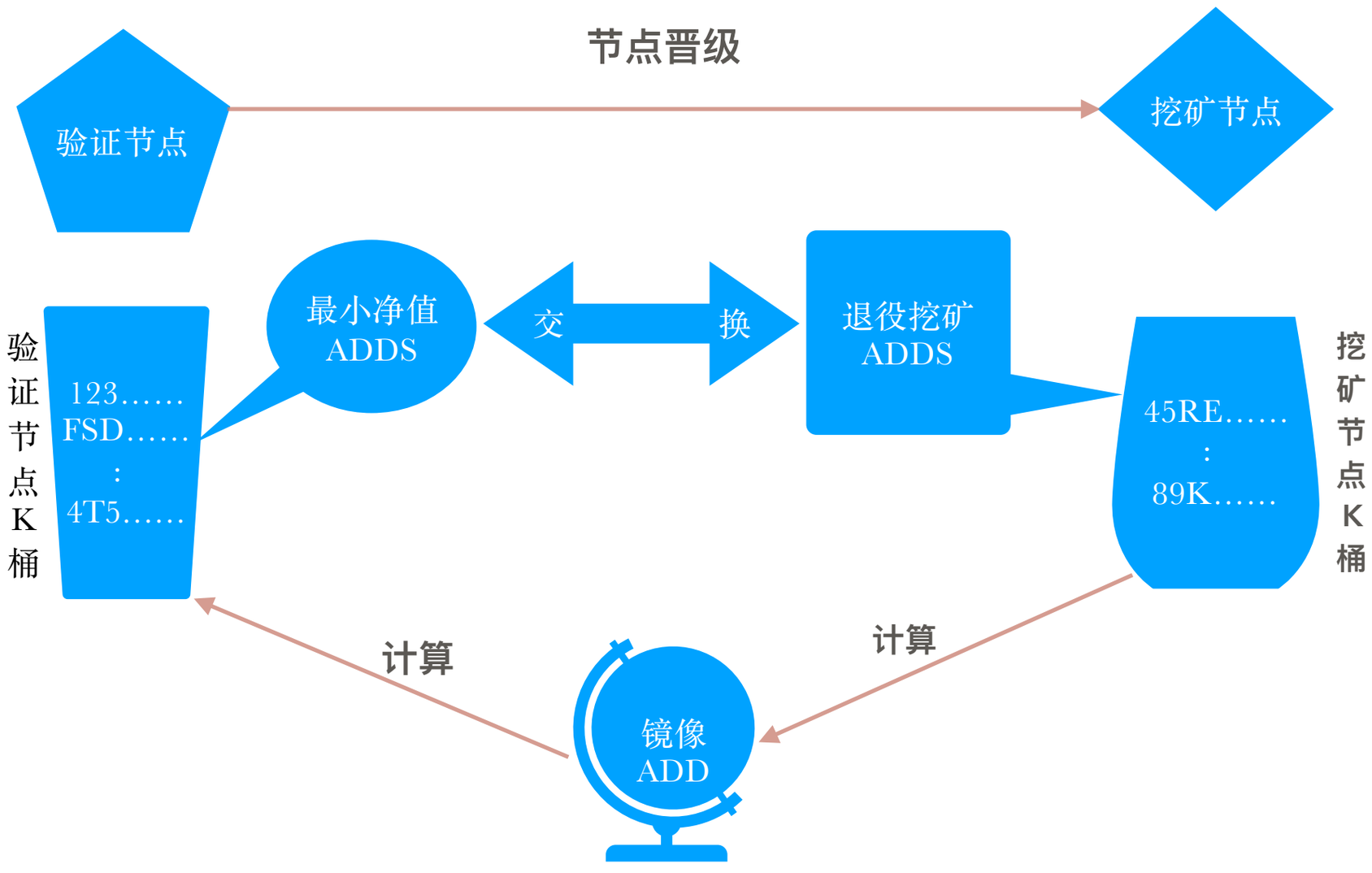
共识体系-共识机制

目前主链界现有的共识机制主要分为POW系，POS系和Delegate系，这三个系列后来者都在一定的程度上解决了前者所暴露出来的问题，但是同时自身也出现了一些问题。算法不足，添加人为因素来弥补，这本身就和区块链去中心化的共识思想相违背。

我们共识机制采用了区别于以上三系的机制原理，最大化的采用算法来解决问题，使用公认的算法来实现公平，避免任何的人为因素参与。当然我们的共识机制也不是十全十美，但是我们会沿着这条路一直走下去，通过算法实现共识机制下生态的大同。

共识体系-机制原理

本共识机制的节点主要分为验证节点和挖矿节点两种节点，每个节点都会有一个全局唯一的哈希地址HAdd，验证节点地址组成的列表称为VK桶，挖矿节点地址组成的列表称为MK桶。验证节点负责对数据的验证，挖矿节点负责挖矿和更新挖矿节点。每个验证节点有一个辈分值和工作量值，符合一定阈值的验证节点通过HANP (Hierarchical Addressable Network Promoted)层次形寻址网络晋级算法来成为挖矿节点候选人节点。同时MK桶会定时退役若干挖矿节点RtADD，然后候选人节点接替RtADD进行挖矿。然后MK桶中挖矿节点采用基于哈希地址最小值胜出挖矿共识。



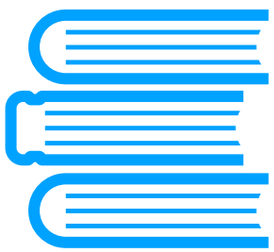
共识体系-挖矿规则

验证节点不获得激励，验证节点的工作是为了获得备份和工作量的积累，这类似于学徒工，在学徒工自己没有证明自己有能力独当一面的时候，智能无偿给师傅打工；挖矿节点具有激励的回报，但是为了挖矿节点不是一成不变的，挖矿节点如果被退役机制选中，就会被新晋级的验证节点代替，而自己就会退役为验证节点，等待下次被选为挖矿节点的机会。

挖矿节点推导公式：**Min(SHA（PreBlockHash+△time）& Mkadds)**。

账户体系

账户概述



账户组构

账户体系-账户概述

账户概述

区块链传统账户的含义主要是以比特币账户公钥-私钥对为基础拓展而来，由于以太坊支持智能合约在比特币的基础上添加了合约账户，而我们的账户是建立在我们的公链体系上，结合我们的架构特点，除了智能合约外我们的账户中添加了权益的相关内容，这样我们的账户体系可以更好的支持和融入我们的公链架构体系之中。

账户体系-账户组构

权益账户

生命本账户的权益等相关内容。

数字账户

存储账户的数字余额，公钥和私钥，发起交易等。

合约账户

用于合约的相关操作，像调用，执行等