在密码学货币领域，确保比特币及其它密码学货币网络安全的基础硬件和挖矿活动是一个经常被人忽视的市场。然而，挖矿与交易结合起来，是创造可观利润的核心市场之一。

在这篇文章中，我将分享比特币及其它密码学货币挖矿领域的概况、支撑挖矿的基础硬件、行业的生态，并深入探究这个领域的收益和市场规模。

如何进行密码学货币挖矿

工作量证明（挖矿）是指将新交易添加到比特币区块链上、并对这些交易的合理顺序达成一致（共识）的过程。

关于这个过程，我最喜欢的一个类比就是把它想象成一个数独谜题（译者注：需要在一个 9*9 的盘面上根据已有的数字推演出其它数字，保证每一行、每一列、每一个粗线设置的九宫格内的 1~9 都不重复）。它是一个需要烧死大量脑细胞才能解出来的难题，但是一旦解出来了，其他人就很容易验证你的答案是否正确。

下面的这个视频提供了一种非常棒的可视化展现，可以帮助我们更直观地理解区块是如何被创建和连接在一起，交易又是怎样被打包进区块中的，以及挖矿如何在这一过程中发挥核心作用：

视频：区块链 101 - 一个可视化演示

从本质上来说，矿工（地理上分散在世界各地的计算机）相互竞争着解决一个计算密集型的难题，一旦解出来就可以确证区块链上可（连带打包在区块中的交易）产生下一个区块。第一个解决难题的矿工可以获得区块奖励（“coinbase奖励” +交易手续费）。一旦新区块被创建，网络中的所有矿工都可以验证该区块的正确性，然后进入到解决下一个区块难题的竞争中。

矿工在比特币和区块链生态系统中扮演的角色

世界各地竞争着解决下一个难题的所有计算机都是挖矿生态系统的参与者。可汇总的计算资源是为比特币提供基本安全保障的核心要素之一。

通过这个网络，比特币的使用者们可以期望：

他们的交易将被比特币区块链所确认。

他们的交易将按照合理的顺序被打包（防止一笔钱花两次）。

比特币区块链的历史将保持不变（不可篡改性）。

作为回报，矿工可以同时获得新挖出的比特币（“Coinbase 奖励”）和区块中每笔交易的手续费。如果用户希望自己的交易被及时打包到比特币区块链上，他们可以自愿增加为自己的交易所支付的手续费。

用于挖矿的硬件

在比特币网络的早期，使用消费级的 CPU 挖比特币还有利可图，然而，比特币网络发展到如今的规模，再这样做已经不切实际了。

目前，比特币生态系统内的矿机由专用集成电路（ASIC）主导。对于其它绝大多数密码学货币而言，图形处理器（GPU）和现场可编程门阵列（FPGA）是主要的矿机形态。还存在许多和比特币使用同一种哈希算法（SHA256）的密码学货币，它们也兼容比特币的 ASIC 矿机。

芯片	定义	挖矿算法	例子	备注
ASIC	芯片组被优化为适合执行一项特定的功能（SHA256）。	SHA256	蚂蚁矿机 S17、阿瓦隆矿机、神马矿机 M20S	尽管 SHA256 是最主要的挖矿算法，然而 ASIC 矿机可以被设计成适用于任何挖矿算法。
FPGA	芯片被设计成可由用户重新编程。	可以被编程为执行任意挖矿算法。	赛灵思 VU9P、BittWare CVP-13、Blackminer	对 FPGA 进行编程和设置都极为困难。
GPU	芯片被设计成适合进行重复计算（通常是视频和图形计算）。	Ethash、Equihash、Cuckaroo29、等。	英伟达 2080Ti、AMD Radeon VII	GPU 适合用来挖除比特币以外的大部分密码学货币。
CPU	芯片被设计成适合执行普通用途的计算任务。	CryptoNight	AMD Ryzen 1050X	虽然最初可能可以使用 CPU 进行挖矿，但如今这样做通常已经无利可图了。

