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发生的，所以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。由于少数大户持有全网大量代币的情况，随着运行时间的增加，全网可能会越来越集中。。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。在晃动的情况下，每秒可以发生12次左右的交易，但是因为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。素描理解表

(PS:越有&quot股份&quot权限，获取账号权限越复杂。这意味着你得到多少钱取决于你为采矿贡献的任务量。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。基础介绍

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，以及每个系统的持有者&#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。股东除了自己投票选举外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个代表，然后这些代表负责生成和验证区块。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块验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，可以实现秒级的共识验证。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，必须验证前一个块已经被可疑节点签名。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。这些多疑的心节点(即见证人)代替其他持币人行使权益，见证人节点求情临时在线，从而处理因PoS签堵人不总是在线而可能导致的堵延时等一系列成果。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，非常适合企业级应用。DPoS是一个非常好的选择，因为工信宝数据交换对数据交易频率要求很高，需要临时摇摆。

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。在采用power(工作量证明)的比特币网络中，获胜概率取决于决定哪个矿工节点拥有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。。

所选择的生动见证将事务打包，并根据时间消耗块。每轮方块消费结束后，见证人随机洗牌并决定新时间后进入下一轮方块消费。

3。DPOS

应用实例

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。基础介绍

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，该系统只需要2/3的普通节点具有上述文章的内容，就可以保证最终输入一致的共识结果。换句话说，在使用PBFT算法的系统中系统中至少有三分之一数量的节点可以容忍(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主要适用于民营连锁和联盟连锁。

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。，激活主节点的有效性操作；

(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，并广播到其他有效节点；

(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(见上图)做出自己的声明，即少数服从多数的准则。假设超过三分之二的超级节点同意说话者&#039；的计划。，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。假设提案在一定时间内没有被同意，如果发现合法交易，其他超级节点可以重新发起提案。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。每个代表首先区分发言者的计算结果是否与自己的记录一致，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。

假设不到三分之二的代表达成共识，随机选出新的发言人，然后重复上述过程。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

向三个代表中的两个发送了恶意信息(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准确的信息，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；右边的代表向其他代表发送了不准确的信息(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都可以验证诚实说话人拟定的方案，并达成三分之二的共识。。代表们也能分辨出说话者到底是对正确的节点撒了谎还是正确的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失效节点数)。这是一个集中的系统-网络中节点的数量和身份必须是已知的和经过验证的。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)Ripppleconsensusalgorithm

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。跟踪节点的主要功能是发布交易信息，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。事务候选集还包括先前共识流程遗留下来的无法确认的事务。

(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建议后，假设该建议不是来自UNL上的一个节点，则忽略该建议；假设它来自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发表于2013年，是一种比Paxos更复杂的一致性算法，可以达到Paxos处理的结果。

。Paxos和Raft达成共识的过程似乎和选举一样。候选人需要说服大多数选民(服务器)投他的票，一旦被选中，就按照他的操作。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。

？拜占庭将军问题(拜占庭将军问题)莱斯利兰波特(leslielamport)在他的同名论文中提出的，是分布式对等网络通信的容错问题。

？在分布式计算中，不同的计算机通过通信和交换信息达成共识，并遵循同一组合作策略措施。但有时分系统中的成员计算机可能会出错，发送错误信息，用于传递信息的通信网络也可能会造成信息维护，使得网络中的不同成员对部分合作的策略得出不同的结论，从而破坏了系统的一致性。这个问题叫做&quot拜占庭容错&quot关于&quot两军的问题。"

？拜占庭假说是梦幻世界的典范。拜占庭综合问题被认为是最困难的容错问题之一。。拜占庭容错协议要求它能够解决由于硬件故障、网络拥塞或断开、恶意攻击等其他计算机和网络的意外行为所导致的各种问题。此外，拜占庭容错协议应该满足待解决问题的规范。

？拜占庭时期，有一个高墙厚墙的城邦，拜占庭，里面蕴藏着死人无法想象的财富。拜占庭周边还有其他10个城邦，同样富裕，但和拜占庭有很大不同。

？拜占庭的十个邻国觊觎它的财富，希望侵占它。然而，拜占庭的进攻非常薄弱，任何单一城邦的入侵都会失败，而入侵者&#039；军队将被摧毁。城邦本身被其他九个互相觊觎的城邦侵略掠夺。

