到底甚么是比特币矿机？这是两个须要许多层级认知的难题。SHA-256基元演算法的概要说明当你输出公钥来弹出你的智能手机或你的笔记型电脑时，公钥有效率原因在于它相关联的是身份验证痛点的惟一解。使当代公钥学（Budaun不利因素身份验证）安全可靠的是，即便没人赢得了基元前或基元后公钥的出访权，也极难赢得适当的公钥。正像你在上面看见的，两个单纯的3位数的数组 “abc “相关联的是两个基本上难以认知的数组。SHA-256的组织工作基本原理是将两个任一宽度的数组，切换为64位数的基元值。输出能是3位数，也能是300个，即使是3000位数。而结论依然是两个64位数的基元值。

单纯来说，当找到两个解时，比特币被认为是挖出来了。它是两个64位数的数组，并且每位数有36个可能的输出。26个字母和10位数字。因此，这就是36^64个输出。

经过856,192,328次的尝试，找到了正确的解。而这个难题通过使用两个已经被证明包含解的区块，已经被大大简化。在绝大多数情况下，解是不存在的。基元率现在我们对甚么是基元有了两个大概的了解，我们能把这个概念进一步扩展到两个被称为基元率的指标。这只是比特币在全球范围内被开采的速度。根据CoinDesk的数据，截至2021年9月6日的基元率约为89 Exa Hash /秒（EH/s）。由于比特币使用SHA-256演算法，每个基元值产生的信息占据了256比特的内存。比特币今日价格信息和能源之间的联系以下关系是由鲁道夫-
兰道尔在1961年提出的，当时他是IBM的研究科学家。

毁灭（或创造）两个信息包所需热量的下限。其中k_B是玻尔兹曼常数，T是系统的温度，单位是开尔文。当代计算机的能源效率大约降低了100万倍。比特币的能源消耗让我们做一些近似的计算，根据到目前为止讨论的数字，尝试计算一下当今世界上比特币能源消耗的大致数字。我知道这很可能严重偏离了目标，但请允许我尝试。1. SHA-256基元值产生256位。每个基元值的最低理论能耗是256 K T ln2。

因此，每个基元值的热量成本至少是7.30/10^19焦耳。2. 算上10^6的热量成本。每个基元值的热量接近于7.30/10^13焦耳。3.核算巨大的尝试次数这个例子花了856,192,328次尝试才得到两个正确的基元值。因此，这就是：每个正确的基元值为6.25/10^4焦耳。

4. 现有的基元率是89EH/s。因此，这是89×10^18每秒的基元值。比特币今日价格我们得出的全球能源消耗率为5.56×10^16瓦。作为参考，两个中等规模的核电站能产生大约1GW的热量。