挖矿生态系统的景观

下面是一张从芯片到终端用户的挖矿生态系统全景图：

代工厂

台积电（TSMC）和三星是两家核心的半导体制造商，它们生产了所有挖矿硬件所采用的硅晶片。尤其是台积电，它在芯片组供应链中占据了主导地位。

举例来说：英伟达、AMD、赛灵思（Xilinx）、比特大陆和嘉楠耘智全部使用台积电作为其核心生产线。

公司	市值	客户	备注
台积电	320 亿美金	英伟达、AMD、赛灵思、比特大陆和嘉楠耘智	在更先进的芯片设计（7nm）中处于领先地位。
三星代工厂	2,200 亿美金*	穿山甲矿机（神马矿机）	

* 三星代工厂隶属于三星电子

打包，测试，组装

晶片生产出来之后，你需要对它们进行测试，切分，并把它们封装进最终的芯片中，然后重新测试。整个流程通常由 OSAT 公司（外包封装测试公司）处理，其中最大的两家公司是 ASE 集团（台湾）与 Amkor Technology。

公司	市值	客户	备注
ASE 集团	180 亿美金	英伟达、AMD	总部位于台湾
Amkor Technology	18 亿美金	不详*	总部位于美国
硅品(SPIL)	40 亿美金（被收购）		被 ASE 集团以 40 亿美金收购

* 绝大部分集成电路公司都没有披露它们的 OSAT 供应商。

集成电路设计与制造商

设计和销售芯片的公司通常被称为无晶圆芯片公司（制造本身由代工厂和 OSAT 公司负责）。

对于 GPU 而言，最顶级的两个制造商是英伟达和 AMD。而对于 FPGA 而言，最顶级的制造商是赛灵思。对于专门用来进行密码学货币挖矿的 ASIC 芯片而言，最顶级的三家制造商则是比特大陆，嘉楠耘智，和穿山甲矿机（Pangolin Miner）（神马(Whatsminer)矿机系列的制造商）。

除了这三类制造商之外，这个行业中还有一些其它的集成电路设计公司，包括：翼比特，芯动科技，Bitfury，Obelisk，以及其它的一些公司。

公司	市值	市场份额	备注
英伟达	1,010 亿美金*	约 70% 的 GPU 市场**	市场包括游戏、数据中心、可视化、以及汽车
AMD	330 亿美金**	约 18% 的 GPU 市场**	
比特大陆	150 亿美金***	约 20% 的 ASIC 市场	刚刚发布他们最新的 7nm 机器——蚂蚁矿机 S17。
嘉楠耘智	10 亿美金***	约 40% 的 ASIC 市场	刚刚发布他们最新的 7nm 机器——阿瓦隆 A9。
穿山甲矿机（神马矿机）	不详	约 20% 的 ASIC 市场	聚焦于 16nm 的 ASIC 矿机。

* 英伟达和 AMD 为所有的用例生产 GPU，而不仅仅是挖矿。

** 市场份额来自 Jon Peddie Research 的估计。

*** 在比特大陆和嘉楠耘智赴港交所上市失败后的最后估值。

**** 估价基于和大矿工的交流和早前的 IPO 申请。

矿工和矿场

芯片被生产出来之后，就可以用来挖密码学货币啦。ASIC
芯片被设计成专门挖一种挖矿算法（通常是 SHA256 或者说比特币），而 GPU 则更具灵活性。

矿工包括：使用一台机器进行挖矿的人，小型挖矿作业（5-10 台机器），中等规模的矿场（10-100台机器），大规模矿场（100-1,000台机器）到工业规模的矿场（1,000
台以上机器）。迄今为，我听说过的最大规模的矿场在多个地区运行了多达 100,000 台矿机。

