迈向光学工作量证明体系

Michael Dubrovsky[1], Bogdan Penkovsky[1], Lucianna Kiffer[2], Marshall Ball[3], and Jiabeiwei Chen[4]

[1]PoWx, Cambridge, MA, USA. Email: mike@PoWx.org, bogdan@PoWx.org
[2]Northeastern University Boston, MA and DAGlabs Tel Aviv, Israel. Email: lkiffer@ccs.neu.edu
[3]Columbia University, New York, NY, USA. Email: marshall@cs.columbia.edu
[4]Translated this paper to Chinese, Email: u3523278@connect.hku.hk

[摘要] 当前虚拟货币使用的 PoW（工作量证明）生态系统需要依赖大量的能源，才能使其在一个类似于去中心化，同时较为安全的环境中运作。然而，虚拟货币挖矿能源成本逐渐升高，不良影响随之而来。此论文提出一个通过改良 PoW 算法，获得为能量高效性光学辅助处理器量身定制的 oPoW（光学工作量证明）算法，从而来减轻虚拟货币对能源的依赖。维护改良版系统中虚拟货币挖矿的安全性依然是高成本的，但是 oPoW 所需成本集中来源于资本支出（CAPEX）。oPoW 算法对哈希函数进行微小修改，因此继承了哈希函数的大部分特性，包括 SHA 哈希方程的安全性。oPoW 新添加的函数功能选择建立于如下假设之上：对于此特定函数，相较于其他专用集成电路（ASIC），光学辅助处理器能（PIC）够进行低耗能高速度的计算。作者将提供该系统的大体理论框架，以及一个特定的实例来展示如何实现 oPoW 算法的运用。作者接着用实证进一步支持其主张，还会介绍一个硬件样板的安装程序，及其工作原理。

该论文是第一个提出用以 PoW 为基础的改良模式来改善比特币高耗能系统的研究成果。除了降低能源消耗，oPoW 相较于其他现有的方案拥有更多的优势：地理位置上实现更高程度去中心化，挖矿民主化，挖矿不受审查机制影响，哈希率稳健增长，以及为现代模拟计算提供一个新的运用方向。

目录

第 1 章 导论

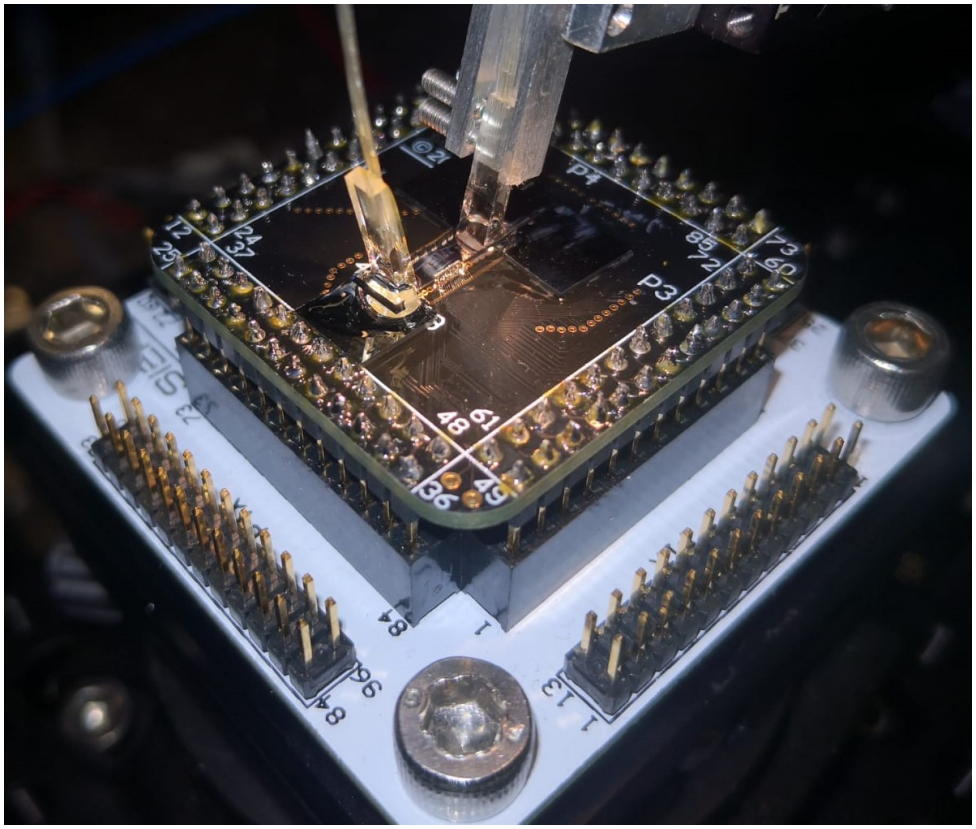


图 1-1 oPoW 硅光学挖矿机样板

大众虚拟货币网络，例如比特币，最主要的功能在于维持一个去中心化的，电子化的分类账来记录交易。实现此功能的关键在于该分类账的内容不需要受任何权威机构，如银行，的控制和证实来实现效力。此类网络的一个简单的设计如下：用户通过电子签名（公众密匙）公开发布交易内容，只有当大多数网络节点承认该交易有效性，该交易才被视为完成。然而，交易网络要真的做到不需要信任/许可机制，同时又能不受不良主体操控，一个能够防止女巫攻击[1] 和双重支付[2]的机制是必不可少的。

尽管过去有不少在电子现金系统内解决这些问题的尝试，比特币的构架（参考 Nakamoto 白皮书[1]）通过巧妙利用哈希现金[2] 工作量证明体系（*PoW*），成为第一个真正解决双重支付和女巫攻击两大问题的网络构架。Nakamoto 的关键点在于，工作量证明体系要求分散式系统内的每个节点证明已证明者完成的工作量使其生效，而此证明所需成本非常之低；同时，他新增了虚拟货币分发机制——各节点能用工作量换得虚拟货币奖励。在此基础之上整个系统能达成一个先前难以实现的拜占庭协议[3]。这样的系

[1]多个节点被一个不良分子控制。

[2]重写分类帐把第一个交易删除，从而用同一个币进行两次付款交易。

统随即见证了比特币及其他虚拟货币的诞生和惊人扩张，实现前所未有的全球化财产自由和财产权保护变得大有可能。

1.1 工作量证明在区块链中的应用

工作量证明体系，也称为定价函数，最初由 Cynthia Dwork 和 Moni Naor 向 Crypto 1992 提出，目的是解决垃圾邮件[4] 等一系列问题。“工作量证明” 其实是指找到一个具体计算难题的解答，此难题不可避免地需要一定计算工作量来完成，因此找到解答即能证明工作量。这样的难题被称为密码学谜题，这些谜题设计使得找到其答案必须通过强力计算法——试验每一个可能的解答直到找到有效答案。此设计同时保证答案很难被找到。解答这些密码学难题在虚拟货币的领域通常被称为*挖矿*，因为找到有效答案的节点能获得奖励（区块奖励）。另一方面，证实某被提出的解答是否真的有效非常简单，只需要进行一轮评估计算。因此，工作量证明能证实此节点付出了一定计算工作量来找到答案，且此答案能被其他节点轻易确认有效。

在比特币网络中，交易被记录在*区块*上，一系列互相连接的区块被称为*区块链*。当某*挖矿机*将交易记录整合成一个区块后，立即开始在此区块中验证随机筛选的特定输入值（*nonce*，一次性随机数值），直到此区块的加密哈希函数值小于一个先前定义的临界值[3]此哈希函数的安全性质使挖矿机不得不强力试验所有可能的 nonce 直到一个符合要求的区块被找到。此符合要求的区块包含了这个密码学难题的解答，所以其本身就是工作量证明。此区块一经公布，任意节点可以通过评估计算区块哈希值看它是否真的小于定义临界值，轻易验证该工作量证明是否有效。比特币使用的是哈希函数 SHA-256（NIST），但多种不同哈希函数也被采用与其他区块链网络中。不同类型的哈希函数对挖矿机电脑处理器和内存有不同工作量要求，但都遵循相同的原理。例如以太坊采用的哈希函数 Ethash，对内存有更高要求[5]。

因此，一条区块链的有效性建立在先前进行的计算工作量有效的基础上。这也意味着，最长的区块链即代表最大工作量，也被自动认可为有效的交易历史纪录（因为最大部分的计算量都被花费于建立此区块链）。修改任何一个区块需要大量的计算量[4]，没有超过整个系统一半的计算能力是不可能实现的（因此被称为 51% 攻击，详见 2.4）。再者，双重支付也是不可能实现的，因为在两条新建立的区块链中只有最长的那一条被视为有效。工作量证明也被采用于更加复杂及高产量（以每秒产生的交易量计算）的去中心化分类帐中，这些区块以有向无环图（DAG）的形式存在[6-7]，而不是简单的链条状。PoW 体系在其运用过程中的良好记录证明，保证了比特币网络中交易不可逆这一特性。然而，PoW 体系面临着规模难以扩大的严峻问题，这最终可能会限制比特币的发展。

