作为虚拟货币行业的人，我们经常会谈到以太坊奖是关于什么的，有很多细节需要注意。你知道以太坊街区奖是怎么计算的吗？今天就让边肖告诉你吧！

ETH是采矿产生的。平均每13秒生成2个块。采矿时，矿工用计算机计算一个函数计算问题的答案，直到一个矿工计算出正确答案，即完成该块的装箱信息，第一个计算出来的矿工将获得2ETH奖励。

如果矿工A首先算出正确答案，矿工A将获得以太坊奖励，并在全网广播告诉所有矿工&quot我已经算出了答案&quot并且让所有正在答题的矿工验证并更新正确答案。如果矿工b算出了正确答案，然后其他矿工会停止当前的解题过程，记录正确答案，开始做下一道题，直到算出正确答案，一直重复这个过程。矿工&#039；s角色

矿工在这个游戏中很难作弊。他们可以&#039；不要掩饰他们的工作，得到正确的答案。。这就是为什么这个解决问题的过程被称为&quot工作量证明&quot(POW)。

每隔12-15秒，矿工就会挖出两块。如果矿工挖的太快或太慢，算法会自动调整题目的难度。出料速度保持在13秒左右。

矿工获得这些ETH币是随机的。挖矿的收益取决于投入的计算能力，也就是说你的电脑越多，你答对的概率越高，越容易获得区块奖励。

与所有区块链技术一样以太坊使用基于激励的安全模型。网络中任何声称是挖掘者的节点都可以尝试创建和阻止验证区域。世界各地的许多矿工正在同时创建和验证区块。

一、以太坊采矿的基本原理

1。像所有区块链技术一样，以太坊使用基于激励的安全模型。网络中任何声称是挖掘者的节点都可以尝试创建和阻止验证区域。世界各地的许多矿工正在同时创建和验证区块。。每个矿工提供&quot证据&quot通过把积木送到区块链来研究数学机制。这个测试类似于一个保证：如果这个测试存在，这个块必须是有效的。

2。对于要添加到主链的块，矿工必须提供这个&quot测试&quot比其他矿工更快。。通过&quot证明&quot矿工提供的数学机制，每个块的确认过程称为工作测试。确认新区块的矿工会获得一定的奖励。什么是奖励？以太坊使用固有的数字令牌——以太坊作为奖励。每当一个矿工尝试一个新的区块。，会生成一个新的以太坊

，提供给矿工。

二、以太坊与比特币的区别

1。相似之处：比特币和以太坊都是成功的区块链技术应用。人们通过比特币了解区块链技术。穿过伊泰广场人们意识到区块链可以独立。所有这些都建立在区块链的基础上，在这里交易被公开记录，货币和资产交易更加方便和优惠，繁琐的中间人被取消。

2。区别：比特币是一种去中心化的点对点数字支付系统。，类似于全球结算银行。而且，这家银行不是一个集权组织的成员，它没有CEO，它没有管理员，只有准则的基本原则和共识。没有其他第三方或信托机构从同行那里转移价值。

3。比特币总量2100WW。。每生成21W块，该块生成的比特币数量减半，每10分钟生成一个块。总的来说是通货紧缩的电子货币。以太坊被定义为分布式对等虚拟机。可以理解为利用代币进行价值分配，吸引各方构建生态系统的平台。以太坊的总额没有上限。

三。智能合同和协议ERC20

1。智能合约首先是合约，以代码的形式规定交易双方。，并为合同的执行指定了一些激活条件。一旦这些条件被激活，约定的交易就会自动执行，通常是一些交易。这些交易会被矿工挖掘，最终并入公链，这是不可否认的，也是不可逆转的。

2。以太坊的智能合约基本都是互联网上开源的。任何用户都可以看到相关界面的定义和激活时间。如果没有统一的标准，很多智能合约会让大家难以理解。这个智能合约做了什么？此刻，ERC20协议已经启动。

3。开发人员可以通过查看其他智能合约，然后调用自己的合约，轻松理解相关接口的作用。标准化是非常有益的，这意味着这些资产可以在不同的平台和项目中使用。否则，它们只能在特定情况下使用。