除了设计芯片以外，一些制造商自己也参与挖矿（例如比特大陆，嘉楠耘智，穿山甲）。举例来说，比特大陆每个月都公开披露他们自己的挖矿状况。

大大小小的矿工都可以加入到一个矿池（将在后文详细介绍）中，如果矿场的规模足够大，他们还可以 solo 挖矿——
只汇集自己的哈希算力来直接寻找区块，不与其他矿工混合算力。

* 一个颇有争议的地方在于，挖矿芯片的制造商在出售芯片之前，可能会提前使用它们进行挖矿。然而，如果你真的有一台能产生利润的设备，你也没有理由把它闲置在仓库里，你也可能会在卖出去之前用它来挖矿。

矿池（单币种和多币种）

对于从个体到非工业级别的矿工来说，在经济上更加合理的做法是加入一个矿池，而非自己单独挖矿。矿池把许多矿工的哈希算力汇集了起来，使得每个矿工的回报曲线能够更加平滑。矿池负责优化所有的哈希算力、运行挖矿程序、收集并分配奖励，并对这些服务收取额外的费用。

有一些矿池专注于挖特定的密码学货币（例如星火矿池，专注于以太坊和 Grin），而其他矿池则设置了多种矿池，覆盖了所有主流的密码学货币（蚂蚁矿池，鱼池，币印矿池，Slushpool，等等）。所有的这些矿池一开始都是专注于挖一个密码学货币（通常是比特币），后来才扩展到涵盖所有形式的密码学货币。

关于矿池的运行方式，我最喜欢的一个类比是将它想象成办公室的彩票池。通过把所有人买的彩票汇集到一起，每个人（矿工）都有更大的机会赢得奖励。

然而，使用矿池就意味着要信任矿池 —— 每个人拥有的准确算力份额以及合理的收入，都由矿池来记录并分发。为了提高透明度，有一些类似
PoolWatch的服务会跟踪和比较各种矿池的报告。

矿池	市场份额	所挖的密码学货币	备注
蚂蚁矿池	34%的比特币算力	BTC、BCH、LTC、ZEC、ETH、以及其它密码学货币。	比特大陆旗下拥有蚂蚁矿池和BTC.com 矿池，因此将它们合并在这一栏。
鱼池	13%的比特币算力	BTC、LTC、ETH、ZEC、Grin、XMR、以及其它密码学货币。	
币印矿池	9% 的比特币算力	BTC、BCH、BSV、ZEC、LTC、以及其它密码学货币。	
Slushpool	8% 的比特币算力	BTC 和 ZEC	
星火矿池	25%的以太坊算力	ETH、Grin 、Beam	

算力市场

矿工除了直接挖矿以外，还可以把自己的算力卖给别人。现实中也是有这样的算力买卖市场的——目前最大的市场是
NiceHash。除此以外，还有一个更小的点对点的算力市场：Mining Rig Rentals。

在这些市场中，人们可以同时出售他们的算力 和/或 购买算力——任何密码学货币的任何算法都行。尽管人们购买算力的原因很多，然而其中最主要的一个原因就是购买算力是一个拥有密码学货币的入口。

很多时候人们使用算力来炒作各种密码学货币——例如，想要采购适合 SHA256 的哈希算力来挖 BSV 而不是比特币（实在是一笔不划算的买卖…）

云挖矿

云挖矿即直接买卖的算力合同，消费者无需接触任何硬件。有点类似于上面提到的

算力市场，通常是由一个中心化的供应商来运营的。

这个领域中最大的两家公司是 Genesis Mining（美国）和Bitdeer(亚洲)。也与上面提到的类似，人们使用云挖矿服务的一个主要的原因是购买算力被当成获取密码学货币的一种入口。通过这种方式，人们可以使用法币来直接购买比特币或其他密码学货币，而不用通过交易所。