[3]系统会自动调整这个极限值从而实现大约每十分钟只有一个区块能被挖到。举个例子，一个 SHA256 哈希函数输出为 256 个位元，如果难度设定要求挖矿机必须找到某 nonce 值使得区块哈希函数输出的头 40 位元均为 0，则找到这个 nonce 值要求挖矿机进行 2^{40} 次试验。

[4]被修改区块之后的所有区块要求的工作量证明全部需要重新计算。

1.2 比特币工作量证明生态系统面临的挑战

比特币在过去十年，从一个由爱好者构成的小规模网络发展到全球性虚拟货币网，它所依靠的 PoW 体系并未有任何更新。最初它被设想为一个全球化去中心化网络（“每个 CPU 代表一个投票权”），而如今绝大多数比特币交易账目记录落于一小部分挖矿公司手上。随着挖矿奖励市值的升高和挖矿机之间更加激烈的竞争，比特币挖矿难度以指数函数增长，使得挖矿产业更加工业化。PoW 体系不断增长[5]的巨大的能量需求，导致挖矿产业地理位置上的集中化——挖矿机集中处于建立在电力成本低区域的大型数据中心，这让很多小型挖矿公司难以加入竞争。

比特币挖矿能量消耗随着其市值升高稳健增长。虽然目前确切的数值存在争议，其能耗如今估计达到每年 75 太瓦时[8]，电力需求甚至超过奥地利整个国家[9]。因此，比特币挖矿机规模越大，其利润就越高。实际上，只有有渠道获得大量的，便宜的电力资源的公司才能经营挖矿[10]。挖矿产业的经济要求使得仅有经营在像冰岛，中国西部这样地区的公司才能获得利润。除了给环境造成不可忽视的负面影响，今天的挖矿产业基本上是建立于政府许可其使用公共设施的协议之上（在某些情况下政府为合作商），然而政府拥有对这些公众设施的完全控制权。也许短期内这并不会成为大问题，从长远的角度来看潜在的规则管制和蛮力攻击可能性[6]会对比特币和其他区块链具有的审查机构防御机制和安全性造成威胁[13]。

建立在高能耗基础上的 PoW 体系带来了一个额外问题——哈希率对区块奖励价值的敏感性。如果区块奖励的市值降低，电费升高，薄利挖矿公司为了止损不得不停止挖矿。这给整个网络的安全性带来不稳定性，尤其是在市场价格变动频繁的情况下。

需要特别注意的是，从算法编程的角度来说，比特币的高能耗是设计者有意加入的特性，而不是一个编程失误。网络扩张和比特币价值提升能够激励 PoW 体系中挖矿机承担更大的工作量，从而保障网络安全性同比例提升。比特币价值的提高代表区块奖励价值提高（有意设计如此），激励挖矿机花费更多资源竞争区块奖励（以比特币计算），也因此消耗更多能源。此机制下即使进行 51% 攻击获得的回报价值提高，进行 51% 攻击的成本也提高。比特币算法并不能直接获得比特币市值信息，但是哈希率的增长从侧面反映出比特币价值的增长[7]。另一种区块奖励算法的构思是——随着哈希率升高，区块奖励反而降低，因此挖矿机没有动机大幅扩张资源成本[8]。该想法确实能够打破能源消耗和币种市值之间的紧密联系，然而，它也意味着更大的安全威胁——进行 51% 攻击的奖励升高但攻击成本并没有升高。

能保障虚拟货币安全性同时降低能耗的新的共识机制逐渐被开发进入公众视野，比如 Chia 和 Spacemesh 采用的持有量证明[9]和时空证明算法[15-16] 的各式形态。虽然这些

[5]哈希率，也就是耗能值，随着网络价值的增长而增长。这样的设计是为了确保实现双重支付攻击有极高的成本，远高于一个成功的双重支付带来的好处。

[6]这个程度的审查机制发生的概率并没有我们想象的那么低。[11-12]，然而此风险可以通过全球化挖矿分布来避免。

[7]尽管这并不完美，因为哈希率随着硬件效率提升也会升高。

[8]比特币区块奖励减半某程度上达到此目的，然而许多人称交易手续费能保障安全性若区块奖励降低。

[9]市场上有许多对此应用的尝试，最出名的以太坊到目前为止还未成功在其主链上应用持有量证明。这些算法机制会带来新的难题[14]。

机制声称其设计无懈可击，它们通常建立在新的安全模式上，而这些新的假设都还未通过大规模实际应用中的压力测试。因此，对于这些新模式的安全问题我们只有极少的实践经验和理解。完全改变比特币的运作模式极大可能会带来新的不可预测的隐患。然而，作者相信以上讨论的主要问题均可通过改良而不是完全替代比特币的根本安全模式——工作量证明。

1.3 新一代工作量证明

为解决规模扩张的难题，作者从改变工作量证明的经济运作模式入手，而不企图发明出一个新共识机制。在比特币和其他类似的网络系统中，PoW 通过给挖矿机施加经济成本负担使得这些网络中的所有节点达成共识协议。然而，经济负担不需要集中来源于耗电费用。事实上，降低运营支出（OPEX），也就是能源消耗支出——挖矿产业的主要成本来源，能够大大改善挖矿产业现状。因此，通过使资本支出（CAPEX）——也就是挖矿硬件成本，成为主要成本来源，整个挖矿生态系统便不再取决于电力费用，且整体挖矿耗电量会大大降低。再者，因为挖矿公司在电费昂贵的区域也能收获利润，自然而然地挖矿产业将会在地理位置上更加分散。再有，低能耗解决了如今挖矿机的发热问题，与降温相关的运营支出也将大幅度降低，这也自然解决了风扇和排热系统带来的噪音问题。以上论述表明个体户和小商业互只要能承担挖矿硬件的费用，都可以加入挖矿产业生态系统，而不需要考虑能否获得低廉能源，或者拥有一个有专业用途的恒温数据中心。从某种程度上来说，对内存有高要求的 PoW 体系，如 Cuckoo Cycle[17]，提高了对静态随即存取存储器（SARM）的利用从而取代纯计算，内存占据了一部分专用集成电路（ASIC）芯片面积，也因而提升资本支出/运营支出（CAPEX/OPEX）比例。

为了最大化挖矿中资本支出/运营支出（CAPEX/OPEX）比例，作者主要进行了两方面调研——其他可行 PoW 算法；生产难度/成本高但是具备高能效性的其他计算硬件（标准专业集成电路范围之外）。我们可以观察到人工智能硬件产业也在向相似的目标发展——越来越多的公司企图商业化小众类硬件构架来实现低耗能计算[10]。这其中就包括前景大好的光学计算，特别是光学辅助处理器。考虑到光学计算拥有商业规模可扩展性和极低能耗的的长远优势，作者总结用光学计算作为低耗能 PoW 的运行平台是十分有前景的。

1.4 光学计算

传统数字类硬件运作依靠的是电流，而光学计算是以光作为运作基础的。光学运用模式早在几十年其就已存在，然而最近人工智能业和通讯行业的发展大大促进了光学计算的发展。研究者预测将光学处理——信号在芯片上通路到最终经过光学加速器——融入到人工智能技术中能够大幅度提升处理速度，同时最大程度上节约能源。再者，半导体产业已经接近其发展极限，意味着数字类电脑难以持续过去五十年的发展路线[19]。这也意味着维持科技发展我们需要其他可行的计算方法和硬件。光学在通讯行业中的运

[10] 人工智能计算量需求以指数形式增长，若没有极大的能量供应传统硬件难以满足如此大的计算需求[18]。

用最直白的阐述了光作为信息处理媒介的巨大优势。毋庸置疑的，光纤缆代替铜电缆这一进步完全改造了洲际之间的沟通，包括速度和效率以指数性增长的互联网。

光学计算的悠久历史追溯于上世纪四十年代的傅里叶转换 (Duffieux 1946)，到八十年代第一代光学神经网络的诞生 (Psalti 1984) 和贝尔实验室对光学晶体管的研究，再到当今光学神经网络，储层计算，和光学量子计算的发展。贝尔实验室对光学计算的研究，全息计算机和光混沌通信启发了接下来冯诺伊曼计算硬件（包括光学深度学习和储层计算）的发展。

深度学习（*Deep Learning*）最近几年，在人工神经网络中应用光学技术的可能性吸引了许多注意力。因此，不少用于向量矩阵乘法（神经网络结构中的基本计算）的新光学硬件技术被研发出市[20-21]。有别于过去依赖于低速空间光调节器[22]，当前已被商业化运用的硬件技术采用结合了微环共振器[20] 和马赫曾德尔干涉仪阵列[21] 的硅光学集成电路。

