很多朋友会问以太坊为什么要进行PoS，你知道以太坊吗，说明有人不&#039；你对这个问题不太了解，是吗？那么你对以太坊了解多少？让&#039；让我们仔细看看边肖的作品！

pos是公共链中的共识算法，作为pow的替代方案。Pow是一种确保比特币、当前以太坊和许多区块链安全的机制。然而，pow算法被批评为在采矿过程中破坏环境和浪费电力。Pos试图通过用不同的机制代替挖掘的概念来解决这些问题。

ps机制可谓是一种虚拟挖矿。由于pow主要依靠计算硬件的稀缺性来防止女巫攻击。当权有可能一个用户花1000美元买电脑，加入网络挖矿，生成新块，从而获得奖励。在pos中，用户可以获得一千美元，购买等值的代币，并将这些代币作为押金放在pos机制中，只要用户有机会产生。，让用户获得奖励。

pos算法如下。有一批持币人把他们的代币放进POS机，所以他们成了验证者。

区块链的特点之一就是去中心化。。即节点会分布在各个地方，形成一个分布式系统。每个节点需要在一个问题上达成一致，理想情况下，它只需要同步状态。

如上图所示，节点B将a=1=a=2的状态同步到？ACDE四节点此时，系统中的状态变为a=2，但如果恶意节点AE在收到通知后，将a=1=a=3改为错误的节点，所有人&#039；s状态此时会不一致，需要一个共识机制来获得系统中唯一正确的状态。

如上所述，分布式系统中存在恶意节点导致系统状态不一致的情况下，存在一个众所周知的虚拟问题——拜占庭一般问题。

拜占庭将军问题是指N个将军进攻一座城堡。如果超过一定数量的将军同时进攻，进攻可以成功，如果少于，进攻就会失败。将军中可能有叛徒。

这个时候有两种情况

1。如果两个叛徒都在BCDE，那么共识算法需要让另外两个将军遵循一个&#039；进攻城堡的决定是正确的。

2。如果A是叛徒，共识算法需要让BCDE剩下的三个忠诚的将军保持一致。这个问题有很多解决方法。如果你有兴趣，你可以亲自去看看(推荐PBFT)。让&#039；的重点是中本聪，目前在以太坊使用。共识和将使用什么？Casper友好的终局性小工具共识如何解决拜占庭一般问题。

说到NakamotoConsensus和CasperFriendlyFinalityGadgetConsensus，你可能不太熟悉，但它们的一些组成部分应该很熟悉——POW(工作量证明)和POS(权益证明)。

POW或POS称之为Sybil抗性机制。为什么需要西比尔抗性机制？刚才我们谈到了拜占庭将军的问题。应该不难看出，恶意节点越多，达成正确共识的难度越大。Sybil攻击是指攻击者可以伪装大量节点进行攻击，Sybil抵抗是指抵抗这种攻击的能力。

POW允许矿工或验证者投入计算能力，POS允许验证者质押以太坊。如果攻击者想伪装多个节点进行攻击，肯定会投入大量的计算能力或资产，导致攻击成本高于收益。以太坊保证的安全性是，除非攻击者获得整个系统51%的计算能力或资产，否则不可能攻击成功。

解决Sybil攻击后，选择系统中最长的链作为大家达成共识的链。

很多人通常把权力和职位看作是简化的共识机制，这样说不够准确，但也说明了它们的重要作用。让&#039；让我们分析权力和地位。

通过hash的不可逆特性，要求每个矿工不断计算某个值的hash符合某个特性，比如前几位是000000。因为这个过程只能靠试错来计算hash，所以是工作量证明。计算完成后，其他节点验证的值满足哈希特征，非常容易验证。验证后成为合法区块(不一定是共识区块，但需要在最长链中)。

以太坊中的挖掘算法使用两个数据集，一个小数据集缓存1和一个大数据集DAG。这两个数据集随着区块链中块数的增加而逐渐变大，初始缓存大小为16MDAG和1G。

让&#039；让我们先来看看这两个数据集的生成过程。

缓存生成规则是有一个种子随机数，缓存中的第一个元素哈希种子，后面数组中的每个元素都是通过哈希第一个元素得到的。

Dag生成的规则是什么？在缓存中找到相应的元素后？根据元素中的值，计算下一次要搜索的下标，经过256个周期后，得到cache中最终的元素值，通过哈希计算得到DAG中该元素的值。

那就让&#039；让我们来看看矿工如何采矿，光节点如何验证

矿工的过程&#039；挖掘就是选择一个Nonce值映射到DAG中的一个条目，通过条目中的值计算出下次要找的索引，循环64次。，得到最后一项，计算该项中的值hash得到结果。将结果与目标进行比较。如果满足条件