智能矿工

智能矿工是最近出现的一个新的品类。挖矿是一个复杂的任务，它要求参与者了解硬件，网络，能源，算力预测，以及针对特定算法的优化等等。此外，随着新的密码学货币不断涌现以及旧的密码学货币的消亡，所有的这些因素每天都在不断地变化。

像 Honeyminer这类智能矿工软件，旨在同时优化上述所有的因素，使得普通的消费者和专业人士都可以通过拥有的算力尽可能多地挣取收益。另外还有两个类似的产品——HashFish和Cudo Miner。

在短时间内，这些产品在供应端聚集起了可观的算力。

挖矿市场的规模和收益

以年为单位计算，密码学货币挖矿行业每年创造超过 80 亿美金的利润。

在所有基于工作量证明的区块链中，利润来自区块奖励和每个区块中包含的交易手续费。根据 CoinMetrics在 2019 年 6 月 25 日公布的最新的挖矿奖励数据，下面是挖矿行业每周，每月，以及每年的挖矿收益。

资产	挖矿周收益	挖矿月收益	挖矿年收益
比特币	13,900 万美金	55,600 万美金	660 亿美金
以太坊	2,800 万美金	11,200 万美金	130 亿美金
莱特币	1,400 万美金	5,600 万美金	67,200 万美金
比特币现金	500 万美金	2,000 万美金	24,000 万美金
ZCash	400 万美金	1,600 万美金	19,200 万美金
合计	18,600 万美金	14,400 万美金	890 亿美金

在密码学货币挖矿的世界里，比特币仍然占据主导地位，仅仅比特币网络本身就创造了 75% 的挖矿收益。

这也与今天（2019 年 7 月 1 日）比特币占据主导地位的市场份额相符合。根据 CoinMarketCap 的数据，比特币占据了 60% 的市值。

然而，挖矿行业创造的整体利润与其所挖密码学货币的价格直接挂钩，所以它会反过来直接影响密码学货币市场（因此，华尔街很难理解这个行业里的公司）。下面将详细介绍。

理解挖矿行业的盈利情况

挖矿行业参与者的整体利润，成本，和盈利情况受到少数几个关键因素影响。

资本支出（Capex）

矿工主要的资本支出是挖矿机器本身的成本加上运营该机器需要的所有设施/建筑物。

举例来说，如果你想要按照零售价采购 10,000 台最新的比特大陆生产的蚂蚁矿机 S17，需要花费 1,600 万美金。大型矿工可以特价采购。然而，当矿机的需求很高以至于很难保证供应时，价格的优惠力度会很小。

