PoS适用于公有链。

3。区块签名者如何发生

在PoS机制下，由于区块的签名者是随机产生的，一些持币者会临时大量持有代币，以获得更有可能发生的区块，从而清除自己的&quot货币天数&quot尽可能多。。所以全网停滞代币会增加，有利于代币在链上的停滞，价格会更加复杂坚挺。因为少数大户可以持有全网大量代币，所以随着运行时间的增加，全网会越来越趋于集中。。与PoW相比，PoS机制下的恶息很低，需要更多的机制来保证对分叉或重复支付的攻击达成共识。在固定条件下，每秒钟大约可以发生12次交易，但由于网络延迟和共识效应，完全广播共识块大约需要60秒。目前，生成块的速度(即清除&quot货币天数&quot)远低于网络通信和广播的速度，因此有必要停止&quot速度限制&quot在PoS机制下生成块，以确保主网络的抖动操作。

4。素描理解法

(PS:越有&quot股份&quot权限，获取账号权限越复杂。意思是你拿多少钱取决于你对采矿贡献的工作量。电脑功能越好，给你的矿就越多。)

(在纯POS系统中，比如NXT，没有挖矿过程，初始股权分配一直活跃，然后只有股权在交易者之间流动，这和梦幻世界的股票很像。)

(3)DPoS(委托股权证明)份额授权认证机制

1。基本介绍

由于PoS的种种弊端，Bitshares开创的DPoS(委托股权证明)应运而生。DPoS机制的核心要素是选举，以及每个制度的持有者&#039；美国本土代币可以参加区块链以外的选举。持有的代币余额就是投票权重。经过投票，股东可以选举董事会成员，也可以就联络平台的发展方向等话题表明态度，这些都构成了社区自治的基础。除了投票选举外，股东你也可以通过授权你自己的选举人票给你怀疑的其他账户来代表你投票。

详细来说，DPoS是Bitshares项目组发明的。股权有权利选出他们的代表来阻止区块的生成和考证。。DPoS类似于现代企业董事会制度。Bitstock系统是指代币持有者作为股东，由股东选举101名代表，然后这些代表负责生成和考证区块。如果持有者想要成为代表，他需要首先用他的公钥向区块链注册。，得到一个长度为32位

的唯一身份标识符，股东可以通过交易停止对该标识符的投票，票数前101名当选代表。

代表轮流挡，收益(交易费)平分。。DPoS的优势在于大大增加了参与区块考证和簿记的节点数量，从而缩短了共识验证所需的时间，大大提高了交易效率。从某种角度来说，DPoS可以理解为一个多中心系统，既有分散的优势，也有集中的优势。。优点：参与验证和核算的节点数量大大增加，可以实现秒级共识验证。缺点：投票自动化程度不高，大部分代币持有者没有参与投票；另外，整个共识机制还是要靠令牌，很多商业用途都不需要令牌。

DPOS机制要求在下一个块出现之前，必须验证前一个块是否由可疑节点签名。与&quot国家矿业公司&quot对于PoS，DPoS使用类似于&quot国会&quot直接选择可疑的心脏节点。这些可疑的心节点(即见证人)代替其他持币人行使权益，见证人节点请求暂时在线，从而解决了PoS签人经常不在线可能带来的阻塞延迟等一系列成果。DPoS机制一般可以达到每秒一万次的事务速度。在网络延迟较低的情况下，可以达到10万秒的水平，非常适合企业使用。DPoS是一个非常好的选择，因为工信宝数据交换需要高频率的数据交易和临时的摇摆不定。

2。股份授权机制下的机构和制度

董事会是区块链网络的权益机构。董事会的候选人由系统的股东(也就是钱的持有者)选举产生，董事会成员有权发起提案和停止对提案的表决。

董事会的主要职责之一是根据需要调整系统的可变参数，包括：

l费用相关：各种交易类型的费率。

l授权相关：对接入网络的第三方平台进行收费和补贴相关参数。

l挡位消耗关联：挡位消耗距离和时间，挡位奖励。

l身份审核相关：审核非机构账户信息。

l与此同时，涉及理事会利益的事项，理事会不予设定。

在Finchain系统中，见证方负责收集网络运行过程中广播的各类交易，并打包成块。他的工作类似于比特币网络中的矿工。在使用PoW(工作量证明)的比特币网络中，获胜概率取决于决定哪个挖掘器节点将生成下一个块的散列能力。在具有DPoS机制的金融链网络中，见证人的数量由董事会决定，见证人候选人由持有人决定。