储层计算（*Reservoir Computing*）储层计算尝试简化循环神经网络的训练过程[23-25]。通过监督训练构建的储层计算系统能够解决模式识别和时间序列预测等难题[26-27]，因而迅速被广泛应用于有多变物理层次的物理实物计算中，如水流[28]。研究人员发现使用光学系统来进行计算，光学储层系统能够实现高速低能耗运作。用于比较，一个用现成光学元件组建的储层系统能够以比谷歌 TPU 快三倍的速度进行语音识别[29]。

尽管近年来光学计算在多项应用中获得成功，限制其被商业化使用的原因一直以来都是大规模生产此硬件的高成本和高难度。其竞争对手数字电脑获利于不断进步的制造技术和无厂模式供应链[11]不断为其提供新产品。相对来说最近才出现的硅光学，其生产能在数字电脑标准芯片的生产过程中完成，这使得大规模生产可复制的光学辅助处理器成为可能。在接下来两个子部分中，作者将提供关于硅光学的简短介绍，及其在深度学习人工智能领域中的应用。另有，在 2.2 部分中，作者简单介绍光学电路进行向量矩阵乘法的工作原理。

1.5 硅光学

过去生产光学系统需要精确的校准，以及昂贵的精密的大号元件。近来光学集成电路（PIC）的发展，通过将大号光学系统移植到碎片大小的光导电路，成功解决了这一问题。光学集成电路的制造过程中，纳米/微型处理技术把极细微的电介质或者半导体拼装成形；精确度越来越高的平板刻法保证校准过程，也使其实现低成本大规模生产。直到 2000 年代初，PIC 还是由昂贵的 III-V 原料制成的。尽管硅并不是最佳的光学材料（没有商业规模的硅镭射，没有电光效应）。但它作为电子设备中无所不在的元素，拥有一个庞大的制造系统。因此制造厂家绕过这些困难，利用大规模优势制造出用于芯片的硅光学元件。硅元件设计随即见证了大突破，例如低损失光纤至芯片耦合器[30]，高速电光调节器[31]，以及锗制芯片上光电探测器[32]。利用过去六十年来取得惊人发展的 CMOS

[11]芯片供应商可以与如 TSMC 和 Global Foundries 等铸造厂合作，而不需要建立自己的生产链。

技术[12]，这些新突破使得在电子铸造厂中制造光学电路成为可能。构架硅光学电路不可缺少的基本元素之一是硅波导。图1-2和图1-3 展现了绝缘体上硅晶圆中的典型波导，其通过内在反射将光波约束在光学电路中（同样的现象见于光纤内导光）。

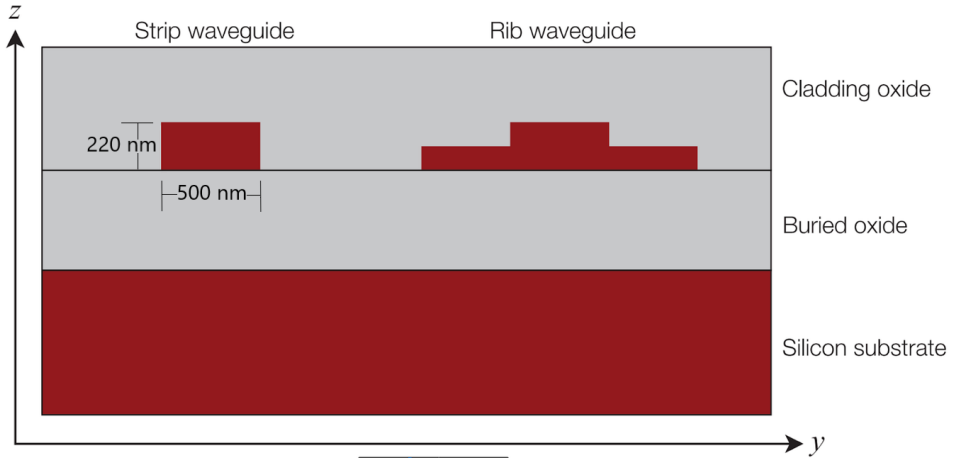
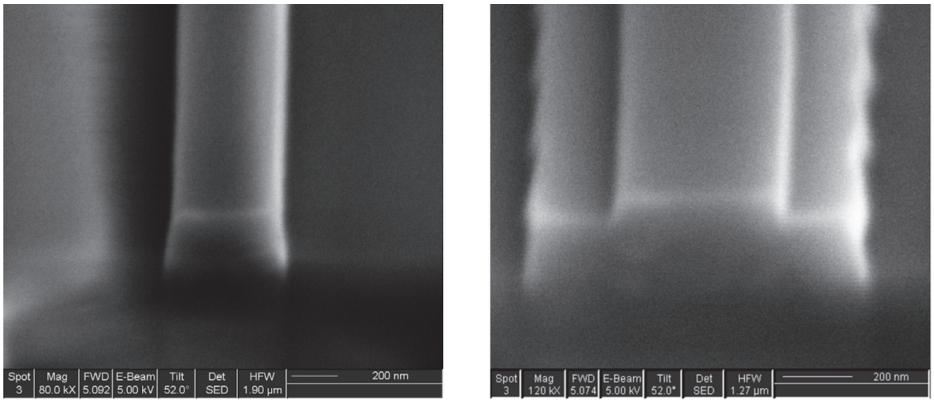


图 1-2 SOI 波导的横截面图



(a) Strip waveguide (b) Rib waveguide

图 1-3 SOI 波导的扫描电子显微镜图[33]

硅光学集成电路在多种数据通讯应用中被用作收发器[34]，并获得了商业规模的成功。如今，数百万硅光学收发器（制造商例如 Luxtera, IBM, 和 Intel）被用于数据中心服务器之间的信息传导。更有数家公司采用商业化硅光学元件于激光雷达和生物传感。更重要的是，重要微型芯片铸造厂（包括 Global Foundries 和 TSMC）要么已经生产硅光学元件，要么就在开启硅光学元件产业链的路上。最近几年，商业化硅光学元件生产的实效性促进了商业化硅光学芯片的发展，进而促进平行计算的发展，用于人工智能的光学辅助处理器也随之而生。

[12]互补金属氧化物半导体 (CMOS) 是一种微型电子元件制造方法，过去 60 年来它成功降低了晶体管的成本和体积高达 10^6 倍。该技术是制造当代数字电路的基础，包括电脑处理器和内存。

1.5.1 集成光学辅助处理器应用于人工智能

由于最近深度学习人工智能算法的成功，MAC 处理需求量大增，这促进了 MAC 处理领域的研究发展，同时激励制造商生产出能够以更低成本更高能效进行这类计算的专业处理器。在 GPU 制造商如 NVIDIA 和谷歌（TPU）有持续进展的同时，其他公司如 Groq （数字型），Graphcore（数字型），以及 Mythic（模拟计算）和 Synthiant（模拟计算）也在不断尝试创新 MAC 处理的电子构架。

在自由空间光通信系统中实现人工智能构架的探索[35-36]，启发了如 LightOn，Fathom，和 Optalysis 等公司尝试实现这类系统的商业化用途。然而，基于不久前普林斯顿神经形态光学实验室[37]，麻省理工大学[21] 和其他学术机构的研究进展，许多创业公司，包括 Lightelligence[38]，Lightmatter[39]，和 Luminous[40]，开始尝试用通讯行业和量子信息处理采用的硅光学元件来制造可用于 MAC 处理的光学电路。此光学技术的目标，如 Nahmias *et al.* 一文[41] 中所详述，是在 MAC 处理方面提供超出电子处理器 2-3 个数量级的能效性，甚至更高数量级的优势，因为光学计算能效性能达到的理论极限是非常高的[42]。对比最先进的 GPU 和一个由铸造厂现成组件构成的光学电路处理器模型的性能，我们发现同样能量消耗的条件下，后者能以 2.8 至 14 倍的速度进行卷积神经网络（CNN）计算[43]。Lima *et al.* 一文中预测一个 128-通道光学芯片的耗能量是 10fJ/MAC，Nahmias *et al.* 一文中[41] 声称这个数值可以进而降低到 2.1fJ/MAC，相较于谷歌 TPU 的 1pJ/MAC[44] 。硅光学辅助处理器领域内这些振奋人心的发展为低能耗技术在人工智能之外的应用发展提供机会。

1.6 光学工作量证明算法（oPoW）

受近来低耗能硅光学元件技术进步的启发，作者展望应用光学计算技术于 PoW 体系的可能性。构建这样 PoW 体系的主要目标是大幅降低能耗。尽管在长远的未来其他挖矿机可能会采用其他模拟计算构架，作者预测光学辅助处理器具备的高能效性及短期内可实现的商业化生产规模，使其最有前途。综上所述，作者提议光学工作量证明（oPoW）——一个以 PoW 算法为基础的，能够最大化集成光学辅助处理器速度优势的算法模型。

第 2 章 低能耗 POW 体系

为了发挥出现有的光学辅助处理器的运作优势，我们选择构造一个改良版本的工作量证明算法，而不是直接采用现有工作量证明算法[1]。接下来作者会简单介绍此光学辅助处理器样板的结构设计和改良版工作量证明算法，以及如何实现低耗能的目标。