这还没有把建设设施的成本考虑进来，这些设施将挖矿从业余爱好变成真正专业的工业规模项目。

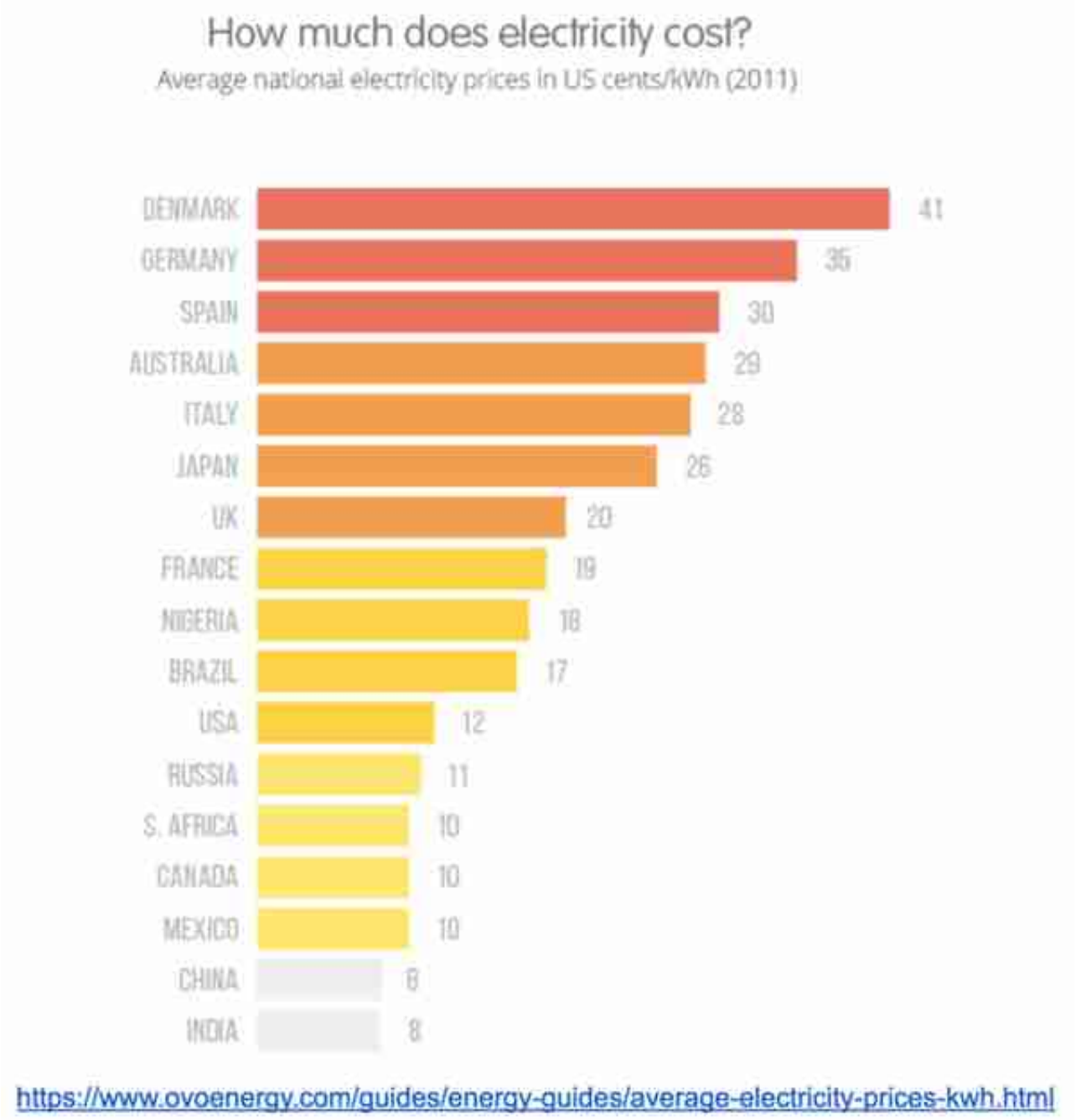
Photo of the HyperBlock mining facility https://www.hyperblock.co/

运营成本（Opex）

对于矿工来说，主要的运营成本是每天运行矿机所需的电费。

举例来说，如果你 7*24 小时地运行 10,000 台比特大陆的 S17 矿机，按每度（kwh）电 0.05 美金计算，每天将会花掉你 36,000 美金（每年大约 1,300 万美金）的电费——仅仅是支撑矿机运行而已。