四、为什么以太坊可以用来发币

因为智能合约的存在，合约可以用来安排资金筹集资金，最后存入账户。而且因为0x7D0用的是同一个标准的ERC20，比如直接交换0x7D0和FAD来支持以太坊生态系统，会更容易。

五、以太坊的贸易限制

1。对于每笔交易，交易发起人必须设定交易的气价上限和气价。不同的操作会产生不同的气体和气体成本。矿工完了，矿工就不跑了，用过的气就奖励给矿工。

2。如果一些气体仍然存在。如果用户声明限制值过低或中间账户Eth不足以支付用气费用，则该费用将被返还给交易的发起者或智能合同的创建者。由于气不足，协议将被取消，用于计算的气将不会返回到帐户。

六。网络计算能力是太方全

以太网当前所有矿机的总计算能力，当前矿簇是按照这个值计算的当前块的难度。

七。以太坊提取难度

块的难度用于提高块验证区域的一致性。创世纪方块的难度是131072，之后每个方块的难度都有专门的计算公式。如果校验块比前一个块快，以太坊协议会增加块的难度。通过调整方块的难度，可以调整验证块所需的时间，即突发速度。检查时间的自我调整以恒定的速率继续生成新的fast。

8。单卡计算能力与挖矿收入的关系

单卡计算能力越大，可以进行的检查越多。得到公式结果的概率是，情况越大，提供的股份数越多，如果使用矿组，矿业的收益越大。

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。散列该项中的值以获得结果，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。

以太坊的爆破奖原来是5ETH。2017年10月，拜占庭升级将爆破奖从5ETH降为3ETH，2019年3月，君士坦丁堡升级将爆破奖从3ETH降为现在的2ETH。。除了每块2ETH的固定奖励外，如果该块参考三级块，离开该块的矿工和创建三级块的矿工还可以获得额外的奖励。

以太坊切块平均时间13秒左右。矿工挖出块后，需要向全网广播，广播的过程需要时间。其他节点的矿工可能在接收到广播的新块之前已经挖到了相同块高的新块，导致以太坊暂时分叉。由于去块时间短，以太坊出现暂时分叉的概率很大。为了不影响矿工&#039；对采矿的热情，以太坊系统规定不在最长链上但被最长链上最近的六个块引用的块称为三级块，也可以奖励。

温馨提示：

1。以上信息仅供参考，不做任何建议。

2。投资前，我建议你先了解项目存在的风险，对项目的投资人、投资机构、链条活跃度等信息有一个清晰的了解，而不是盲目投资或者误入资本市场。投资有风险，入市需谨慎。

响应时间：2021年6月29日请以平安银行在官网公布的最新业务变动为准。

[我了解平安银行]想了解更多？过来看看&quot我知道平安银行&quot~

以太坊的挖矿过程和比特币差不多。ETH是由采矿产生的。平均每15秒生成一个块。采矿时，矿工用计算机计算一个函数计算问题的答案，直到一个矿工计算出正确答案，即完成该块的装箱信息，第一个计算的矿工将获得三个ETH的奖励。

如果矿工A首先算出正确答案，矿工A将获得以太坊奖励，并在全网广播告诉所有矿工&quot我已经算出了答案&quot并且让所有正在答题的矿工验证并更新正确答案。如果矿工b算出了正确答案，然后其他矿工会停止当前的解题过程，记录正确答案，开始做下一道题，直到算出正确答案，一直重复这个过程。

矿工很难在这个游戏中作弊。他们可以&#039；不要掩饰他们的工作，得到正确的答案。。这就是为什么这个解决问题的过程被称为&quot工作量证明&quot(POW)。

每隔12-15秒，矿工就会挖出一块。如果矿工挖的太快或太慢，算法会自动调整题目的难度。出料速度保持在13秒左右。

矿工获得这些ETH币是随机的。挖矿的收益取决于投入的计算能力，也就是说你的电脑越多，你答对的概率越高，越容易获得区块奖励。

关于什么是以太坊奖励，以太坊方块奖励如何计算的介绍到此结束。不知道你有没有找到你需要的资料？如果你想了解更多这方面的内容，记得关注这个网站。