，则证明该区块已被挖。如果不满足条件，就用nonce代替继续挖掘。。矿工在采矿时需要将1G的DAG读入内存。

光节点的验证过程和矿工的挖掘过程基本相同。

块报头中的Nonce值映射到DAG中的项目。，然后通过缓存数组计算该项的值，通过项中的值计算下次要找的下标，循环64次得到最终项。计算项目中的值哈希以获得结果，并将结果与目标进行比较。如果符合条件，则通过验证。。轻型节点在验证时不需要将1GDAG读入内存。Cache用于每次计算DAG的项目值。

以太坊为什么需要这两个大小不同的数组进行辅助哈希运算？什么&#039；直接哈希运算有什么问题？

如果只进行重复计算，会导致采矿设备专业化，降低分散化程度。因为我们日常的计算机内存和计算能力都是需要的，如果我们挖掘，只需要哈希运算。矿用设备会被设计成具有超高的计算能力，但内存可以降到很少甚至没有，所以我们选择1G大内存，增加内存访问的频率，增加矿用设备对内存访问的需求，更接近我们日常的电脑。

让&#039；让我们看看中本共识是如何解决拜占庭将军的问题的。首先看看区块链的拜占庭将军问题。这是什么？

在区块链中需要达成一致的是哪个链为主链。虽然采用了最长链原理，但是由于分叉问题，，仍然会带来拜占庭一般的问题。

本来以太坊中pow的目标是抵抗51%以下的攻击，但是如上图所示，如果恶意节点继续沿着自己挖的区块挖，主链上就有分叉了。恶意节点在计算能力没有达到51%的情况下就可以超越主链，进而成为新的主链。为此以太坊使用ghost协议将块奖励分配给上图中的B1和C1，并尽快合并到主链中，这样主链的长度(根据合并后的总长度，长度只是一个抽象的概念。根据以太坊中的块权重累积)仍然大于恶意节点&#039；自己开矿。

网络中的用户通过认捐一定数量的以太坊成为验证者。每次，系统从这些验证者中随机选择块创建者，剩下的验证者验证创建的块是否合法。。验证者将获得区块奖励，未选中的区块若未通过验证，将扣除一定数量的质押金，若验证错误，将扣除

全部质押金。

如上图所示，权益证书在每一个特定区块设置一个检查点，用于验证前一个区块。2/3的验证者通过验证，如果验证通过，则该区块的链成为最长合法链(不可回滚)。

我们简单分析了股权证书本身。以太坊的权益证书更复杂的一点是与碎片化机制结合时的操作流程。本章将在一篇关于碎片机制的单独文章中详细介绍。

本文主要讨论共识机制是为了解决分布式系统中的拜占庭一般问题。并且分析了以太坊中的共识机制一般包括最长链选择和一个sybil抵抗机制(pow或pos)。重点分析了pow和pos的流程和设计思想。稍后，我们将重点讨论智能合约。

12月21日消息以太坊核心开发者蒂姆贝科(TimBeiko)在推特上宣布，以太坊将推出首个公共测试网络KintsugiMergeTestnet，用于全面升级到兴趣证书(PoS)。。TimBeiko还表示，虽然客户端开发和UX将继续改进，但鼓励用户尽快开始使用Kintsugi，以便熟悉合并环境中的以太坊网络。主要升级将由存放32ETH的抵押人进行。现在230万个ETH测试网络已经由72，000个验证者存放在新网络中，这表明社区已经为&quot加密领域最大的升级&quot。此外，根据报告，应用程序开发人员不会有太大变化。只与共识层或执行层交互的工具基本不受影响。

什么是权益证明？

股权证明是区块链网络达成共识的共识机制。

这将要求用户抵押他们的以太坊，以成为网络中的合法验证者。在工作负载认证(pow)中，验证者的职责与挖掘者相同：对事务进行排序并创建新的块，以便所有节点都能就网络状态达成一致。

权益书相比工作量证明制度有很多改进：

1。提高能效——。你不&#039；挖砖块不需要很多能量。降低门槛。，硬件要求降低了——你不&#039；不需要优秀的硬件来获得构建新模块的机会。更强的去中心化——好处证明了网络中可以提供更多的节点。

4。更强大的碎片链支持——，可以扩展以太网的关键升级

股权证明，股权质押和验证者

股权证明是鼓励验证者接受更多质押的基本机制。。就以太坊而言，用户需要质押32ETH才有资格成为验证者。验证者被随机选择来创建块，并负责检查和确认那些不是由他们创建的块。一个用户&#039；的权利和利益也被用来作为一种方式来激励良好的验证行为。。比如用户可能因为下线(认证失败)而失去部分权益，或者因为蓄意串通而失去全部权益。