？拜占庭进攻非常强，十个城邦只有一半能同时防守突破。换句话说如果有六个相邻的城邦共同防御，就会成功，获得拜占庭的财富。然而，如果其中一个背叛了其他城邦，则允许一起入侵，但在其他城邦防御时退出。，就会导致只要五个或更少的城邦军队同时防守，那么所有防守城邦的军队都会被消灭，然后被其他城邦(包括那些(少数)背叛他们的城邦)入侵掠夺。

？这是由许多互不怀疑的城邦组成的网络。各城邦必须共同努力完成自己的权益。而且，城邦之间和谐沟通的唯一途径就是通过信差骑行在城邦之间传递信息。。城邦决策者可以&#039；不要聚集在一个中心会议上(所有城邦的决策者都不要&#039；不要互相怀疑他们的和平会在他们的城堡或者军队之外失去。

？城邦的决策者可以在任意的时间和频率互相派遣任意数量的信使。每条消息包括以下形式：我们的城邦会在某一天的某个时间发动攻击。你愿意参加吗？"如果接收

城邦同意，城邦会在原信后附上签名或盖章的回复，寄回给发信城邦。然后，新合并信息的副本被逐一发送到其他八个城邦，要求它们也这样做。最终目标是用所有十个城邦决策者的印章在原始信息链上盖章，就能按时达成共识。最初的结果是会有一个有十个邮票的包赞成同时攻击，一些丢弃的包包括一些但不包括一些邮票。

？在这个过程中，出现了第一个问题，即如果每个城邦向其他九个城邦各派一名使者，那么这十个城邦各派九名使者，也就是说在任一时刻都要计算90次传送。而且每个村子都收到了九条信息，每条信息都可能写有不同的攻击时间。

？在这个过程中，还有第二个问题，就是会允许某些城邦超过一个攻击时间，故意背叛攻击发起者。所以他们会重播不止一个(甚至很多)包，产生很多甚至几个足以淹没一切的噪音。

？有了上面提到的两个问题，整个网络系统可能会发生快速的变化。，并演变成不可信信息和攻击时间相互矛盾的纠结体。

？拜占庭假设是幻想网络世界的模型。在幻想网络世界中，由于硬件故障、网络堵塞或断网以及恶意攻击。网络上可能有很多不可预知的行为。拜占庭容错协议必须处理这些故障，并满足待解决问题所需的规范。

？中本聪的拜占庭将军问题得到了完美的解决&#039；区块链南部。也就是说，以上两个问题都完美解决了。

？本质上，拜占庭一般问题的第一个问题是时间和空间的障碍导致信息不准确，不及时。

？区块链&#039；第一个问题的解决方案是应用分布式存储技术和比特流技术(BT技术，一种新的点对点传输技术，具有节点同时充当客户端和服务器的特点，没有中心服务器)，将整个网络系统中的所有交易信息汇总到一个一致的、分布式存储的和近乎实时同步更新的电子总账中。一致的分布式独立账本解决了空间障碍问题；几乎同步地，实时地。所有账簿备份的持续更新和核对解决了时间障碍问题。

？这个过程更详细的描述是关于将区块链系统中所有交易活动的记录数据统一在一个标准化的总账中；区块链系统的每个节点都会保留一份总账的副本；所有总帐备份都是实时的。，继续更新、对账和同步。区块链系统的每个节点都可以在总分类账中添加记录；每一个新增加的记录都会实时广播到区块链系统；因此，每个节点上的总帐的每个副本都同时更新。，并且所有总帐备份都是同步的。

？拜占庭将军的第二个问题，本质上是关于信息过载和信息干扰。信息过载和信息

干扰问题导致决策延迟。甚至决策体系瓦解，无法决策。

？区块链&#039；对第二个问题的解决方案是，区块链系统的任何节点在发送每个新添加的记录时都需要附加一条额外的信息。。对于区块链系统的任何一个节点来说，获取这个附加信息都是感兴趣的，并且只有一个节点能够获得它。这样，区块链系统的任何节点在添加附加信息时都无法达成一致的问题就太多太乱了。这里区块链系统的任何节点获取该附加信息的过程是众所周知的工作负载证明机制。