。选出的鲜活的见证人，根据时代包装交易，消费区块。每一轮方块消费结束后，见证人会随机洗牌并决定新的次数，然后进入下一轮方块生产。

3。使用DPOS的例子

bitshares采用dpo。DPoS主要适用于联盟链。

4。草图理解表

(4)PBFT(实用拜占庭容错)适用于拜占庭容错算法

1。基本介绍

PBFT是一种基于苛刻数学证明的算法。需要经过三个阶段的消息交互和部分共识，才能达到最终的一致输入。这三个阶段分为前期准备、准备和提交。。PBFT算法证明，系统只需要上述文章内容的一般节点的2/3，就能保证最终输入一致的共识结果。换句话说，在使用PBFT算法的系统中，可以容忍系统中至少1/3数量的失效节点(包括故意误导、故意破坏系统、超时、重复发送消息、伪造签名等的节点。也称为&quot拜占庭&quot节点)。

2。PBFT

应用实例

知名联盟连锁HyperledgerFabricv0.6采用PBFT，v1.0引入SBFTPBFT的改良版。PBFT主要适用于私有连锁和联盟连锁。

3。草图理解表

上图为PBFT的简化协议通信形式，其中C为客户端，03为有效节点，0为主节点，3为缺陷节点。整个协议的基本流程如下：

(1)客户端发送抗辩。，激活主节点的业务操作；

(2)主节点收到请求后，发起三阶段协议，向从节点广播请求；

(a)在序列号分配阶段，主节点将序列号n分配给请求。广播客户端的序列号分配消息和请求消息m，并向每个从节点发送结构预准备消息；

(b)在交互阶段，从节点接收pre-prepare消息，并广播给其他服务节点；

(c)在序列号确认阶段，每个节点在视图中验证请求和顺序后，广播一个commit消息来实现从客户端接收到的请求，并为客户端处理它。

(3)客户端等待来自不同节点的关怀。如果有m1个引用是相同的，那么echo就是操作的结果；

(5)DBFT(授权拜占庭容错)授权拜占庭容错算法

1。基本介绍DBFT是以PBFT为原型的。在这个机制中，有两种参与者，一种是&quot超级节点&quot专业记账的，另一类是不参与系统记账的一般用户。一般用户根据自己的权益比例投票给超级节点。当需要通过一个共识(簿记)时，从这些超级节点中随机选出一个发言人拟定方案，然后其他超级节点按照拜占庭容错算法(见上)做出声明，即少数服从少数的准则。假设超过三分之二的超级节点赞同代言人计划。，达成了共识。该提议成为最终发布的块，并且该块是不可逆的，并且所有外部交易都是100%确认的。假设在一定时间内没有达成协议，如果发现合法交易，其他超级节点可以重新发起提议。重复投票过程，直到达成共识。

2。应用实例DBFT[XY002][XY001]NEO，国际加密货币和区块链平台，是DBFT算法的开发者和采用者。

3。草图理解表

假设系统中普通用户选出的超级节点只有四个，当需要通过一个共识时，系统会从代表中随机选出一个发言人拟定方案。发言人将把提议的方案交给每个代表。每个代表先区分发言者的计算结果与自己的记录是否一致，然后与其他代表讨论，验证计算结果是否准确。假设三分之二的代表同意议长的计算结果&#039；s方案准确，则该方案通过。

