最近有很多小伙伴问了关于proofofwork的问题。边肖结合多年的经验整理了proofofwork的一些不足之处，下面有哪些相应的资料与大家分享。

概念验证的本质用一个普通人能理解的话来说，就是用硬盘挖矿。没错，PoW用CPU挖矿(或者显卡和ASIC挖矿机，本质是更强的运算芯片，本质上和CPU一样)，PoS用持币比例挖矿。，DPoS是基于投票来决定超级节点，而PoC是通过硬盘来挖掘。

我们可以这样理解：

——谁的PoW芯片快，谁就容易挖到矿；

-谁在PoS中持有更多的钱？，谁容易挖到矿；

-谁在DPoS中获得的票数多，谁就能成为挖矿的超级节点；

-在PoC中，谁的硬盘容量大，谁就容易挖矿。

够简单明白吗？

要了解PoC的具体原理，还是得从比特币PoW说起(研究区块链，PoW是一个你永远绕不开的技术概念)。

PoW全称是工作证明，即工作量证明。这里所谓的工作量，是矿工&#039；sCPU(或者显卡，ASIC芯片，我们之前说过，这些硬件只是速度更快，本质和CPU没什么区别)来执行一种叫做哈希算法的计算。简而言之，谁能在单位时间内执行更多的哈希计算？谁有更大的机会产生满足要求的散列结果，然后获得写入区块链的权利。

可以说比特币PoW的本质是争夺矿。每一个新区块的出现都是给矿工一个&quot难题&quot，和矿工通过计算能力竞争。谁能找到&quot回答&quot那先符合要求。矿工通过购买牛逼的计算芯片，持续消耗电能进行高频高强度的哈希计算，获得更强比例的计算能力，进而获得更大概率找到&quot回答&quot。如果一个比特币矿工拥有全网20%的计算能力，理论上可以挖掘出20%的新区块，获得20%的区块奖励(最初每个区块有50个比特币奖励，现在减少到12.5，明年继续减半)。

PoW挖掘规则简单粗暴，计算能力可以自由进出，因此可以建立足够的安全性，保证区块链不被篡改。这也是为什么虽然技术看似简单，但比特币却能成为币王，约占市值的一半。

另外，、比特币叉币(如BCH、BSV)、莱特币LTC、以太坊ETH、门罗Monero、Dash都是使用PoW机制挖矿的货币，但这些货币在一些技术参数上可能与比特币不同。但大体思路都差不多。

我们今天的主角PoC和比特币PoW类似，但是有一些实质性的区别。我们知道比特币的威力需要矿工不断重复地进行哈希计算。矿工需要高强度运行他们的计算芯片，消耗相当大的电力资源。

我们的PoC开辟了一条非常巧妙的途径：它需要矿工事先计算出大量的hash结果，并将这些数据存储在硬盘中；采矿时，矿工们也在争先恐后地解决&quot难题&quot不同的是，对&quot难题&quot应该在硬盘中找到数据，而不是实时计算。自然，谁的硬盘容量越大，谁的硬盘容量就越大。备选答案&quot提前存储。谁更有可能找到&quot正确答案&quot可以与&quot难题&quot。

可能有人会问，在PoC的这种机制下，矿工有没有可能通过芯片计算答案来作弊？不会吧。PoC的算法设计决定了它何时寻找&quot回答&quot它对存储空间非常敏感，但对芯片的计算能力不那么敏感。强大的计算能力并没有给矿工的成功率增加多少&#039；挖矿，但是有更多的存储空间可以让挖矿的成功率翻倍。PoC的这一特性也被形象地称为&quot空间换时间&quot。

POW是工作证明的简称，中文翻译是工作量证明，是一种去中心化、开放透明、不可篡改的算法机制。比特币基于POW共识算法，已经安全平稳运行了10年。。目前ETC也采用这种算法机制，通过计算功率来挖矿可以获得奖励。

详细

证明

直接翻译过来就是&quot详细证明&quot。

相关

工作

经历

指相关工作经历。所以如果你想写你以前在相关行业做过什么，你&#039；最好写上你对这项工作的熟悉程度。

proofwork的优势：

1。机制本身当然很复杂，还有很多细节，比如：自动调整挖掘难度，分块奖励逐步减半等。这些因素基于经济学原理，能够吸引和鼓励更多的人参与。

2。理想状态，这种机制，可以吸引众多用户参与其中，尤其是先获得的越多，将推动加密货币初期的快速发展和节点网络的快速扩张。在Cpu挖矿时代，比特币吸引了很多人参与&quot采矿&quot，就是一个很好的证明。

3。相对来说，发行新硬币是公平的。采矿&quot并将比特币分发给个人。

缺点：

1。计算能力由计算机硬件(Cpu、Gpu等)提供。)，耗电，是直接消耗能源。与人类追求节能、清洁、环保的理念相悖。然而，如果我们必须找到&quot货币价值&quot对于&quot加密货币&quot，那么这方面应该是最有力的证据。

2。随着这种机制的发展，提供计算能力的不再是简单的CPU。而是逐渐发展到GPU，FPGA，甚至ASIC矿机。用户也从个体挖矿发展到大型矿池、矿，计算能力的集中越来越明显。这与去中心化的方向背道而驰，渐行渐远，网络的安全也逐渐受到威胁。有证据表明Ghash(一个矿池)曾经对赌博网站进行过双花攻击(简而言之，一笔钱花了两次)。

3。比特币块奖励将每四年减半。当开采成本高于开采收入时，人们&#039；美国人对采矿的热情会降低。计算能力会降低很多，比特币网络的安全性进一步堪忧。

PoC是能力证明的缩写，翻译成中文就是能力证明。顾名思义，它是一种通过存储容量的大小来确定块生成权限的算法。。PoC共识机制用更通俗的语言来表达，就是用CPU和GPU来预算一堆彩票号码，然后填满硬盘。挖掘就是找到中奖的彩票号码。

目前，大部分数字货币&#039；s矿用PoW(工作量证书)。.OnlyBurst,BHDandNewbyuseconfirmatorytest(abbreviationofProofofConcept)consensusmechanismtoprovetheirwork

bilingualexampleworkproof.

工作量证明

proofofwork是很多人头疼的事情，尤其是在认识和现实的冲突中。proofofwork的以下哪个缺点也面临类似问题？关注我们，为您服务，是我们的荣幸！