？共识机制主要解决如何记录和保存区块链系统数据的问题。。工作量证明机制是一个需要区块链系统的节点通过做一些困难的工作来获得结果的过程。

？区块链系统中的一个节点生成一个新的事务记录，该节点将新的事务记录广播到整个网络。。整个网络的每个节点接收该事务记录，并与所有其它事务记录分开形成事务记录列表，以打包成块。。首先散列列表中的所有交易；然后对得到的哈希值进行哈希运算，得到Merkle树和Merkle树的根值；将Merkle树的根值和其他相关字段组合成一个块头。

？每个节点通过将块头的80字节数据和块头的一个不停的随机数相加，进行不停的哈希运算(其实这是一个双哈希运算)；不断将哈希结果值与未来网络的目的值进行比较。直到哈希结果值小于目标值，得到满足要求的哈希值，工作量证明完成。

？分布式区块链系统是一个静态变化的系统(硬件运行速度的增加)网络中节点参与水平的变化)。系统的不断变化，一定会带来系统计算能力的不断变化。计算能力的变化会导致消耗计算能力(工作)获得符合要求的哈希值的速度不同。最终的结果将是区块链增加和减少的速度的巨大差异。。这是个大问题。为了解决这个问题，区块链系统根据计算能力的变化自动调整劳动难度。也就是说用移动平均法来确认难点是每小时生成块的速度是预定的平均值。

？在区块链系统中，一个符合要求的哈希值由n个前导零组成，零的个数取决于网络的难度值。为了将积木搭建的时间控制在十分钟左右，区块链系统采用了流水完成的难度算法。。难度值每2016块调整一次。

？新的难度值基于第一个2015块(实际上应该是2016块，由于写作中的常见错误，使用了2015年而不是2016年的区块时间进行计算。

？难度=目标值*生成第一个2015块所用的时间/1209600(两周内的秒数)

？这样，通过正则算法，区块链系统保证所有节点计算的难度值一致，积木搭建时间也差不多。

？(1)结果不可控。。它依靠机器执行散列函数的运算来获得结果；计算结果是一个随机数；没有人能间接控制计算的结果。

？(2)计算对称。也就是说，获得结果和检查结果所需的工作量是不同的。。计算结果所需的工作量远远大于接受结果所需的工作量。

？(3)主动控制计算难度。以便将块的形成时间控制在十分钟左右。区块链系统主动控制每个符合要求的散列，并在大约十分钟内获得它。

？第一，方法复杂，容易。

？第二，系统达成的共识是复杂的。节点之间没有太多的信息交换。

？第三，系统相对不稳定可靠，任何破坏系统的企图都需要投入相当大的资金。

？首先，它消耗少量的计算能力。也就是浪费电力等资源。

？第二，区块识别时间确实很长，而且很难缩短。

？第三，新创建的区块链非常简单，并受到计算能力的攻击。

？第四，容易产生区块链分叉，波动的区块链需要多次确认，而且这种情况可能会时不时的持续下去。

？第五，计算能力的逐渐集合，导致与去中心化的系统想象基础的冲突越来越明显。。

？公平证明机制是工作量证明机制的替代方法，试图解决浪费工作量计算的问题。目前，其成功的应用是区块链硬币计数系统。

？股权证明并不要求区块链系统的节点完成一定量的计算工作，而是要求区块链系统的节点表明对一定量货币的所有权。

？衡平法上的证明机制首先应用于区块链的硬币计数系统。。

？当硬币计数区块链系统的块生成时，节点需要构造一个&quot硬币权益&quot交易，也就是把自己的一些币和预设的奖励发给自己。当执行散列计算时。哈希值的计算只与交易输出、一些额外的流量数据和后来的时间(是一个正数，代表自1970年1月1日以来的秒数)有关。然后，按照类似工作量证明的要求，检查这个哈希值

是否正确。

？除了散列计算的难度被设置成与&quot货币时代&quot在交易输出中，具有计数硬币的区块链系统的公平性证明机制非常类似于工作量证明机制。其中，货币年龄的定义是交易产出规模与其存在时间的乘积。。公平证明机制中的哈希值只与时间和流动数据有关，所以没有办法通过完成更多的工作来快速得到。