如果少于三分之二的代表达成共识，将随机选择新的发言人，并重复上述过程。这种集团制度旨在保护系统免受无法履行其职能的领导人的影响。

上图假设部分节点诚实，达成100%共识。将验证方案A(区块)。

由于发言人是随机抽取的代表，所以他可能不诚实，或者有缺点。上图假设说话人给三个代表中的两个发了恶意消息(方案B)。同时，向代表发送准确的信息(方案A)。

这种情况下，恶意信息(方案B)无法通过。中间和左边代表的计算结果与说话人发来的不一致，说话人拟定的方案无法验证。，导致两人拒绝通过该计划。因为左边的代表收到了正确的信息，与自己的计算结果一致，所以能够对方案进行确认，然后成功完成了一次验证。但是，这个计划仍然可以&#039；我不能通过，因为三分之二的代表达不到共识。然后会随机选出一个新的发言人。，重新结束共识过程。

上图假设演讲者很诚实，但其中一个代表很；左边的代表向其他代表发送了不正确的信息(b)。

在这种情况下，说话人拟定的正确信息(a)仍然可以被验证，因为左边和中间的诚实代表可以验证诚实说话人拟定的方案，并达成三分之二的共识。。代表也能分辨出说话人到底是骗了对节点还是对节点终究是不诚实的。

(6)SCP(恒星共识协议)恒星共识协议

1。基本介绍

SCP是Stellar(一种基于互联网的去中心化全球支付协议)开发和使用的共识算法，基于联邦拜占庭协议。。激进的非联邦拜占庭协议(如上面的PBFT和DBFT)当然保证可以通过火力分配方法达成共识，并且可以实现拜占庭容错(至少可以容忍系统中三分之一的本地节点数)。它是一个集中式系统-网络中节点的数量和身份必须预先知道和验证。联邦拜占庭协议和联邦拜占庭协议的区别在于可以去中心化，同时可以实现拜占庭容错。

[...]

(7)RPCA(Rippleprotocolconsistencyalgorithm)Rippleconsensusalgorithm

1.Basicintroduction

RPCA是Ripple(基于互联网的开源支付协议，可以完成去中心化的货币兑换、支付和清算功能)开发和使用的共识算法。在涟&#039；在美国的网络中，事务是由客户机(应用程序)发起的。，通过跟踪节点(trackingnode)或验证节点(validatingnode)将事务广播到整个网络。跟踪节点的次要功能是分发交易信息和响应客户的账簿请求。。校验节点不仅包括跟踪节点的所有功能，还可以通过协商一致在账簿中增加新的账簿实例数据。

波纹的共识发生在验证节点之间，每个验证节点都预先配置了一个可疑心脏节点列表。，称为UNL(唯一节点列表)。列表中的节点可以对事务进行投票。共识过程如

下：

(1)各校验节点会不定时的接收网络发来的过往交易，与国外账簿数据校验通过后，，非法交易被直接丢弃，合法交易将被归纳成一个候选集。在事务候选集之外，还有以前的共识过程遗留下来的事务。

(2)每个验证节点将自己的事务候选集作为建议发送给其他验证节点。

(3)验证节点收到其他节点的提议后，如果不是来自UNL上的节点，则忽略该提议；如果它来自UNL的一个节点，它会将提案中的交易与其他地方的交易进行比较。如果有相同的交易，该交易将获得一票。在一定时间内，当交易获得超过50%的票数时，交易进入下一轮。不超过50%的交易将在下一次共识流程中确认。

(4)验证节点将拥有50%以上票数的事务作为提案发送给其他节点，同时将所需票数的阈值提高到60%，重复方法(3)和(4)直到阈值达到80%。

(5)校验节点将80%UNL节点确认的交易正式写入外账数据，称为最后一笔已结账账，即最后(最新)出现的账。

在涟漪&#039；s共识算法，投票节点的身份都是事先知道的，所以算法的效率比PoW等匿名共识算法更有效率，确认交易只需要几秒钟。这也决定了共识算法只适用于联盟链或者私有链。。Ripple一致性算法的拜占庭容错(BFT)为(n-1)/5，这意味着全网20%的节点可以容忍拜占庭故障而不影响正确的一致性。