值得注意的是，近乎所有已知的改良 PoW 算法都是为了抵制专用集成电路（ASIC）挖矿，也就是说，这些改良的目的是实现 GPU/CPU 挖矿[2]，防止某专门设计硬件的计算优势被利用。这些改良包括 Scrypt（莱特币 LTO 采用），Cryptonight，Equihash，以及最近出现的 ProgPoW。除了 ProgPoW 还未被实际运用，其他已被采用的改良算法都难于对抗专用硬件本身存在的巨大优势，所以都没有成功实现抵制专用硬件挖矿的目标。*The State of Cryptocurrency Mining*[45] 一文中深度讨论了这个现状，最后作者总结道——

> “对于任何算法，硬件工程师们总能找到一条可走的路，打败通用硬件。这是通用硬件从根本上存在的限制因素（弱势）。”

相对于设计 PoW 算法来抵制专用硬件（ASIC）挖矿，设计光学 PoW 算法从根本上简化了这个工程问题。运行该算法，光学硬件相对于其他专用硬件拥有最大效率。所以此改良 PoW 算法是为了实现光学硬件优势，而不是为了让通用硬件打败专用硬件。

2.1 重型哈希函数（HeavyHash）

我们设计的光学 PoW 算法是建立于比特币运用的 PoW 体系（哈希现金结构）基础之上，既能够保证加密安全性，又能够发挥出光学辅助处理器的最大优势。PoW 体系计算量主要在于评估计算哈希方程式，设计此改良版 PoW 最直接的方法是采用光学硬件可以计算的哈希方程式。然而，我们最初就决定放弃采用 all-optical hash（为光学硬件专门设计的哈希函数）或者 Physical One Way Functions（通过物理硬件构造实现的单向函数），因为这两个模式存在重复性（非单一性）[46] 问题，以及在这个阶段我们还不能完全理解他们的安全性性质。为了光学运作重新构造一个新的哈希函数的方案也被否决了，从 IOTA 的惨败[47] 中我们可以看出运用一个未验证的新哈希函数存在的复杂性和未知风险。这些考虑让我们最终选择结合数字型哈希函数（digital hash）和低精度矩阵向量乘法（low precision matrix-vector multiplication，目的在于实现光学加速）构造出重型哈希函数（HeavyHash），详情请见第三章。重型哈希函数（HeavyHash）是一个已知哈希函数，比如 SHA256，和一个加权函数（weighting function）的迭代函数复合，评估重型哈希函数的负担主要在于计算加权函数。如果计算加权函数主要是通过计算一个大数据量的实数矩阵向量乘法，那么通过运用光学辅助处理器我们可以实现高效率的计算[21]。

[1] 许多人已意识到利用光学计算的经济优势：许多光学计算专家已考察过利用光学来挖比特币的可行性，然而现有的 PoW 算法并不适合模拟计算。哈希函数如 SHA256 的特定设计让数字处理器有更高效率优势。

[2] 其最终目标在于硬件供应的民主化，而不是提高能效率或地理位置分布去中心化。

数字型哈希函数的计算负担和加权函数的计算负担的比例可以在一个大幅度范围内具体调整，因为这两个函数存在不同数量级[3]的复杂性。

2.2 光学 PoW 样板

通过最简化的方式表达，光学工作量证明体系（oPoW）其实就是在哈希现金体系[2]中采用我们专门为光学加速器定制设计的重型哈希函数，从而实现光学硬件高效性和高安全性的双重目标。为了测试点对点功能实效性我们设计出运用 oPoW 的硬件样板和软件样板（一个基于 oPoW 的的比特币硬分叉和一个 oPoW 硅光学（silicon photonic）挖矿机）。在比特币代码中重写哈希函数方程式很容易完成，所以这里我们着重介绍硬件样板设计。如下是该系统的简短介绍——硅光学集成电路为中心，以及其模拟计算的运作原则。

2.2.1 系统

我们已知多种运用标准化硅光学组件来实现矩阵向量乘法模拟计算的设计结构。主要的操作方式有两种：1）普林斯顿光学实验室设计的环形滤波组器构架[20] 2）马赫-曾德尔干涉仪（MZI）折射仪网格，比如多次被参考的 Shen *et al.*[21]（麻省理工大学）论文中的三角网格。

我们设计的进行矩阵向量乘法模拟计算的光学组件是一个长方形的定向耦合器网格结构[4]。如图2-1，运行比特币硬分叉节点软件的树莓派微型电脑（RasPi）与 Qontrol 公司制造的控制板配对，该控制板与我们定制的集成电路，跨阻放大器（放大光电探测器提供的信号）以及硅光学芯片所固定在的中介板[5]交流信息。图1-1可以近距离观察芯片构造，图2-2展示的是芯片原型的俯视图。树莓派微型电脑（RasPi）负责计算重型哈希函数（HeavyHash）中的数字哈希函数部分，然后通过 Qontrol 控制板把模拟计算部分传达到硅光学芯片。

[3]N 倍哈希函数输出数位，对应 N 倍哈希函数计算量，对应 N^2 倍加权函数的计算量，基于矩阵乘法的性质。

[4]16. 该网格设计使用的算法由 Sunil Pai 根据他在斯坦佛的研究成果[48] 提供。

[5]印刷电路板，跨阻放大器以及硅光学芯片是与 SiEPIC 合作制造的。SiEPIC 是一个与英属哥伦比亚大学有关联的集成光学工程公司。

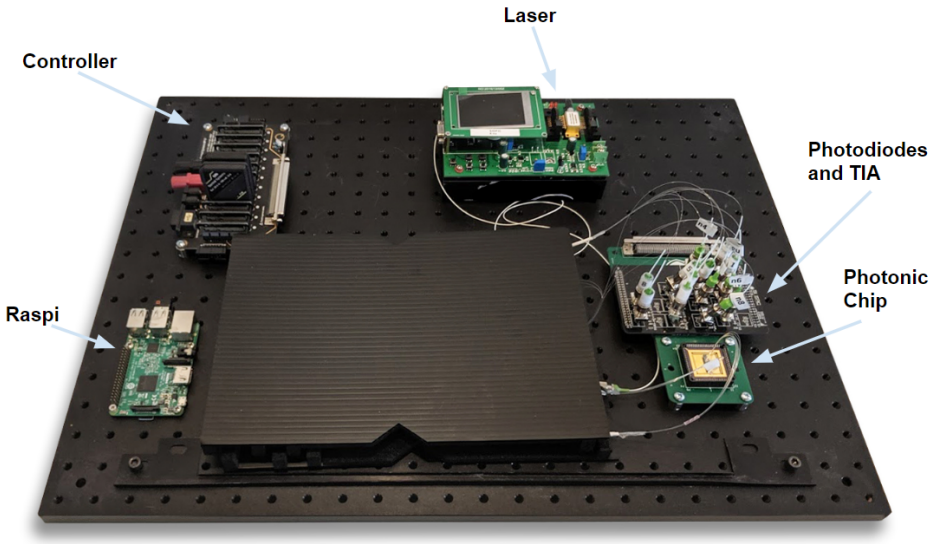


图 2-1 挖矿机样板设计。不包括组件之间接线——树莓派电脑通过 USB 与 Qontrol 控制板交流信息，Qontrol 与安装了芯片和跨组放大器的印刷电路板相连接。

2.2.2 硅光学芯片

如图2-2所示，该芯片将单面光F耦合器输入信号拆分成 16 个光输出信号。每一个光输出信号都会单独被（可导热，平衡光纤）马赫-曾德尔调变器[6]调变（相对应树莓派电脑提供的电信号）。调变器输出信号传输到矩阵向量相乘的定向耦合器网格[7]，该矩阵乘法网络的输出光信号通过光F耦合器收集到光纤中，紧接着通过光电二极管和跨阻放大器转换为电信号。如果投入商业化生产，光电探测器将被包括在芯片上，从而简化整个设计构架，也不再需要考虑光纤连接（激光输入可以通过覆晶封装的方法耦合）。

[6]关于马赫-曾德尔调变器的简单介绍请见 2.2.3 部分。更多详细信息可参考 *Silicon Photonics Design: From Devices to Systems by Lukas Chrostowski and Michael Hochberg*[33] 一书中对典型硅光学组件的章节。

