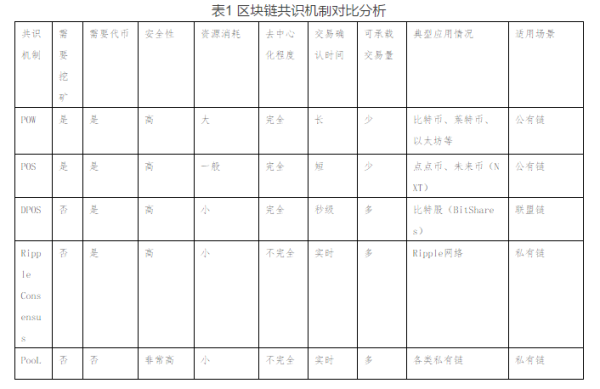
## ****区块链共识机制****

常见的共识机制有POW工作量证明、POS权益证明、DPOS股份授权证明、Ripple共识机制以及PooL验证池



* **POW（Proof of work）**

POW即工作量证明，就是众所周知的挖矿，它是一种竞争共识，通过工作量的证明来获得生成区块的权力。

它的优点是完全的去中心化，各个节点完全平等，而且可以自由的进出；缺点则是POW会造成大量的挖矿资源浪费，达成共识的周期也比较长。

* **POS（Proof of Stake）**

POS即权益证明，是POW的一种升级共识机制，它主要解决了POW工作量计算浪费的问题。当前POS已有很多不同的变种，但基本还是根据每个节点所占有代币的数量和时间（即权益）来决定其挖矿的难度。

它的优点是缩短了各个节点之间达成共识的时间，缺点则是同POW一样仍然需要挖矿，并且POS会使得“富者更富”。

* **DPOS（Delegate Proof of Stake）**

DPOS即股份授权证明机制，是POS的一个变种。它的原理是让每个持有代币的人进行投票，由此产生一定数量的“超级节点”，由这些节点来轮流产生区块。

它的优点是不再需要通过挖矿来产生区块，从而可以大幅缩小交易确认的时间，能够达到秒级的共识验证，缺点则是DPOS还是得依赖于代币，不适用于一般的商业应用。

* **Ripple Consensus（瑞波共识机制）**

Ripple Consensus是一种数据正确性优先的网络交易同步机制，它是基于特殊节点列表达成的共识。在这种共识机制下，必须首先确定若干个初始特殊节点，如果要新接入一个节点，必须获得51%的初始节点的确认，并且只能由被确认的节点产生区块。因此，它区别于前面几类共识机制的主要因素是有一定的“中心化”。

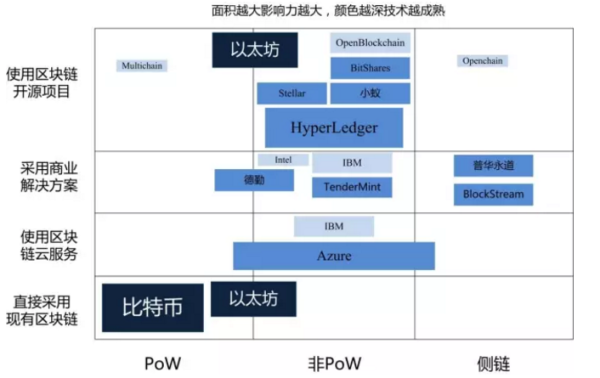
Ripple Consensus的优点是能保证任何时候都不会产生硬分叉，并且交易能被实时的验证；而缺点则是新加入节点要取得与其他节点的共识所需时间较长。

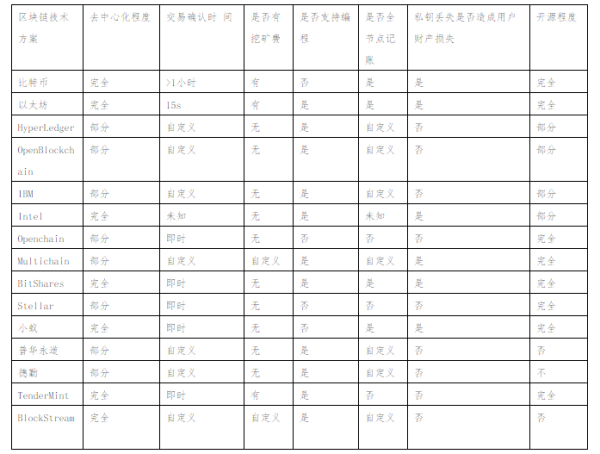
* **POOL验证池**

POOL验证池是基于传统分布式一致性算法加上数据验证的机制，也是目前行业链大范围在使用的共识机制。

它的优点是无需建立代币，在成熟的分布式一致性算法（Pasox、Raft）的基础上，能够实现实时共识验证；缺点是性能会随着节点数的增加而变差，并且去中心化程度不够。

## ****区块链技术方案分析****





### 1 比特币

比特币的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。

### 2 以太坊

以太坊是一个专注于智能合约应用的数字货币和区块链平台，它的去中心化技术使交易摆脱了停机和审查的麻烦，解决了传统合约的纠纷等棘手问题，并且还能避免欺诈和第三方的干扰。以太坊的目标就是提供一个带有内置的成熟的图灵完备语言的区块链，用这种语言可以创建合约来编码任意状态转换功能，用户只要简单地用几行代码来实现逻辑，就能够创建各种满足需求的系统。

从技术架构角度看，以太坊是一个与底层区块链和协议无关的通用分布式运用开发平台和编程语言，包括数字货币以太币（Ether）和以太脚本（EtherScript），用于构建和发布分布式应用。它具备开放通用的特性，且内置有图灵完备虚拟机，可以运用任何货币、协议和区块链。网络上的每一个节点都可以运行以太坊虚拟机来发布分布式智能合约程序。

以太坊有自己的分布式系统：包括文件服务Swarm、信息传输Whisper和信誉担保。Swarm是个去中心化文件服务；Whisper是加密通信传输系统；信用担保提供去信任网络中建立信誉和降低发现的系统，可以由第三方提供。

此外，以太坊本身也是开源软件，具备了开源项目的快速创新特性，通过代码共享让新的项目可以快速的迭代出符合市场需求的产品。目前，以太坊正被一些金融机构、银行财团（比如 R3），以及类似三星、Deloitte、RWE 和 IBM 这类的大公司所密切关注，由此也催生出了一批诸如简化和自动化金融交易、商户忠诚指数追踪、旨在实现电子交易去中心化的礼品卡等等区块链应用。

以太坊两年来得到了技术社区和商业机构的大力支持，发展迅速，未来很有可能会成为区块链领域最具竞争力的解决方案之一。

### 3 HyperLedger

Hyperledger是一个由Linux基金会管理的开源区块链项目, 由IBM、Intel、埃森哲、JP摩根等公司领衔参与。HyperLedger被定义为：负责协调多个客户端的服务数据和低层次的“沟通和共识层”，一个致力于提高全球金融基础设施的“数据骨干”。

Hyperledger利用了和比特币相同的UTXO/script 交易决策，并根据金融服务所需要的功能进行了扩展,HyperLedger提供了一种替代POW的共识机制，是一个带有可插拔各种功能模块架构的区块链实施方案，它的目标打造成一个由全身会来共同维护的一个超级账本。是允许将数据骨干理念扩展到多个组织层,作为全新金融基础设施的重要组成部分。