2。草图理解模式

共识过程中节点交互示意图：

共识算法流程：

(8)池验证池共识机制

池验证池共识机制是在激进分布式一致性算法(Paxos和Raft)的基础上发展起来的一种机制。Paxos算法是1990年提出的基于消息传递的具有高容错性的一致性算法。。过去Paxos一直是分布式协议的规范，但是Paxos很难理解，更难完成。Raft是一种比Paxos更复杂的一致性算法，可以解决Paxos解决的问题。。Paxos和Raft达成共识的过程似乎和选举一样。候选人需要强迫多数选民(服务器)投他一票，一旦被选中，就按照他们的操作。Paxos和Raft的区别在于选举的详细过程。。池验证池共识机制就是基于这两种有能力的分布式一致性算法，辅以数据验证机制。

区块链是基于P2P网络，由节点参与的分布式账本系统。它最大的特点是&quot分散化&quot。。也就是说，在区块链体系中，用户之间、用户与机构之间、机构之间，不需要建立相互怀疑，只需要依靠区块链协议体系就可以完成交易。

但是，如何保证账本的准确性、威信和可靠性呢？？为什么区块链网络上的节点参与簿记？节点诈骗怎么办？如何防止书籍被篡改？如何保证节点间的数据一致性？这些都是区块链建立一个&quot分散&quot交易，这就产生了一种共识机制。

所谓的&quot共识机制&quot是在特殊节点通过投票在短时间内完成交易的验证确认；出现分歧时，几个节点参与决策，达成共识，无需中央控制。即在没有相互信任的情况下，群体之间如何建立信任关系。

区块链技术使用一套基于共识的数学算法来建立一个&quot信任&quot机器之间联网，从而通过技术背书而不是集中的信誉机构进行全新的信誉发明。

不同类型的区块链需要不同的一致性算法，以保证区块链上的最后一块能随时反映整个网络的形状。迄今为止

主要有以下几类区块链共识机制：POW工作量证明、POS公平证明、DPOS授权公平证明、Paxos、PBFT(拜占庭容错算法)、dBFT、DAG(有向无环图)

。

接下来主要讲一下稀有POW，POS和DPOS共识机制的原理和应用场景

概念：

功的证明，本来是一个经济学术语。指系统为达到某种目的而设定的测量方法。复杂理解是确认自己做了一定工作量的证明，是通过对工作成果的认证来证明自己完成了相应的工作量。

工作负载证明机制具有完全分散的优势。在具有工作量证明机制共识的区块链中，节点可以自由进出，通过计算随机hashhash的数值解来争夺记账权，从而获得生成block的正确数值解&#039；s能力是节点计算能力的详细表现。

应用：

POW最著名的应用是比特币。在比特币网络中，在分块生成的过程中，挖掘者需要解决复杂的密码数学问题，找到一个合适的由n个前导零组成的分块哈希，零的个

数取决于网络的难度值。。这期间需要少量的试算(工作量)，计算时间取决于机器的哈希运算速度。

找到一个合理的散列是一个概率问题。当一个节点的计算能力占整个网络的n%时，，节点有n/100的概率找到块散列。节点成功找到满意的Hash值后，会立即对整个网络进行广播打包，网络的节点会立即对广播进行验证，并对块进行打包。

如果验证通过，表示某个节点一旦成功解谜，就不再与后面的块合作，而是选择接受这个块，记录在自己的账本上，然后与下一个块合作进行猜测。只要网络中的块能最快解出谜题，就会被添加的账本中的其他节点复制。为了保证整个账簿的唯一性。

如果节点作弊，会导致网络的节点验证失败，直接放弃其封装块。这一块不能记入总账，作弊节点消耗的成本就浪费了。因此，在巨大的开采成本下，矿工自觉自愿遵守比特币系统的共识协议，保证了整个系统的安全。

优缺点

优点：结果验证速度快，系统节点数量多。作恶的成本高，从而保证矿工的自觉遵从。

缺陷：需要的算法数量少，达成共识的时间长

概念：

利害关系证明。要求认证者提供一定数量的加密货币的所有权。

权利证明机制的运行模式是，当发明一个新块时，矿工需要创建一个&quot货币权利&quot交易，交易会按照事后设定的比例给矿工自己发一些硬币。。根据每个节点的比例和时间&#039；s令牌，公平性证明机制降低了根据算法等比例挖掘节点的难度，从而加快了随机数的搜索速度。