以太坊的股权证书是如何工作的？

不同于工作量证明，验证者不&#039；不需要使用大量的计算能力，因为它们是随机选择的，它们之间没有竞争。他们不&#039；不需要挖掘区块，他们只需要在被选中时创建区块，在未被选中时验证其他人提交的区块。这种验证称为证明。。你可以认为证据是在说&quot我看这件不错&quot。验证者会因为提出新的区块并证明他们所看到的区块而获得奖励。

如果你提供恶意封杀的证明，你将失去你的股权。

权益证书和安全证书

仍然存在51%攻击的威胁，但是对于攻击者来说攻击成本越来越高。要发动51%的攻击，需要控制以太坊51%以上的股份。。这不仅是一笔巨款，而且很可能导致以太币贬值。这是非常容易破坏你的货币价值的大部分权益。当然，有更强的动机来保持网络的安全和健康。

信标链上的权益减少，踢出去，其余的处罚协调，防止其他恶意行为。验证者还将负责记录这些事件。

优点和缺点

优点

股权质押让你更容易跑一个节点。这不需要在硬件或能源方面进行大量投资。如果你不&#039；如果你没有足够的钱抵押，你可以加入抵押池。

股权质押更加分散。它允许更多的人参与进来。而更多的节点不&#039；这并不意味着像采矿一样增加回报率。权益质押可以确保安全保障。碎片链允许以太坊同时创建多个块，增加事务吞吐量。将部方网络纳入工作量认证体系。这将降低网络攻击所需的计算能力。

缺点

与工作量证书相比，股权证书还处于起步阶段，没有经过实际应用的检验。

记账权奖励的eth，不再由矿业提供，而是通过持有eth分红，类似于银行存款的利息。

以太坊区块链上的代币叫以太，代码是ETH。，可以在很多加密货币的外汇市场进行交易，也是以太坊用来支付交易费用和运营服务费的媒介。

以太坊是一个开源的公共区块链平台，具有智能合约功能。通过其专用的加密货币Ether，提供了一个分散的虚拟机(&quot以太坊虚拟机&quot)来处理对等合同。

[扩展数据]

什么&#039；以太坊和比特币的区别：

1。Eth和比特币方向不同

首先，ETH和比特币在区块链体系背后的方向完全不同。比特币&#039；的定位简单来说就是数字货币。，可以认为是点对点的电子现金。它的诞生是为了取代法定货币，解决金融危机。主要用于支付和价值转移。所以比特币背后整个区块链网络的方向主要是基于货币，解决交易和支付的问题。ETH不一样。虽然也是数字货币，具有一定的交易属性，但是ETH背后的以太坊区块链的网络定位是世界级的通用计算平台。它只是借用了比特币中的区块链技术，并在此基础上向偏向互联网的操作系统级应用发展。

2。ETH和比特币的功能不同

由于以太坊和比特币的定位不同，其数字货币功能也不同。比特币&#039；的方向是货币，它希望成为常规货币的替代品。所以，在比特币系统中，数字货币BTC是极其重要的一部分，可以说是整个系统的最终体现。其功能是作为支付交易的媒介和价值储存的载体。但以太坊的目标是操作系统层面的计算平台，更偏向于互联网服务。它的价值在于有多少用户使用以太坊这个平台，你给我提供的服务有多好。所以这就决定了ETH只是以太坊平台中的一个重要环节，而不是所有平台价值的体现。它只是以太网工坊中提高服务质量和处理交易的货币工具，使平台上的点对点交易和应用更加便捷。所以，虽然比特币和以太坊都是数字货币，但比特币想成为法定货币的替代品。作为一个去中心化的电子现金系统，大家都在用。整个系统更像是由区块链技术支持的特定应用。

三、ETH和比特币的机制和原理不同

比特币和以太坊的共识机制不同。。在比特币区块链网络中，起数据维护作用的共识机制是PoW机制，即工作量证明机制。它的工作原理是大家一起参与，谁处理的最快最好，谁就获得记录数据的权利，然后获得比特币的奖励。。由于比特币的应用方向是货币，使用场景是点对点的支付和没有中心化机构参与的交易，比特币强烈需要去中心化和安全性，而PoW机制处理交易太慢，需要耗费大量资源。但是安全性和去中心化程度极高，所以和比特币很契合。