？每个计数区块链系统的交易输出有一定的概率产生与货币的年龄和交易的货币量成比例的有效工作。

？首先，它缩短了达成共识的时间。

？第二，不需要消耗少量电力。

？首先，仍然需要哈希计算。

？第二，所有的确认都只是一个概率表达式。，而不是一件正面的事情，可能会受到其他攻击。

？授权份额认证机制类似于股权认证机制，是BitShares采用的区块链公共知识算法。。授权份额认证机制是区分威权选举和轮流执政以肯定区块出现的一种方式。

？授权份额的认证机制是节点选举若干代理，代理验证记账。其他方面类似于股权证明机制。

？每个节点根据其持股比例有相应的影响力，51%节点的投票结果将是不可逆的，具有约束力。以达到及时高效的方法达到51%的赞同率的目标。每个节点可以将其投票权授予一个节点。。票数最多的前100个节点按照既定的时间表轮流生成块。每个节点被分配一个时间段来消耗该块。

？所有节点将获得相当于平均水平的块中包含的交易费的10%作为奖励。

？一、大幅增加参与验证核算的节点数量，

？第二，共识验证可以快速完成。

？主要的缺点是我们仍然可以&#039；我无法摆脱对代币的依赖。

？在分布式计算中，不同的计算机试图通过信息交换达成共识；但是，有时系统或

成员计算机上的和谐计算可能会由于系统误差而交换错误的信息，从而影响系统的最终一致性。

？拜占庭将军的问题是根据错误计算机的数量寻找可能的解决方案，找不到相对的答案，只能用来验证一个机制的有效水平。

？拜占庭问题的可能解决方案有：

？在N3F1的情况下，一致性是可能的。其中n是计算机总数，f是有问题的计算机总数。。计算机之间交换信息后，每台计算机列出所有丢失的信息，并将大部分结果作为解。

？第一，系统运行可以摆脱对令牌的依赖，约定每个节点由业务参与者或监管者组成。安全性和稳定性由业务利益相关者来保证。

？第二，共识的延迟大约是2到5秒。

？第三，共识效率高，可以满足高频交易量的需求。

？第一，当1/3或以上文章的记账员停止工作时，系统将无法提供服务；

？第二，当上述文章有三分之一或三分之一以上被记录时，记账人就能识别恶。系统中可能存在会留下加密证据的分叉。

？蚂蚁改进了适合拜占庭的容错机制。机制是通过权益选择记账人，然后记账人通过拜占庭容错算法达成共识。

？这个算法在PBFT的基础上改进如下：

？首先，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；

？第二将静态共识参与节点改进为可以静态进入和参与的动态共识参与节点；

？第三，为共识参与节点的产生设想了一套基于持有权比例的投票机制，通过投票确定共识参与节点(记账节点)；

？第四，在区块链中引入数字证书，解决了投票中记账节点真实身份的认证问题。

？第一，专业记账员；

？第二能容忍任何种类的错误；

？第三，记账是很多人做的，每一块都有定局，不会出现区块链分叉；

？第四严格的数学证明保证了算法的鲁棒性；

？第一，当1/3或以上文章的记账员停止工作时，区块链系统将无法提供服务；

？第二当1/3或以上几条的记账人分别作恶，而其他所有记账人恰好连接成两个网络孤岛时，恶意记账人可以使区块链系统分叉，但会留下密码证据；

？Ripple共识机制是一些节点选择特殊节点组成特殊节点列表，特殊节点列表中的节点达成共识。

？初始自组织节点列表就像一个俱乐部，它希望接收一个新成员。，必须由51%的俱乐部成员投票决定。共识遵循这个核心成员51%的权益，外人没有影响力。Wave共识机制将股东与其投票权分开，因此比其他制度更集中。

？瑞博共识机制只要参与共识的形成，就大大增加了共识形成的时间。在实践中，瑞博区块链系统达成共识需要3-6秒，这比比特币区块链系统的10分钟要快得多。。同时，瑞博区块链系统每秒可以处理数万笔并发交易，而比特币区块链系统每秒只需要7笔交易。

涟漪共识机制有不同的方式来处理节点的共识。。瑞博的信任节点讨论发明新块的时间是在区块链更新之前。先讨论，达成共识后再更新区块链。

由于涟漪共识机制的共识是由特殊节点达成的，普通节点不需要保护一个完整的历史账本。。各节点可根据自身业务需要，选择同步性好的历史账簿或最近步骤的任意账簿。这也意味着对存储空间和网络流量需求的增加。