申请：

2012Peercoin(点币)由网名SunnyKing的网友推出，是权限证明机制在加密电子货币中的首次应用。PPC最大的创新在于其挖矿方式是POW和POS的混合，新币采用工作量证明机制发行。，利用权益证明机制维护网络安全。

为了完成POS，SunnyKing在中本聪创建了自己的比特币基地，还特意想象了一种

特殊类型的交易，叫做Coinstake。

上图是Coinstake的工作原理，其中币龄是指货币的持有期。如果你有10枚硬币，持有10天，那么你已经收集了100天的币龄。如果你用了这10个硬币，硬币的年龄就花了(保留了)。

优缺点：

优点：达成共识所需时间缩短，浪费的精力比工作量证明的多。

缺点：本质上网络中的节点还是需要进行挖掘操作，难以保证传送的真实性

概念：

委托股权证明机制，类似于董事会的投票，内置了股东实时投票系统，就像系统在捧一个股东&#039；永远不会结束的会议。所有股东在这里投票决定公司&#039；的决定。

授权股证可以试图解决保守的PoW机制和PoS机制的问题，同时可以通过实施科技专制来抵消集权带来的负面效应。。基于DPoS机制的区块链分权取决于一定数量的代表，而不是某些用户。在这样的区块链中，一些节点投票选举一定数量的节点代表，这些节点代表一些节点确认区块，坚持系统有序运行。

同时区块链的一些节点有权随时任命和委派代表。如果有必要，有些节点可以通过投票的方式让现任节点代表获得代表资格，重新选举新的代表，这是专制的梦想。

应用：

Bitshare是一种使用DPOS机制的加密货币。通过引入见证的概念，见证人可以生成块，每个持有位的人都可以投票给见证人。。失去总赞成票的前n(n一般定义为101)名候选人可以被选为见证人，需要满足所选见证人的数量(n):至多半数投票人认为n已被充分下放。

证人候选人名单每保护期(1天)更新一次。然后随机安排证人，每个证人有2秒钟时间&#039；允许按顺序生成块的时间。如果见证服务器无法在给定的时间片中生成块，则块生成权限将在下一个时间片中授予相应的见证服务器。。DPoS的这种想象力使得块生成更快、更节能。

DPOS充分利用了股东&#039；以公平民主的方式投票达成共识。他们投的N个证

人，可以算是N个矿池。并且这N个矿池的相互权益是完全平等的。股东可以随时通过投票改变这些证人(矿池)，只要他们提供的计算能力不动摇，电脑宕机，他们试图利用自己的权利作恶。

优缺点：

优点：增加参与验证和核算的节点数量，实现秒级一致验证

缺点：中心级弱，安全性较POW弱，节点代理人为选择，公平性较POS低。同时，整个共识机制仍然依赖令牌的发放来维持代理节点的稳定性。

所谓共识和复杂的理解，是指我们都达成一致的意思。在区块链，这实际上是一个规则。每个节点根据这个规则确认自己的数据，最终维护全网数据库的一致性。

如果以生活为例，公司会比平时多开一次会，但是因为老板不在，我们需要自己决定要不要做一个项目。

在这样一个群龙无首的环境下？

如何达成这种共识，最终形成决策交给老板？这个过程需要共识机制发挥作用。

这个时候可能有人建议大家做个声明，做个声明。最后自己投票，提议者会记录讨论和发言过程，最后取消举手表决的结果，交给老板。

最后，根据&quot如果投赞成票的人数多于支持的人数，就启动项目；否则，退出&quot规则。，构成了决定。那么投票规则就是共识机制。

在区块链世界之外，因为区块链运行的是分布式账本，也许是分布式数据库，当创建一个新的区块时，如何检查区块下面各个账户的准确性？，让每台电脑上注销的书暂时一致？这需要一个共识机制的存在。因此，共识机制是使区块链系统能够保持每个节点的账户(也许是数据)长期一致的一组机制。在

区块链中，共识是区块链科技值得信赖的解决方案。

共识自批，自批生效，支持出局。

就像你总是遵循社群机制，做一些自私的事情。

那你就成了恶意节点，步履艰难。