**区块链几大共识机制及优缺点**

首先，没有一种共识机制是完美无缺的，各共识机制都有其优缺点，有些共识机制是为解决一些特定的问题而生。

# POW( Proof of Work）工作量证明

一句话介绍：干的越多，收的越多。

依赖机器进行数学运算来获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网50%节点出错。

优点：

1)算法简单，容易实现；

2)节点间无需交换额外的信息即可达成共识；

3)破坏系统需要投入极大的成本；

缺点：

1)浪费能源；

2)区块的确认时间难以缩短；

3)新的区块链必须找到一种不同的散列算法，否则就会面临比特币的算力攻击；

4)容易产生分叉，需要等待多个确认；

5)永远没有最终性，需要检查点机制来弥补最终性；

# POS Proof of Stake，权益证明

一句话介绍：持有越多，获得越多。

主要思想是节点记账权的获得难度与节点持有的权益成反比，相对于PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和PoW相同。它是Pow的一种升级共识机制，根据每个节点所占代币的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度

优点：在一定程度上缩短了共识达成的时间；不再需要大量消耗能源挖矿。

缺点：还是需要挖矿，本质上没有解决商业应用的痛点；所有的确认都只是一个概率上的表达，而不是一个确定性的事情，理论上有可能存在其他攻击影响。例如，以太坊的DAO攻击事件造成以太坊硬分叉，而ETC由此事件出现，事实上证明了此次硬分叉的失败。

# DPOS Distributed POS

DPOS与POS原理相同，只是选了一些“人大代表”。

BitShares社区首先提出了DPoS机制。

与PoS的主要区别在于节点选举若干代理人，由代理人验证和记账。其合规监管、性能、资源消耗和容错性与PoS相似。类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。

DPoS的工作原理为：

去中心化表示每个股东按其持股比例拥有影响力，51%股东投票的结果将是不可逆且有约束力的。其挑战是通过及时而高效的方法达到51%批准。为达到这个目标，每个股东可以将其投票权授予一名代表。获票数最多的前100位代表按既定时间表轮流产生区块。每名代表分配到一个时间段来生产区块。所有的代表将收到等同于一个平均水平的区块所含交易费的10%作为报酬。如果一个平均水平的区块含有100股作为交易费，一名代表将获得1股作为报酬。

网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。然而，这不太可能发生，因为制造区块的代表可以与制造前后区块的代表建立直接连接。建立这种与你之后的代表(也许也包括其后的那名代表)的直接连接是为了确保你能得到报酬。

该模式可以每30秒产生一个新区块，并且在正常的网络条件下区块链分叉的可能性极其小，即使发生也可以在几分钟内得到解决。

成为代表：

成为一名代表，你必须在网络上注册你的公钥，然后分配到一个32位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。

授权选票：

每个钱包有一个参数设置窗口，在该窗口里用户可以选择一个或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建特别以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。

保持代表诚实：

每个钱包将显示一个状态指示器，让用户知道他们的代表表现如何。如果他们错过了太多的区块，那么系统将会推荐用户去换一个新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个钱包进行更多交易前要求选出一个新代表。

抵抗攻击：

在抵抗攻击上，因为前100名代表所获得的权力权是相同的，每名代表都有一份相等的投票权。因此，无法通过获得超过1%的选票而将权力集中到一个单一代表上。因为只有100名代表，可以想象一个攻击者对每名轮到生产区块的代表依次进行拒绝服务攻击。幸运的是，由于事实上每名代表的标识是其公钥而非IP地址，这种特定攻击的威胁很容易被减轻。这将使确定DDOS攻击目标更为困难。而代表之间的潜在直接连接，将使妨碍他们生产区块变得更为困难。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

缺点：整个共识机制还是依赖于代币，很多商业应用是不需要代币存在的。

# PBFT ：Practical Byzantine Fault Tolerance，实用拜占庭容错

介绍：在保证活性和安全性（liveness & safety）的前提下提供了(n-1)/3的容错性。

在分布式计算上，不同的计算机透过讯息交换，尝试达成共识；但有时候，系统上协调计算机（Coordinator / Commander）或成员计算机 （Member /Lieutanent）可能因系统错误并交换错的讯息，导致影响最终的系统一致性。