涟漪共识机制撤销了发行货币挖坑的机制。，利用原始货币(1000亿枚)发行硬币，从而防止采矿时的少量能源消耗。

所谓&quot共识机制&quot是通过在特殊节点投票，在极短的时间内完成交易的验证和确认；是的，一笔交易如果几个利益不相关的节点能达成共识，我们可以认为全网也能就此达成共识。进一步说，如果一个中国的微博大V，一个美国的虚拟币玩家，一个非洲学生，一个欧洲游客don&#039我不认识对方。但是他们都认同你是个坏人，所以基本上可以判断你不坏。

为了使整个区块链网络节点坚持相同的数据，保证每个参与者的公平性，整个群系统中的所有参与者必须有一致的协议。，也就是我们这里要用到的共识算法。比特币的所有节点都遵循相同的协议标准。协议标准(共识算法)由相关共识规则组成，分为两大核心：工作量证明和最长链机制。。所有规则(共识)的最终表现就是比特币最长的链条。共识算法的技巧是保证比特币在最长的链条中保持运行，从而保证整个记账系统的一致性和可靠性。

区块链的用户在进行交易时不需要考虑对方的信誉，不需要信任对方，也不需要有可信的中介或中心机构，只需要根据区块链协议实现交易即可。。这种没有可信第三方中介的成功交易的前提是区块链的共识机制，即在相互理解和信任的市场环境下，参与交易的所有节点都想着自己的利益，没有非法的欺骗效果或行为。因此，每个节点都会主动自觉地遵守预设的规则来识别每笔交易的真实性和可靠性，并将通过检查的记录写入区块链。每个节点的利益是不一样的，所以从逻辑上来说，并不具有合谋欺诈和欺骗的效果。当网络中的一些节点具有公共信誉时，这一点尤其明显。区块链技术使用基于数学原理的共识算法来建立一个&quot信任&quot节点之间的网络，并应用技术手段实现一个创新的信誉网络。

目前区域金融行业主流的共识算法机制包括工作量证明机制、股权证明机制、份额授权证明机制、池验证池四大类。

工作量证明机制就是工作量的证明。，是在生成新的交易信息(即新的块)以参与区块链时必须满足的要求。在基于工作量证明机制的区块链网络中，节点通过计算随机哈希的数值解来争夺记账权。找到生成块的正确数值解的能力是节点计算能力的详细表现。工作量证明机制具有完全分散的优点。在具有共识工作量证明机制的区块链中，节点可以自由进出。。我所熟悉的比特币网络应用工作量证明机制生产新货币。但由于比特币网络应用了工作量证明机制，接收了全球计算机的大部分计算能力。其他想要尝试使用这种机制的区块链应用程序很难获得非常广泛的计算能力来维护自身的安全。同时，基于工作量证明机制的挖掘行为也形成了少量的资源浪费，且达成共识需要较长的周期，因此这种机制不适合商业应用。

2012年，化名SunnyKing的网友推出Peercoin，以工作量证明机制发行新币，以权益证明机制保护网络安全。这是权益证明机制在加密电子货币中的首次应用。。与要求认证者进行一定量的计算不同，权益证明要求认证者提供一定量加密货币的所有权。权益证明机制的运行模式是，当创建一个新区块时，矿工需要创建一个&quot货币权利&quot交易。交易会按照预先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。这种共识机制可以缩短达成共识所需的时间。但本质上，网络中的节点仍然需要进行挖掘操作。所以PoS机制并没有从根本上解决PoW机制难以应用到商用范围的问题。共享授权认证机制是一种新

的保证网络安全的共识机制。。在试图解决保守的PoW机制和PoS机制问题的同时，还可以通过实施科技专制来抵消集权带来的负面效应。

股份授权认证机制类似于董事会投票，内置股东实时投票系统。就像这个系统持有一个股东&#039；任何时候开会，所有股东都在这里投票决定公司&#039；的决定。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。在这样的区块链一些节点投票选举一定数量的节点代表，代表一些节点确认区块，保持系统有序运行。同时，区块链的一些节点有权随时任命和委派代表。如有必要，所有节点可以投票取消当前节点代表的资格。新代表的连任是专制的假象。

份额授权证明机制可以大大增加参与验证和记账的节点数量，从而实现秒级共识验证。然而，这种共识机制仍然不能完美地解决区块链在商业中的应用问题。因为共识机制无法摆脱对令牌的依赖，而且很多商业应用都不需要令牌。

池验证池是基于传统的分布式一致性技术，辅以数据验证机制建立的，这是目前区块链普遍采用的共识机制。

池验证池可以不依赖令牌工作，在有能力的分布式一致性算法(Pasox、Raft)的基础上可以实现秒级共识验证，更适合多方参与的多中心商业模式。但是池验证池也有一些缺点。比如共识机制所能达到的分布式水平，就不如PoW机制。