[7]对定向耦合器的简单介绍请见 2.2.3 部分。

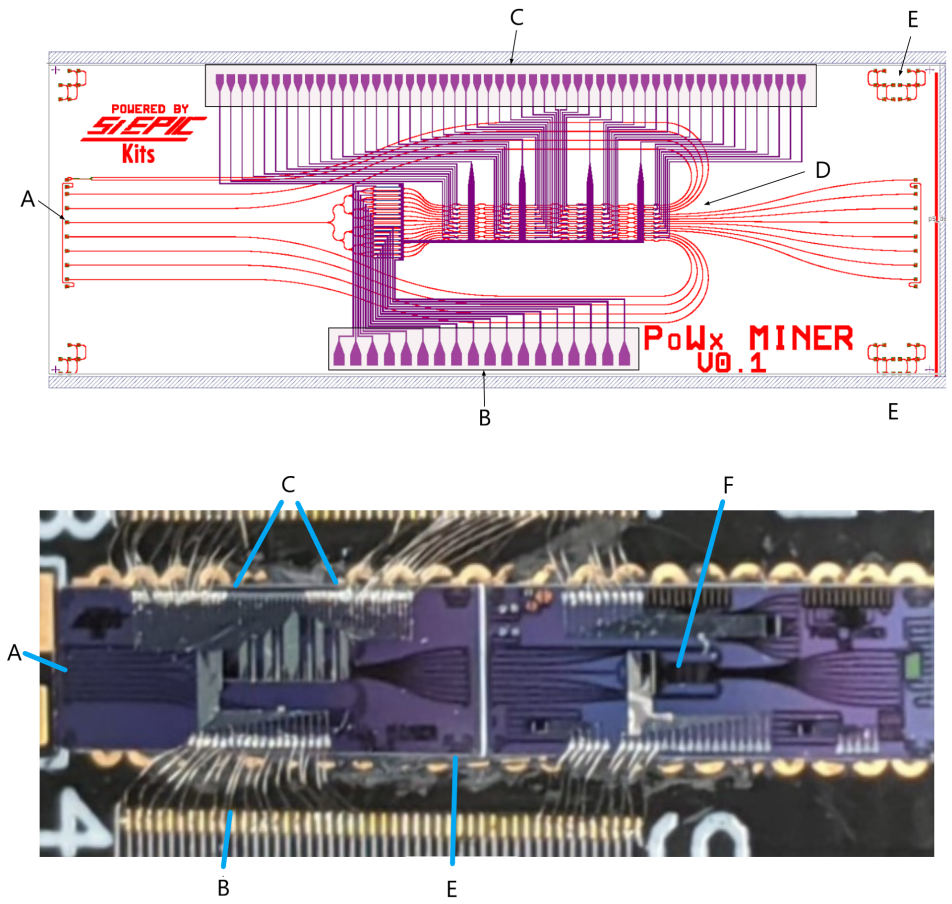


图 2-2 上：光学电路图。A. 激光输入（1550nm，电讯一般波长) B. 控制调变器将电子信息转导为光学信息的金属垫 C. 调整定向耦合器网格的金属垫 D. 包含计算结果信息的光学信号从这里通过光栅耦合器输出到光纤中，光栅耦合器是每个波导的终点 E. 校准光纤耦合的调整电路。下：oPoW 挖矿机样板，接线和光纤连接前的裸芯片图。A-E 同上。F. 测试电路

2.2.3 定向耦合器网进行么正矩阵乘法的工作原理

Reck *et al.*，Russell *et al.*[49-50] 论文中对通过光学/干涉进行矩阵乘法进行了广义的讨论。Pai *et al.*[51] 一论文中对几种为矩阵乘法设计的集成光学构架以及其调试算法进行了具体的论述。以下部分对我们采用的方法涉及的工作原理进行直观的论述。

如图2-3所示，单束输入激光被平均拆分成多束相等的波导，每一束波导被输入一个可以削弱光强度的调变器。

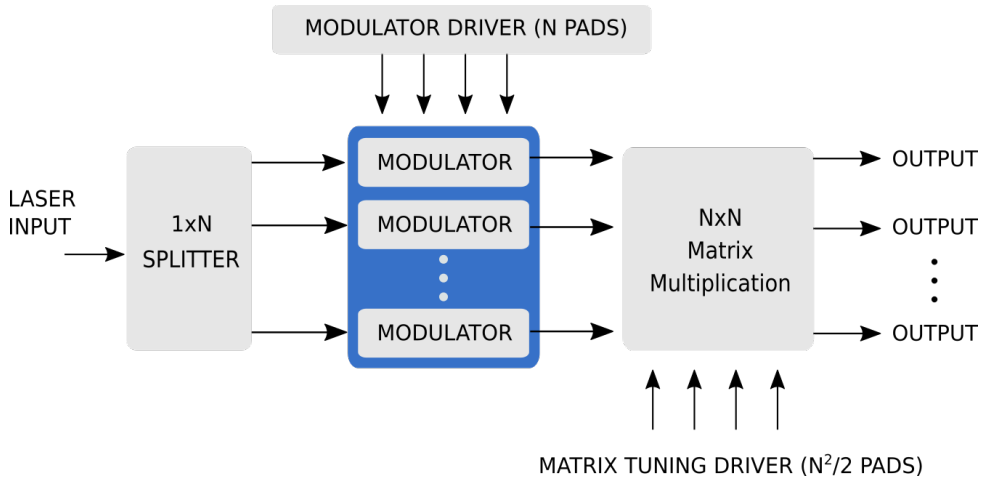


图 2-3 组件大致方块图（金属为蓝色）。在我们的设计中 N=16，金属（打线接合）垫为 MZM 调节器提供电信号连接。另一套金属垫为定向耦合器提供加热器调节功能

我们选用的马赫-曾德尔调变器，如图2-4所示，将输入光束拆分成两束波进入两个光支路，其中一光支路的波产生相移，然后两束波在输出端重新合并。通过加热器[8]改变其中一个光支路折射率，该支路中的光信号便会产生相移。

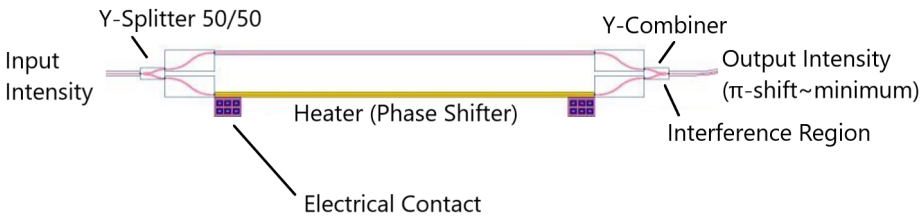


图 2-4 马赫-曾德尔调变器

在一个理想化的设备中，一个完整的 π 的相移会导致完全破坏性干涉（两波相消），而小于 π 的相移会导致部分破坏性干涉。调变器受收到的电信号调控，输入电信号因此转换成拥有模拟强度的光信号。比如，在一个四位元系统中，完整的 π 位相移对应 0000，零位相移对应 1111，部分破坏性干涉则对应于这两者之间。调变器的输出信号进入定向耦合器（如图2-5所示）网格，其分光比取决于每个输入光波相位 ϕ 和 ϕ' 以及耦合区域的有效光学几何性质。耦合区有效几何光学性取决于其物理几何性质（耦合区长度和波导之间的间隙）以及可通过热度因素调节的折射率。

[8]PN 结相移器能达到更高的速度和效率。

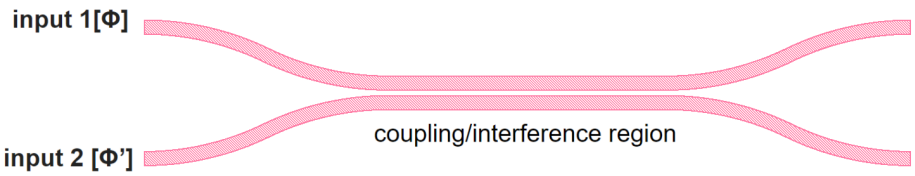


图 2-5 定向耦合器基本设计

通过加热器调整定向耦合器网格每一层里每一个波导的光波相位延迟，以及耦合区域的有效光学长度，得到一个具有么正性质的随机的传递矩阵[9]（Transfer Matrix in Optics）是可能的。如果我们把每个调变器输出的光波振幅和相位看作输入向量 [I][10]，把网格的传递矩阵看作矩阵 [U]，那么在数学意义上此耦合器网格的输出结果相当于一个向量与矩阵的乘积 [U]*[I]。然而，光电探测器探测到的信号只对应于光信号的强度而不是其相位，所以，探测器提供的模拟电信号实际上是乘积结果向量 [O] 的绝对值。Pai *et al.* 在最新发表的论文中对此结构和其他几种相似但有不同取舍的结构进行了详细的讨论[48]。值得注意的是，尽管么正矩阵（如果只探测振幅则是正交矩阵）对于此构架是最理想化的，但只要通过某些额外的调整此构架即可适用于任何实数矩阵（数值处于 0-1 之间），为简洁之便这里不做详细叙述。假设低精度数模/模数转换可与应用案例需求兼容，通过光学来进行这样的运算的优势是巨大的：本质上来说所有的光束都在进行平行处理。

作者预测采用一个为光学硬件定制的工作量证明算法能为区块链网路提供多种优势，比如更高的安全性（更好的防御 51% 攻击）以及总体上相对于类似网络系统更低的耗能量。关于以资本支出为主的 PoW 体系带来的许多经济方面和安全性方面的影响的具体分析将会单独发表，作者将在接下来的部分对此提供简述。