拜占庭将军问题就根据错误计算机的数量，寻找可能的解决办法，这无法找到一个绝对的答案，但只可以用来验证一个机制的有效程度。

而拜占庭问题的可能解决方法为：

在 N ≥ 3F + 1 的情况下一致性是可能解决。其中，N为计算机总数，F为有问题计算机总数。信息在计算机间互相交换后，各计算机列出所有得到的信息，以大多数的结果作为解决办法。

1）系统运转可以脱离币的存在，pbft算法共识各节点由业务的参与方或者监管方组成，安全性与稳定性由业务相关方保证。

2）共识的时延大约在2~5秒钟，基本达到商用实时处理的要求。

3）共识效率高，可满足高频交易量的需求。

1)当有1/3或以上记账人停止工作后，系统将无法提供服务；

2)当有1/3或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据

下面说两个国产的吧~

# dBFT：delegated BFT 授权拜占庭容错算法

介绍：小蚁采用的dBFT机制，是由权益来选出记账人，然后记账人之间通过拜占庭容错算法来达成共识。

此算法在PBFT基础上进行了以下改进：

将C/S架构的请求响应模式，改进为适合P2P网络的对等节点模式；

将静态的共识参与节点改进为可动态进入、退出的动态共识参与节点；

为共识参与节点的产生设计了一套基于持有权益比例的投票机制，通过投票决定共识参与节点（记账节点）；

在区块链中引入数字证书，解决了投票中对记账节点真实身份的认证问题。

1)专业化的记账人；

2)可以容忍任何类型的错误；

3)记账由多人协同完成，每一个区块都有最终性，不会分叉；

4)算法的可靠性有严格的数学证明；

2)当有1/3或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据；

以上总结来说，dBFT机制最核心的一点，就是最大限度地确保系统的最终性，使区块链能够适用于真正的金融应用场景。

# POOL验证池

基于传统的分布式一致性技术，加上数据验证机制。

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证。

缺点：去中心化程度不如bictoin；更适合多方参与的多中心商业模式。

# RBFT：Randomized BFT 随机拜占庭容错

标准的，最终同步BFT协议，如PBFT的理想替代方案

随机BFT协议通过以非常高而非确定性的概率保证正确性，规避了FLP共识的不可能性结果。RBFT协议允许完全异步，伴随的是性能问题。

与最终同步、确定性的BFT协议相比，经典RBFT协议效率不高，主要原味是加密工具的开销大。但是心的RBFT协议可能会改变这一情况，例如HoneyBadger通过选用最合适的加密工具，在100个节点的情况下用于随机化和处理大批量请求时，具有良好的性能。

大批量请求的延迟产生负面影响，但是这可以通过高效和确定性的BFT协议结合PBFT的Hybird BFT协议解决，例如HoneyBadger。这种混合BFT协议有早期例子，但未来HybirdBFT协议通过使用模块化BTF设计框架来改进。

# PoA（Proof of Authority）：权威证明

我们可以建立一套完善的航空飞行规则，所有航班的飞行员都经过严格的审查，他们都有着自己的身份证明以及飞行员资格认证，并且遵循着相同的规则来飞行。这样的话我们解决了安全问题，保证每架飞机都安全地为我们运送更多的旅客。这边是PoA（Proof of Authority）的核心思想。

所谓权威证明（PoA），就是使用一组所谓的“权限” 来允许人们在区块链上创建新的节点并确保区块链的安全。以太坊测试网（Kovan）便是采用PoA算法。

在PoA中，验证者（validator）是整个共识机制的关键。验证者不需要昂贵的显卡，也不需要足够的资产，但他必须具有已知的，并且已获得验证的身份。验证者通过放置这个身份来获得担保网络的权利，从而换取区块奖励。若是验证者在整个过程中有恶意行为，或与其他验证者勾结。那通过链上管理可以移除和替换恶意行为者。现有的法律反欺诈保障会被用于整个网络的参与者免受验证者的恶意行为。