本文主要讲解区块链工作量证明机制的一些算法原理，以及比特币网络如何证明其工作量。希望能对共识算法有一个基本的洞察。

工作量证明系统的主要特点是客户端要做一些困难的工作才能丢失一个结果，验证者可以通过该结果轻松检查客户端是否做了相应的工作。。该方案的一个核心特征是不对称：对于请求者来说工作是适度的，对于验证者来说容易验证。它不同于验证码，验证码更容易被人类而不是计算机解决。

下图显示了工作负载证明过程。

例如，创建&quot你好，世界！"对于一个基本角色来说。我们给出的工作负载要求是，可以在这个字符之前添加一个名为nonce的整数值。对改变的字符执行SHA-256运算(添加随机数)。如果丢失的结果(以十六进制形式表示)是&quot0000&quot，验证通过。为了实现这种工作负载证明的目标，有必要不断降低nonce值。对获得的字符创建执行SHA-256散列操作。根据这个规则，需要4251次运算才能找到前面有四个零的散列。

通过这个例子，我们对工作量证明机制有了初步的了解。。有人认为，如果工作量

证明只是这样一个过程，是不是只要记住nonce是4521就可以让计算通过验证了？当然不是，这只是一个例子。

接下来，我们将输出一个简单的单词变化你好，世界！整数值&quot，整数值为1~1000。也就是把输出变成1~1000的数组：Hello，World！1;你好，世界！2;...;你好，世界！1000。然后，数组中的每个输入依次由下面的工作负载来证明——找到以四个零为前导部分的hashhash。

由于hash值的伪随机特性，根据概率论的相关知识很容易计算出来，估计需要尝试2的16次方。以便得到以四个零作为前导部分的散列hash。但是，如果你统计一下刚才1000次计算的实际结果，你会发现平均计算次数是66958次，非常接近2的16次方(65536)。在这种情况下，数学中期望的计算次数实际上是要求的&quot工作量&quot，而且反复证明工作量会是一件符合统计规律的概率性的事情。

用于计算输入字符并得到相应目标结果的计算次数如下：

对于比特币网络中的任何一个节点，如果想要生成一个新的区块参与区块链，就必须在比特币网络中解决这个谜题。这个问题的关键要素是工作量证明函数、方块和难度值。工作量证明函数就是这个问题的计算方法。块是这道题的输入数据，难度值决定了理解这道题所需的计算量。

比特币网络使用的工作量证明函数就是上面提到的SHA-256。数据块实际上是在工作负载证明链路中产生的。。旷工通过不断构造块数据来检验计算结果是否能满足要求的工作量，以此来区分块是否满足网络难度。块头是比特币工作量证明函数的输入数据。

难度值是矿工的主要参考目标。它决定了旷工需要多次哈希运算才能生成合法块。比特币网络每10分钟生成一个区块。如果在不同的网络计算能力条件下基本保持生成新块的速度，那么难度值必须根据网络计算能力的变化进行调整。。总的准则是不管挖掘能力如何，保持网络10分钟生成一个新块。

难度值的调整在每个完整节点中独立且主动地发生。每2016块，所有节点都会按照一致的格式自动调整难度值。这个公式是基于2016块新生成的成本突破时间与预期时间的比较(如果每10分钟生成一笔贷款，则预期时间为20，160分钟)，按照实际时间与预期时间的比值进行调整。换句话说如果方块生成速度快于10分钟，增加难度值；反正难度值降低了。公式如下：

新难度值=旧难度值*(20160分钟/过去2016块花费的时间)。

工作量认证需要目标值。比特币工作量证明的目标值计算公式如下：

目标值=最大目标值/难度值。,其中最大目标值为一个恒定值0x00000000000fffffffffffffffffffffffffffffffffffffffffffffffffffff

目标值与难度值成正比，比特币工作量证明的达成是矿里计算的块哈希值必须小于目标值。

我们也可以简单理解为比特币工作负载的过程如下通过不断改变块头(即尝试不同的nonce值)并将其作为输入，进行SHA-256哈希运算，找出一个具有特定格式哈希值的进程(即需要一定数量的前导零)，前导零越多越难。