2.3 节能

工作量证明（PoW）区块链的总耗能量不是取决于单个哈希函数计算量，而是整个挖矿网络运作该区块链消耗的总能量。举例来说，如果 SHA256 被一个相对较低计算量的哈希函数取代（从而降低计算单个哈希函数的耗能量），若运用于同样的硬件模式（ASIC），所有的挖矿机将会被迫计算更大数量的哈希函数来满足上调后的难度要求（保证安全性）。

然而，假设计算 PoW 的成本主要源于一个能量高效性的硬件模式（虽然硬件成本费更高），该 PoW 体系区块链总体上会更节能。尽管，表面看似矛盾地，每单个哈希函数的运算成本更高。这是由于 PoW 计算难度可以通过调整使得每个区块的建造成本相等，尽管每个哈希函数的计算成本不一致。因为区块链的总成本取决于每个区块奖励

[9]实践中，由于电子输入数值数量有限，我们提供的此样板只能实现一部分么正矩阵，但这在商业化规模系统中并不会是一个根本问题。

[10]根据设计所有输入相位都是一样的。

的价值，并非获得奖励所要求解答的哈希函数数量，我们可以直接对比使用不同哈希函数的区块链成本中不同组成因素（耗能支出，运营支出，硬件损耗，资本支出）的相对值[11]。

只要能量高效性硬件模式能够相较于其他硬件模式，提供边际成本优势，作者认为理性主体会选择此硬件模式来达到挖矿利益最大化。

综上所述，已知存在一个资本支出主导每函数计算成本的硬件，通过定制出一个偏向此硬件模式的 PoW 算法，低耗能的目标就可以实现。

2.3.1 节能量计算模型

作者接下里对比采用 oPoW 的网络系统和一个类似的哈希现金网络系统两者之间的能量支出差异，假设电力价格相等。再者，作者假设两个系统中区块奖励价值相等，调整挖矿难度使得两系统内建造每区块的成本相等。每哈希函数总成本是一个有关硬件成本（资本支出摊销于硬件任期）和能量成本（即运营支出）的函数。摊销后的资本支出和运营支出的相对比率直接决定了该生态系统整体挖矿花费结构。

假设某系统的区块奖励为 R，它等值于每区块摊销资本支出（CAPEX）加上每区块运营支出（OPEX）加上平均利润 ϵ，因此有：

$$R = \text{CAPEX} + \text{OPEX} + \epsilon$$

设某数字硬件系统中，运营支出（OPEX）为每哈希消耗千瓦时 × 每千瓦时美金价 = $O_{数字}$，每哈希摊销资本支出（CAPEX）= $C_{数字}$，在此 pow 体系中每个区块有 $K_{数字}$ 哈希函数，所以有

$$R = K_{数字} * (O_{数字} + C_{数字}) + \epsilon$$

同样的，若我们假设区块奖励和矿机利润率在数字和光学系统中相同，且在此 opow 体系中每个区块有 $K_{光学}$ 哈希函数，所以有

$$R = K_{光学} * (O_{光学} + C_{光学}) + \epsilon$$

因此，两个系统中每个区块的总能量成本分别是 $K_{数字} * O_{数字}$ 和 $K_{光学} * O_{光学}$。接下来我们可以计算出光学系统相较于传统数字系统的节能量：

$$\begin{aligned} \text{节能量} &= \frac{\text{数字硬件能量成本} - \text{光学硬件能量成本}}{\text{数字硬件能量成本}} \\ &= \frac{K_{数字} * O_{数字} - K_{光学} * O_{光学}}{K_{数字} * O_{数字}} \\ &= 1 - \frac{K_{光学} * O_{光学}}{K_{数字} * O_{数字}} \end{aligned}$$

[11] 作者在此假设市场会自动调节哈希率直到各体系中挖矿成本是相同的。

我们可以把这个方程简化为一个关于（在数字和光学系统中）每哈希函数能量支出/摊销硬件成本比例的方程。也就是说，定义 MIR^O 和 MIR^D 分别为光学和数字系统中挖矿硬件低效率比，

$$\begin{aligned}\mathrm{MIR}^O &:= \frac{\text{每函数评估光学硬件能量成本}}{\text{每函数评估光学硬件总成本}} \\ &= \frac{O_{\text{光学}}}{C_{\text{光学}} + O_{\text{光学}}} \\ \mathrm{MIR}^D &:= \frac{\text{每函数评估数字硬件能量成本}}{\text{每函数评估数字硬件总成本}} \\ &= \frac{O_{\text{数字}}}{C_{\text{数字}} + O_{\text{数字}}}\end{aligned}$$

因此我们有：

$$\text{节能量} = 1 - \frac{\mathrm{MIR}^O}{\mathrm{MIR}^D}.$$

2.4 从经济角度考虑安全性

为了保障分类账安全性，比特币网络每年花费 50 亿美金奖励挖矿机。通过比特币膨胀，该成本最终是由比特币持有人来承担的。所有针对于去中心化虚拟货币安全性/共识机制进行的分析和研究，都面临一个关键问题：安全性预算到底能买来多少真实可靠的安全性?

通过解读经典的 51% 攻击[1] 和哈希率随时间的变化，作者讨论建设于 oPoW 的区块链的安全性经济成本。

2.4.1 低运营支出 PoW 体系中 51% 攻击防御性

51% 攻击指的是某攻击者获得超过整个系统一半的计算力量，从而打破共识协议，进行双重支付，审查某些支付，等等不良操作。理论上来说进行该攻击的成本大于或等于整个系统的资本支出（良性节点持有的硬件）以及该攻击持续时间内所有运作支出（能量支出）。所有 PoW 区块链的安全性都建立在此基础上——进行 51% 攻击预计成本是极高的。

假设在一个应用某特定 oPoW 算法的区块链系统中[12]，某攻击者想要获得 51% 的计算能力却几乎没有可能租用到足够多的硬件来完成此攻击。因为此系统中的挖矿机几乎没有可能同时出租一大部分计算能力[13]，且因为不存在其他系统使用该硬件，市场上不存在第二个此硬件供应商（使用通用性硬件（如 GPU）的系统，并没有这项优势）。因此此攻击者必须购买（或者生产）等值于几乎整个系统资本量的硬件，来获得 51% 的计算能力。注意到如果该系统受到攻击，该硬件潜在的再利用价值降为微乎其微。

[12]若多个网络系统使用相同的 PoW 算法，情况就变得复杂，因为一个系统中的挖矿机可用于攻击另一个系统。

[13]尽管并非不可能，但是租用整个网络系统中大致一半的硬件的意图很难不被识出，同时硬件持有者有拒绝把硬件租出给攻击者的动机——网络被攻击后其硬件也随之失去价值。

因为 51% 攻击中攻击者同时需要承担攻击时段的运营支出，该攻击者会尽量缩短攻击持续时间。比如，对于双重支付，此攻击只需要持续直到受害人确认交易（比如不大于一天）。假设该攻击时段内 T 个区块被生产，哈希率为 H ，每哈希函数资本支出为 C_x ，每哈希函数每区块生产时间（比特币网络中为 10 分钟）运营支出为 O_x ，我们可以得出该攻击的成本为 $H*C_x+T*H*O_x$。在任意系统中若一天挖矿中运营支出 << 整个系统的资本支出，攻击成本则是以完成此攻击需要的所有硬件成本为主。

该分析同样适用于比特币。尽管比特币有高运营支出，一个持续较短时间的攻击（以天或星期来计算的时段）成本主要来自于获得该攻击必须的硬件。以蚂蚁矿机 S9 为例，其市场价格为 700 美金，哈希率 14TH/s，相当于 1.5e-7 的当前比特币的哈希率，也就是每秒 0.019 美金的期待奖励值。假设运营支出不会超过挖矿期待奖励值（否则挖矿就无利润），这表明蚂蚁矿机 S9 的资本支出起码是其运营支出最大值[14]的 157000（或 36800）倍。因此一个持续几天（或产生几百个区块）的攻击成本运算中，资本支出为主要成本。因此，若资本支出能较运营支出占系统总成本中更大的一部分，时长较短的攻击成本就更高。

总而言之，作者相信从长远的角度来看 oPoW 体系能够比运营支出占大比例的 PoW 体系提供更强大的 51% 攻击防御性。因为有许多指标表明 oPoW 能导致更快的哈希率增长以及更好的防止哈希率受区块奖励价值降低的影响[15]（哈希率不会随区块奖励降低而降低）。