电费的平均支出视矿机所在地域和所用电力来源而定，差别很大：



矿工的本性激励他们去寻找世界上最便宜的能源，这就是为什么 Coinshares 估计支撑比特币网络运行的 75% 的电力来自可再生能源，主要就是水力发电。

除了维持矿机运行所需的电费以外，其它不间断的运营成本还包括：散热，人工，维护，安全和普通设施运营。一般来说，可以粗略地估计不间断的运营成本是电费的 1.5 倍。

根据我们上面关于运营 10,000 台比特大陆的 S17 矿机的例子，可以粗略地估计其成本为：

1,600 万美金的资本支出 + 300 万美金（进口税）+ 400万 美金（设施+安全）

2,000 万美金的运营成本（每年）

6,700 万美金的潜在收益（基于今天的比特币价格）

以上只是一个粗略的估计，仅仅是为了展示矿工需要付出的各种成本的规模。真正的成本将完全取决于你所处的地理位置和所用建筑等。

然而，由于我们下面将介绍的市场因素，上述成本将不断变化。

市场因素

尽管资本支出和运营成本是两项矿工可以控制的因素，但市场的力量在很大程度上决定了挖矿的盈利情况。

矿工成本 & 可见的供给

与很多传统的产品不同，矿机制造商（比特大陆，嘉楠耘智，神马矿机等等）会根据矿机的盈利情况（比特币价格）来调整矿机的价格。

当密码学货币的价格出现大幅拉伸时，矿机本身的价格也会随之剧烈波动。疯狂时期，整个二级市场都在抢购更多的矿机，即使是老的矿机也能咸鱼翻身。

总的来说，我总是希望机器的定价能接近在那个时间点可以创造的公允价值。

除此之外，矿机的供用往往是比较受限的，尤其是比较新的矿机。继续拿上面提到的比特大陆的 S17 矿机为例，这些机器已经被抢购一空了。与团队中一些人交流时，他们告诉我，他们并不指望在 11 月初以前能保证充足供应。

算力

矿工获取下个区块打包权的机会与他们的算力占整个比特币网络算力的比重成正比（为了简单起见，使用比特币来进行说明）。

用最简单的例子来说明，如果你作为一名矿工，拥有的比特币算力占全网算力的 1% ，那么你就可以期望自己从比特币网络获得总奖励的 1%。

不过，比特币网络的总算力总是处于不断变化之中，因此每个矿工的盈利情况取决于有多少矿工加入或离开这个生态系统。比特币协议有一套内部的方法来调整挖矿难度。

比特币价格

因为区块奖励是直接以底层的密码学货币支付的。举例来说，如果你在挖比特币，那么你赚到的区块奖励就是用比特币来支付的。因此，奖励的价值与比特币本身的价格直接挂钩。

比特币越值钱，挖矿的奖励就越值钱。要从事挖矿行业，你必须发自内心地看好你所挖的密码学货币，因为你的盈利情况取决于它。

比特币在所有密码学货币（除第一名之外）中占据主导地位的主要原因之一就是它透明、开放而公平的发行计划。从创世区块开始，比特币就有一个固定的发行计划，规定了它发行的上限——最多只会有 2,100 万枚比特币被创造出来。

挖矿是创造比特币并将其流通到全世界的一种方式，今天每个比特币的区块奖励是 12.5 个比特币；然而，这个数量随着每挖出每 21 万个区块就减少一次。当第 63 万个区块（估计是在 2020年 5月 24 日左右）被挖出来时，区块奖励将减少到 6.25 个比特币——这也被称为减半事件。

想要了解之前的减半事件是如何影响比特币和其它密码学货币网络的，请查看这篇来自 CoinMetrics 的非常棒的文章，他们梳理了以前的减半事件。

如果你想更进一步了解比特币的发行计划，以及当比特币都被挖完以后会发生什么，请参阅这两篇关于比特币发行和总体安全预算的文章（为Dan Held带来的全面报道打 call）。

一句话总结 ——
比特币的价格和比特币的基础发行计划极大地影响了挖矿本身的盈利情况。

我的主要收获

在对密码学货币的挖矿领域进行深入研究之后，以下是我最大的收获：

我们往往忽视了挖矿行业和基础硬件在区块链网络中扮演的重要角色。

算力 = 密码学货币 = 金钱。对于许多人来说，算力是进入加密世界的关键。

正如我们看到比特币的金融化一样，我预测我们将看到算力也会类似地金融化。

如果你是在这个领域内开办算力市场，交易所，提供金融产品，或任何与挖矿行业有关服务的企业家，我很乐意和你交流。可以在我们基金的网站上找到我的联系信息：Proof of Capital。