比特币证明工作量的方法大致可以概括如下：

这个过程可以表示如下：

比特币的工作量证明就是我们俗称的主要工作&quot采矿&quot。了解工作量证明机制这将为我们进一步理解比特币区块链的共识机制奠定基础。

不管你能不能接受，以后都会变的。

区块链技术给数字经济带来了剧变的曙光。

这种剧烈的变化在过去50年的互联网历史上发生过两次。第一次剧变是一个全球性的

网络.第二个剧变是全球性的应用.第三次剧变正在酝酿。

——3354从《腾讯区块链方案白皮书》？当我第一次读这篇文章时，我不能&#039；我无法想象这是一家世界级的企业。对一项新技术的评估。

瞬间引起了我的兴趣。什么是&quot剧变&quot刻薄？也就是说，有可能建立我们现有的

经济结构和认知完全改变了我们的生活方式。

一种区块链技术，从2009年诞生的比特币技术概括而来，

居然得到这么高的评价。不是&#039；这难道不是一件奇怪的事情吗？会不会发生

已经很刺激了。我们欢迎一项创新，并可能参与其中。不是每个

时期的人都有这个机会。多么幸运！

不管你接受不接受，以后都会改的。全球很多经济学家、企业家、国家政治家都在推动

崇拜区块链，宣称区块链技术将重塑商业、货币和世界，互联网、银行、证券将建立

。

证券、安防、物流、电力、制造、会计税务、法律服务、文明行业、医药卫生等众多行业

。

当然说到&quot区块链&quot，我会一直提到&quot分散化&quot并且举了很多一般的例子。但是

但是我是一个认真的人，我希望找到自己来做这个区分。我面前的逻辑到底是什么

？一切推论之前都要先了解本质，要了解区块链的核心技术逻辑。

看了一些书和资料，除了&quot比特币&quot，要理解区块链，有两个核心术语

:共识机制和智能契约。共识机制是区块链技术的核心。要理解&quot共识机制&quot，我们不得不提到著名的&quot白

&quot；

法庭上的一般问题&quot，拜占庭一般问题是LeslieLambert提出的点对点通信中的基本

问题，主要用于分析分布式节点传输信息时如何保持数据一致，即一致性的

问题。

拜占庭将军

一群拜占庭将军带领一支军队分别围攻一个村庄。为了简化问题，每个

军的策略仅限于攻击或撤离。

由于部分部队进攻，部分部队撤退可能会产生灾难性后果，将军们必须通过

投票达成一致策略，即全体部队一起进攻或全体部队一起撤退。因为将军们

在农村方向不同。他们只能通过快递联系。

在投票过程中，每个将军都会通过快递通知他的

他的所有将军，让每个将军根据自己的投票和其他所有将军发来的信息进行投票。

通过了解个人投票的结果来决定策略。

系统的问题在于，将军中可能会出现叛徒，他们可能不仅会投票支持糟糕的策略，还会选择性地发送投票信息。。这样就破坏了各军的团结协作。由于

军队需要通过信使进行通信，哗变的将军们可能会通过伪造信件的方式，将

假票作为其他将军发送出去。甚至在保证所有将领忠诚的情况下。，也可以&#039；t干净的信使被敌人杀死，甚至

被敌人间谍交换等等情况。所以很难通过保证人员和通讯的可靠性来解决问题

。

如果忠诚的将军们一开始还能以多数决定战略，那就说拜占庭荣

错了。

拜占庭一般问题被认为是容错问题中最难的类型之一。在具有n个节点的

中

在系统中，每个节点都有一个输入值，有些节点是有缺点的，甚至是恶意的

。

在分布式计算中，不同的计算机通过通信交换信息达成共识，并遵循同一组合作策略

轻微措施。但是，有时系统中的成员计算机可能会出错，发送错误的信息，用于传输

信息的通信网络也可能导致信息保护，使得网络中的不同成员对整体合作策略

得出不同的结论。，从而破坏了系统的一致性。

但是，&quot工作量证明链&quot中本聪在构思比特币系统时应用的(PoW)模型很好地解决了共识问题

。至于什么&quotPoW&quot讨论它是很有趣的。

智能合同是一组以数字形式定义的承诺，包括合同参与者可以在

上实现这些承诺的协议。合同是区块链的第二个地方。合同参与方

延迟达成协议进入区块链系统。双方约定完成后，合同最终执行，

不可更正。至于&quot燃料&quot执行合同所需要的，也就是手续费，也是需要提前支付的。

智能合约可以解决日常生活中罕见的违约行为，如果应用到各个行业，可以防止

违约的声誉问题。

在区块链出现之前，商事范围内的信任关系一般依靠诚实守信的团体和中介。可以成立机构或其他组织。在区块链的新类别中，信任连接的建立是基于网络的

，甚至是网络上的一个对象。区块链推动的智能合同将要求双方根据

保持自己的意愿。。

在区块链系统中，共识机制和智能合约保证了数据的真实性和合约的可执行性，而现实

就是现在&quot分散&quot。当然还有很多技术上的东西没有提到，有意思的可以

在

下深化。虽然大多数人&#039；s对区块链的了解还停留在比特币和各种代币，也就是金融业的创新

。然而，在了解了区块链的核心逻辑后，业内人士&quot区块链&quot，所在区域

分别为。

区块链在各行业的应用刚刚进入上半场，相信会想到很多好的创新方向。

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，用户和机构之间，机构之间，不需要建立互信，只需要依靠区块链协议体系就可以实现交易。