2.4.2 低运营支出 PoW 体系中哈希率的增长和弹性

挖矿成本从运营支出为主转为资本支出为主，提升了整个网络对长远安全保障的有效投资价值（投资形式为区块奖励和交易手续费）。挖矿机产生的任何运营支出成本并不会促使哈希率的增长，因此，并不会有助于长远的安全保障。随着更多资金流入资本支出，构成整个网络的专业性硬件数量也越大，因而加高了攻击门槛。还有一个与资本支出主导相关的好处在于，若货币价值降低（挖矿奖励价值降低）或者电价出现波动，低运营支出挖矿机有较小的动机停止挖矿机工作。比特币的哈希率增长与硬件挖矿效率增长相比其实是小巫见大巫。通过分析某特别定义的哈希率 *Specific Hashrate*（可大致解释为哈希率除以每哈希函数计算花费），我们看出比特币的安全程度受其价格的影响很大。2018 年第四季度，比特币价值波动较大，其价值在某个期间甚至流失了其原先市场价值的 45%。挖矿机为了避免电费成本停机，导致比特币哈希率从 60 EH/s 降到 35 EH/s[52]（虽然比特大陆发行了一款新的高运作表现 7nm 挖矿机[53]，且有许多其他硬件制造商加入竞争，哈希率还是大幅降低）。oPoW 的经济结构能创建一个扩张更快，更稳定，更忠诚的挖矿机市场。

[14]运营支出应该是接近于区块奖励的三分之一，这样挖矿公司的投资回报率处在一个较为合理的范围。

[15]注意到在某些情况下，能量成本可能一部分属于资本支出而不全属于运营支出，若挖矿公司实际上在投资能量设施。显然这有利于哈希率稳定性只要这些设施不会被再利用于其他用途，然而能量设施相较于计算硬件体积大，难运输，需要更多维护。

第 3 章 改良哈希现金

在此部分中，作者展示简单改良哈希现金 PoW 系统中核心的哈希函数，能够提高工作量证明计算成本。

注意到若在不同硬件系统中此成本提高程度不同，我们可以逻辑推断出挖矿公司会转换使用更高效的硬件系统。再者，若改良版 PoW 使得能量成本占据新系统中总挖矿成本（假设新系统中总成本也更低）更小的一部分，节能的目标便能实现。

然而，此部分作者只简单介绍如何改良哈希现金类 PoW 体系的一个通用框架，从而在不牺牲安全性能的前提下实现上述目标。作者提供的改良十分简单——只需要对核心哈希函数进行一个简单的黑盒变换。因此将此变换复合到现存体系上并不存在太大困难。

此变换框架必需两个元素：1) 一个评估计算难度高的函数 2) 一个加密哈希函数。为实现第一个必需元素作者提出理论复杂性质，并命名为 “必须有效难度最小值”。参照 Bellare 和 Rogaway 论文使用的范例[54], 作者通过用公用随机函数模拟加密哈希函数，证明此框架符合所需的安全性。在实践中，加密哈希函数可以被具体为 SHA256，或其他任意加密函数。

3.1 哈希现金概述

一般来说，在 PoW 体系中我们需要保证：任意一个潜在证明者，对应已给出的一个随机难题 c，必须在付出某数量级的计算力量后才能提供出一个有效证明 π，对应此难题 c。

哈希现金遵循如下观察现象：已知某随机预言机, 找到一个属于某稀疏子域（占 $2^{-\lambda}$ 陪域）的输入值，需要进行函数评估的次数遵循几何分本（参数为 $2^{-\lambda}$ ）。

用 PoW 的语言表述，我们可以把一个随机字符串 c 看作：其指明一个随机预言机。具体表述为：使 $H_c(\cdot) := H(c, \cdot)$。这样一来，哈希现金的某个证明则是某字符串 x 使得：

$$H_c(x) \text{ 首 } \lambda \text{ 位均为 } 0。$$

在比特币应用中，区块头（Block Header）实际上是提供了一个随机难题。SHA256 则是表明这个随机预言机的方式。

在以下部分种作者将使用 H 代替 H_c，或者 $H(c, \cdot)$。

3.2 重型哈希函数框架

此框架的思路其实非常简单。假设存在某函数，使得两个不同的硬件系统评估此函数所需成本不同，同时评估成本较低的硬件系统（目标系统）满足我们的其他要求（比如，在目标系统中评估此函数消耗能量低）。因此，与此函数复合后的加密哈希函数，能

够实现：1) 保留原本加密哈希的许多安全性能 2) 评估此复合版哈希函数在目标系统中需要的成本较低。我们称这个复合版哈希函数“重型哈希函数”。

具体来说，设 H 为某加密哈希函数在系统 P 中评估成本为 C_H。理想条件下此成本对应评估此函数的平均成本，基于该系统硬件当下最高水准（以及对于电价的保守估计）[1]。再者，设 f 为某置换函数，在系统 P_1 评估成本为 $C_f^{P_1}$，在系统 P_2 中评估成本为 $C_f^{P_2}$ （假设这些成本包括从系统 P 转换到新系统产生的成本）。现在设改良哈希函数：

$$H'(x) := f(H(x)).$$

我们可以很快推出，H' 在系统 P_1 in 成本为 $C_H + C_f^{P_1}$，在系统 P_2 成本为 $C_H + C_f^{P_2}$。[2]我们会展示此复合函数 $f \circ H$ 中 f 函数的特殊性使得其评估对于布尔电路非常困难，因此基于此复合函数的 PoW 系统需要的工作量主要随 f 函数困难性提升而提升。为了让此 PoW 系统具有实效性，我们还需要 f 函数的评估对于布尔电路困难但不是极度困难，否则用布尔电路验证答案是否有效会过于昂贵。但在此部分中作者针对讨论找到答案所需的工作量，而不讨论证明答案的过程。

置换函数能保持安全性。 在阐述如何将复合版哈希应用于工作量证明体系之前，作者首先解释为什么将加密哈希函数与某些函数复合（特别是那些能“保持最小熵”的函数）能够最起码保持加密哈希函数的安全性质。虽然此理论并不适用于所有情况，但若加密哈希复合的函数是一个置换函数，在此特殊情况下此理论属实。具体来说，一个随机预言机，H，与任意置换，Π 复合后，任然是一个随机预言机。从某些程度来说，这告诉我们此复合版函数 $\Pi \circ H$ “继承”了 H 的性质。

Fact 3.2.1 (置换能保持随机预言机的性质)**.** *If $H : \{0,1\}^n \to \{0,1\}^m$ 是一个连续性随机分布函数，Π 是一个在 $\{0,1\}^m$ 域上的置换，则 $H' \equiv \Pi \circ H$ 的分布形式和 H 是一致的。*

并不难看出此事实遵循：一组函数的任意一个置换复合后的函数自同构。

由高难度函数得出的高难度置换。 同时注意到任何函数可以通过费斯托密码转换成一个置换函数。对于任意 $g : \{0,1\}^n \to \{0,1\}^m$，定义函数 $\Pi_g : \{0,1\}^{n+m} \to \{0,1\}^{n+m}$ 如下：

$$\Pi_g(x, y) := (x \oplus g(y), y)$$

再者，Π_g 的计算难度不会低于 g 的计算难度（modulo XOR），即使是摊销到许多随机实例上。

然而，作者注意到特别对于哈希现金类的 PoW 系统，此高难度函数 f 并不一定需要是置换。（然而，把高难度函数转换为置换函数有助于复合版函数 $f \circ H$ 继承某“类似”于随机函数的函数 H 的性质。）

[1]然而，这样的复杂性在理论上很难处理，我们的命题会以较传统的预言机辅助电路为模型。在此模型中不同的硬件系统相对应于不同的电路模型（拓扑结构和逻辑门函数），和不同的复杂性量值。

[2]再者，若 $C << C_f^{P_1}, C_P i^{P_2}$，且再通过 Merkel-Damgard 转换扩展 H' 的域，P_1 vs P_2 系统的相对成本则接近于 $C_f^{P_1}/C_f^{P_2}$。

重型哈希函数。 作者在讨论高难度函数 f 必须的难度系数之前，首先展示如何通过复合 f 来建立改良版加密哈希函数。

$$H'(x) := H(f(H(x)), H(x))$$

如之前提到的，证明者必须评估此高难度函数 f，在哈希函数 H 输出值上的对应值。显然，每一个新的哈希函数输入值能产生新的哈希输出值，随之为 f 提供一个新的输入值。再者，考虑到 f 本身可能存在某些良好性质，证明者必须再次评估评估哈希函数 H 在 f 输入值和输出值上的对应值。此评估实际上表达了 f 输入值和输出值之间的随机稀疏关系。[3]

为了解释如上设计原因，回到哈希现金中对某哈希函数 F 的大致描述：

对于字符串 x，找到证明 y 使得 $F(x, y)$ 首 k 数位均为 0。

具体来说，以上表达意味着找到一个点，来满足一个稀疏关系（在某【随机】x 描述的子多维数据集中找到一点，其通过 F 的输出值满足某稀疏谓词公式 P，P 对于任何 k 首位为 0 的输入值 P 值为真）。以上思路存在一个危险性，f 函数可以被特别定制，使得决定某 H 输出值——z^* 是否存在于数集 $\{z : P(f(z)) = 1\}$ 可能比计算 f 本身简单得多。为解决这个问题，我们可以利用 H 破坏 P 中任何结构：找到输出值 z 满足 $P(H(z)) = 1$（若用密匙函数 H_x 来表达 H 则找到 z 满足 $P(H_x(z)) = 1$）。换句话数，在比特币 PoW 中评估复合函数 $H \circ f \circ H$。