以太坊采用PoS共识机制，即权益证明机制。它的工作原理是大家共同参与，谁持有的以太币多，谁就越容易获得记录数据的权利。然后获得ETH奖励。以太坊的应用方向是操作系统。它希望每个人都在它的系统上部署智能合约和开发去中心化应用。虽然以太坊也需要去中心化的属性，但是比比特币需要更高的效率和更低的成本。否则你平台的数据处理效率太慢，手续费高。谁愿意在你的平台上发展？所以以太坊采用PoS机制，不像PoW机制那么分散，但是效率更高，不需要花费大量资源处理数据。

四、ETH和比特币的生态不一样

ETH和比特币不一样。因为比特币要做货币了，它的价值生态的支撑点在于共识价值，也就是有多少人认可它，用它来交易。。所以比特币的通用设计实际上是一种通货紧缩的经济模型，把比特币的数量限制在只有2100万，所以由于稀缺性的属性，价格会越来越高，更容易获得共识价值。与以太坊不同，支撑其价值生态的点在于产品。即整个平台提供什么样的服务，解决什么样的痛点等服务价值。与安卓、微信等产品类似，以太坊是以太坊平台的工具，可以用来购买气，用于手续费、筹款等使用场景。因此，在以太坊的通行证设计中，以太币的数量没有限制，流通上限是每年1800万，开采难度会随着时间的推移而增加，相对通货膨胀率每年都会降低。总的来说，虽然ETH和比特币都是数字货币，但它们代表了背后的整个区块链体系。功能、原理、生态价值都有区别。以太坊的本质是一个操作系统级的计算中心。以太坊打破了数字货币原有的定位，在比特币的基础上开创了新的方向。它除了本身的货币价值外，还包含整个产品的价值。这是前所未有的。只有了解了这一点，才能理解以太坊为什么是区块链2.0的代表。

以太坊2.0升级的核心是以太坊2.0碎片化和PoS共识机制。。PoS共识机制的采用是为了提高以太坊协议的能量效率，增加以太坊区块链的安全性。以太坊2.0是碎片化的，以太网链不再需要通过每个节点处理链上的每一个事务。

在碎片化系统中，每个节点只需要处理大约1%或更少的事务，从而大大提高了区块链的效率。实施ETH2.0后，不仅网络性能大幅提升，投资者还可以减少重资产(slf0037)的投入。。一致协议Casper和分片技术使网络底层协议发生了巨大的变化，并进一步推动了区块链扩展技术的发展，不断达到商用标准。截至2021年1月7日1

6时，已有超过230万个ETH被锁网。，占以太坊总供应量的2%。然而，这仍然只是更新的第一阶段。根据官方消息，Uniswapv3已经部署到以太坊主网。根据官方文章，Uniswapv3是目前为止该协议最强大的版本。集中的流动性为流动性提供者提供了前所未有的资本效率，为交易者提供了更好的执行能力，以及分散融资的核心基础设施。就以太坊的路线图而言，神五表示，随着合并日期的临近，路线图的很多方面越来越可行。乐观估计今年年底可以完成升级。合并后，执行链将在共识链内运行，每个信标链块将包括执行链中的一个块。他还表示，合并需要很多复杂的技术，目的是让整个过程尽可能简单。对于用户、客户端、开发者和智能合约来说，合并会更顺利，用户也不用太担心。目前很多集中交易所、分散交易所、分散质押协议、基础服务提供商都进入了以太坊2.0的跑马圈地轨道。。不难想象，未来会涌现出更多的服务商，以太坊2.0STakingplate也将成为交易所和钱包的标配。那么ETH1.0的PoW链还能挖多久？目前没有明确的答案。但是可以肯定的是在以太坊完全从PoW转型为PoS之前，以太坊基金会必须花足够的时间证明PoS链是安全的。只有这样，所有开发者和用户才能安全地完成切换。所以整个价值1000多亿美元的生态系统，才能真正完整的运行在信标链上。没有人知道这个项目需要多长时间才能完成，这是一个很大的未知数。而这些未知可能是以太坊2.0转换的巨大阻力。所以我们乐观的认为，PoW链至少可以持续挖掘两到三年。

链乔教育在线旗下学硕创新区块链技术工作站是唯一获批&quot区块链技术专业&quot&quot智慧学习工场2020-学硕创新工作站&quot由中国教育部学校规划建设发展中心实施。专业站立足于为学生提供多元化的成长路径。推进产学研改革&#039；构建应用型、复合型人才培养体系。

感谢您阅读本文，本文详细介绍了以太坊为什么要进行PoS。如果你不&#039；我对以太坊了解不够。如果你想进一步了解以太坊为什么要进行PoS，可以在本站首页搜索你想了解的内容！