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，这导致了共识机制。

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和确认；有分歧的时候，没有中央控制，几个节点参与决策，达成共识。即没有相互信任基础的集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机器之间的网络，从而通过技术背书而不是集中的声誉机构来创造一个全新的声誉。

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)

。

接下来主要讲常见的POW、POS和DPOS共识机制的原理和应用场景

概念：

工作证明，原本是一个经济学术语。指系统为实现某一目标而设定的测量方法。简

单的理解就是确认自己做了一定工作量的凭证，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，通过计算随机哈希的数值解来争夺记账权，获得正确数值解生成分块的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，在分块生成过程中，矿工需要解决复杂的密码数学问题，找到一个符合要求的分块哈希，这个哈希由n个前导零组成，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。当一个节点拥有全网n%的计算能力时，，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，，表示某个节点已经成功解谜，不再与未来的区块合作，而是选择接受这个区块，记录在自己的账本中，然后进行下一个区块的合作猜测。只有网络中能最快解出谜题的那块才会被添加到账本中，被其他节点复制。为了保证整个账簿的唯一性。

如果一个节点作弊，会导致该网络的节点无法通过验证，间接放弃其打包的块，无法记入总账，作弊节点消耗的成本也就浪费了。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：结果可以快速验证，系统节点数量多。作恶的成本高，从而保证矿工的自觉遵从。

缺点：需要的算法数量少，达成共识的周期长

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。

权限证明机制的操作模式是，当创建新块时，矿工需要创建&quot货币权利&quot

交易，交易会按照预先设定的比例给矿工自己发一些币。。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按比例挖掘节点的难度，从而加快了寻找随机数的速度。

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。

为了实现POS，SunnyKing在中本聪比特币基地自创，专门构思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。如果你使用这10个硬币，硬币的年龄被消耗(保留)。

优缺点：

优点：缩短达成共识所需的时间比工作量证明更浪费。

缺点：本质上仍然需要网络中的节点进行挖掘操作，难以保证转移的真实性

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。

授权股证可以尝试解决传统PoW机制和PoS机制的问题，同时可以通过科技民主的实施来抵消集权带来的负面效应。。基于DPoS机制的区块链分权依赖于一定数量的代表，而不是所有用户。在这样的区块链中，所有节点投票选举一定数量的节点代表，节点代表将代表所有节点确认阻塞并保持系统有序运行。

同时区块链各节点有权随时委派和任命代表。如有必要，各节点可以通过投票让当前节点代表获得代表资格，重新选举新代表，实现实时民主。

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。。获得同意票数总数的前n(n一般定义为101)名候选人可被选为见证人，选出的见证人人数(n)应满足以下要求：至少有半数投票人认为n已得到充分分散。

见证候选人列表每维护周期(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的这种思想使得块生成更快且更节能。

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。，而且这N个矿池的相互权益完全平等。股东可以随时通过投票改变这些证人，只要他们提供的计算能力不稳定，计算机停机，或者他们试图利用他们的权力作恶。

优缺点：

优点：减少参与验证和核算的节点数量，从而实现秒级共识验证

缺点：中心化程度弱，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。

区块链共识机制的讨论让很多人头疼，尤其是在认识和现实的矛盾方面。几个主流的区块链共识机制也面临类似的问题，关心我们。