**POA 网络（POA Network）：**

好了，终于到了我们的正题，什么是POA网络？ POA网络便是建立在PoA共识之上的底层区块链。在POA网络中，每个验证者（validator）都必须在美国境内拥有公证许可。人们需要通过POA网络身份DApps进行身份验证，包括住址证明和无犯罪记录证明等。然后进行所谓的启动仪式（initiation ceremony）来获得密钥。通过的验证者便可以担当起保护网络的安全的重任，并获得回报。 POA网络作为一个底层链，其上的每一个新的专用链都可以使用相同的验证器，或者拥有自己的一套验证器以及其他任何类型的可验证许可证。



通俗的理解就是，以前我们交易需要一群互不认识的人来拼算力，艰难的计算一道复杂的数学题，从而争出个输赢。而现在，我们只需要有一个信得过的人（至少得到了他们团队的认可）做担保，便可快速通过交易。而这个人也会因为为这笔交易做担保，而获得报酬。要是这个担保人使坏怎么办？没关系，其他的可信担保人看着呢，他要是敢使坏，我踢你出局。而要是担保人故意为难你呢？没关系，现有的法律可以保证你的合法权益（注意，数字资产丢失不在我国法律保护范围）。

附上一个他们网络中一位验证者对PoA机制的视频介绍链接：[https://youtu.be/5RumGukS8pw](https://link.zhihu.com/?target=https%3A//youtu.be/5RumGukS8pw" \t "_blank)

最后还需要强调一下，POA网络除了共识机制以外，和以太坊网络完全一样。也就是说你在以太坊网络上想干的事都可以在POA网络上干，什么智能合约啦，发行新币啦，建立自己的DApps啦，都没有问题。

**如何评价POA网络：**

说了那么多，上面都是答非所问。现在来谈谈我对POA网络的看法。

POA网络确实是对以太坊网络现如今诸多不合理问题的一个解决方案。他相对于以太坊网络有很好的兼容，同时具有极大的优势。

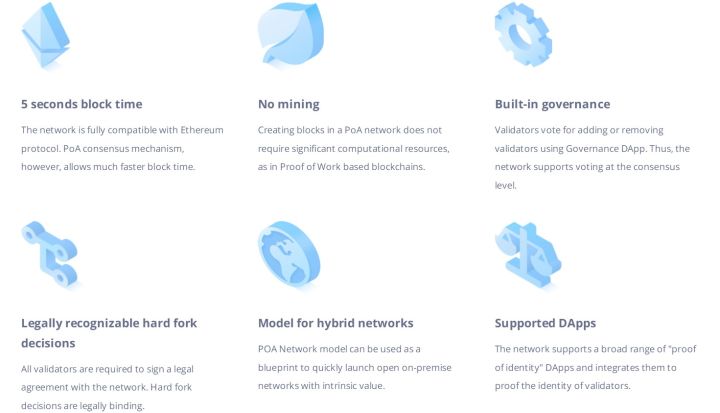
1. 官方宣称**5s**就能打包一个区块，而我们的大以太受阻塞时，可能一个小时后，你还收不到你的代币。

2. 不需要挖矿，节能环保

3. 整个网络，验证者互相监督，随时可以投票加入新的验证者或者剔出不合格验证者

4. 所有的验证者都跟网络签署了协议，若谁要想在POA上弄个新的分叉出来（POC？），那不行，这是要走基本法的

5. 高度可扩展性和高度兼容性，智能合约也信手拈来，让其成为优化的ETH  
2.0



优点固然多，解决方案也巧妙。但是不知道大家有没有和我同样的疑问，这样的机制还是一个去中心的网络吗？在智能合约作为信任的基础上，POA网络将人与人由合约建立其的信任，转变成人与人对网络中验证者的信任。而将对验证者的信任，转变成对那些对验证者身份进行审核的人的信任。最终转变的结果是，**我相信你们选出来的验证者绝大多数都是好人，且这之中大多数人互相不认识，不会串通起来为所欲为**。解决区块链问题往往难以得到两全，有时候获得速度，可能就要丧失一些安全。这个“两全之策”背后，确无法让我停下思考，这样的网络真的安全吗？这样的网络真的可以托付起未来区块链改变互联网的重任吗？

# POA Proof of Application

无