3.3 必须有效难度系数最小值

实际运用重型哈希函数需要一个能满足复杂系数很强的函数。作者不仅希望此函数能满足在此部分中阐述的复杂系数低端临界值，还希望此临界值定义是严格的，从而证明工作量有效性对于数字计算工具并不会过于昂贵。然而，此部分主要介绍低端临界值要求，使得在某已知硬件系统中大量生产工作量证明的成本高昂。

3.3.1 复杂系数条件

设 $f : \{0,1\}^n \to \{0,1\}^m$ 为某候选函数。基于以上提供的证明机制，作者接下来从一个普适的角度阐述难度条件。在给出定义之前，以下是定义涉及到的参数的一个非正式简述：

- f 函数输入值长度：n。
- f 函数输出值长度：m。
- 每成功评估必须的工作量最低临界值：w。

[3]评估 H 函数在 f 函数输出值上的对应值直觉看来已经足够完整。要求评估 H 函数在 f 输出和输入值双项的对应值，也许只是一个分析的产物，实际上 $H''(x) := H(f(H(x)))$ 也许已经足够。这是因为，起码对于此特殊情况——f 是一个置换且 H 是随机的，$y = H(f(H(x))$ 可有效表达出 $H(x)$（以及 x）。然而，该简化可能会导致某些信息丢失，所以作者这里决定采用一个更完整的构建。

- 存在成功评估最大数量：T。[4]
- 意外情况可能性：ϵ。

Definition 1. 我们称 f 对于某电路是 (ϵ, w, T)-*MEH*（参数满足必须有效难度最小值）若以下条件成立：设 A 为一个可“按一个按钮”[5]接收连续性随机变量 $x \in \{0,1\}^n$ 的电路。A 可进行任意数量的操作（按按钮的成本很低且固定）。A 也可以输出“候选答案”：元组 (x, y)。若输出 x, y 中 x 并不是按按钮收到的，或者 $y \neq f(x)$，此输出元组被忽视不计。对于任意 $t = 1, 2, 3, \ldots, T$，任意 A，A 工作量[6]小于 $t \cdot w$ 但成功输出不小于 t 个不同的元组 $(x_i, f(x_i))$ 的概率最大为 ϵ。[7]

3.4 随机预言机模式下的分析

作者接下来展示此转换。转换中改良版函数若是置换，基于随机预言机的 PoW 机制相对于某已知硬件模式的计算成本会提高。

固定成本随机预言机 在此模型中，作者假设所有硬件系统唤起预言机 H，都有某固定成本 C_H。作者假设非均匀模型计算，其中计算成本的衡量遵循标准复合性质。以下命题阐述在哈希现金系统中应用合适的重型哈希函数，要求的工作量会随函数 f 难度系数增长而增长。

Proposition 3.4.1. *若 f 对某电路是 (ϵ, w, T)-MEH，则当哈希现金 PoW 应用此函数 H'，H' 定义为 $x^{\epsilon U} \mapsto H_2(f(H_1(x)), H_1(x))$（$H_1 : U \to U$ 及 $H_2 : U \times U \to U$ 均为随机函数），且安全性/稀疏性参数 λ 合理时：一个最佳证明者对 H_1 进行非适用评估的工作量的分布在统计上接近（$\epsilon + 2^{-\lambda}$）于一额变尺度指数/几何分布（通过 $w(C_f + 2C_H)$ 工作量的成功概率为 $-\ln(1-2^{-\lambda})e^{\ln(1-2^{-\lambda})w}$）*

证明. 设 P^* 为一个证明者。考虑某事件，E，P^* 提交一个成功证明 x^* 满足 H' 头 λ 位数为 0，在只评估 H 函数于 x^* 或 $(f(H(x^*)), H(x^*))$ 其中一个或零个的情况下。此事件的概率为 $2^{-\lambda}$ 除于 H 函数评估的选择。

否则（不小于 $1 - 2^{-\lambda}$ 的概率下），P^* 必须评估函数 H 于 x^* 和 $(f(H(x^*)), H(x^*))$ 双项。设 S 代表 x 的某数集，满足 P^* 评估 H 函数于 x 和 $(f(H(x)), H(x))$ 双项。在 E 事件不发生的条件概率下，$P*$ 获得任何有效证明的概率最大为 $1 - (1 - 2^{-\lambda})^{|S|}$。

显然，P^* 起码进行了 $2|S| \cdot C_H$ 的工作量。作者希望进一步证明它一定还进行了 $|S|C_f$ 的额外工作量。为证明此，作者构建了一电路 A'，该电路能基于随机批次的输入值找到 $|S|$ 个 f 函数的解答。

[4]因为此体制中参数是固定的，每个输入值对应的答案可以被找到然后总结成一个查看表（成本在于计算解答出每一个输入值对应答案），之后的解答成本就很低，摊销成本大致等于查找表格的成本。此参数设计的意图在于使得这类型“攻击”无效。

[5]以 PoW 的的角路来看相当于计算解答 SHA2。

[6]对于专用集成电路，工作量可以被大致解释为芯片面积乘时钟周期。我们最终在乎的是美金成本，即对应其生产成本和运行芯片的能量成本。

[7]注意到也许存在一个更简洁的表达式来阐述实例运用重型哈希函数的必要条件。作者在此只提供一个案例。

构建这样一个电路，作者只需简单考虑 P^* 做出的尝试。我们可以将对 H 函数进行的尝试组织为两类：1）属于 U 集 2）属于 $U \times U$ 集。新的（之前未有过的）第一类尝试对应于 MEH 命题中的“按钮游戏”，第二类对应于候选答案。

若第一类尝试是有适应性的，我们会记录一个代码字典来决定某尝试是否是新的。这代表 $c \cdot q_a$ 工作量，其中 c 是一个常数，q_a 是属于第一类的尝试数量。根据我们的假设，若 P^* 获得上述数集 S（大小为 $|S|$）有效答案，则有：P^* 进行了小于 $w|S|$ 的工作量的概率最大为 ϵ。 □

3.5 难题猜想

在此部分中作者对以上机制具体应用中需要的难题进行猜想，这些难题用 PIC 硬件（相对于 ASIC）评估成本较低。基于此硬件的特殊性（特别是，用光子获得大部分可靠输出值的难度），作者将提供与以上简单机制有某些不同之处的方案。

3.5.1 候选函数：随机线性变换

作者设想施特拉森（Strassen）矩阵演算法基本上是第一选择（它几乎完全满足必须有效难度最小值），它提供令人满意的参数，对于评估矩阵和随机向量的乘积（定点运算）也是最佳选择。

作者设想此难题满足必须有效难度最小值（实践中真实复杂性是用计算摊销成本美金价值来衡量的）的理由很简单：定精度线性代数是计算机科学多个领域的核心，尤其是计算机图形学和机器学习。进行这些这些计算的吞吐率惊人的高，特别是源于机器学习的惊人发展。因为它是如此多应用中的核心元素，我们可以合理推测出：尽管领域中存在某些革命性创新，通过 ASICs/FGPAs 进行定精度线性代数计算的实际成本已经基本稳定，未来成本降低的程度也基本可以被预测[55-56]。另一方面，近几年来不少引人注目的创业公司的成立都是基于 PICs 能够用较低成本进行这些计算的承诺。

再次注意到作者希望此函数难题符合以下要求：

1. F 对于数字硬件满足必须有效难度最小值
2. 利用光学模拟计算低精度矩阵向量乘积能够加快 F 计算

候选高难度函数 F_Q 的具体表述可见图3-1。实际上，F 其实是一个函数分布模型。作者猜想此类中某随机函数有高概率性满足必须有效难度最小值。

候选难题：F_Q（矩阵乘法）

选样矩阵 Q（指明 F_Q）

选样连续性随机矩阵 $Q \in [0,1]^{n\times n}$，输入数目被舍位至 4 位数元。

函数方程式 F_Q

1. 输入值 $x = (x_1, x_2)$, 解释 x_2
2. 演绎二进制向量矩阵乘法（在 $\mathbb{R}$ 上）：$y' = Q \cdot x_2$。
3. y' 输入数位舍位至 4 位数元，得到 y。
4. 输出 $z = (y \oplus x_1, x_2)$，其中 $y \oplus x_1$ 是 y 和 x_1 二进制表示法进行逻辑异或门（XOR）的结果

图 3-1 满足有效难度稀疏最小值（MEH）的候选高难度方程，F_Q

3.5.2 关于高难度线性转换

作者提出的方案的核心在于应用一个线性转换，此线性转换对数字硬件要求工作量比对光学硬件要高。然而，作者在此只能猜想某已知线性转换是高难度的。

幸运的是，如以上提到的，矩阵向量乘法在实践中已被详尽研究过，因此时间测试经验提供的界限大概率上是没有漏洞的。再者，矩阵 Q 并不是一成不变的，通过调节光学硬件矩阵 Q 可以在毫秒内被调整，从而估值任意线性转换。不幸的是，想要用每个 nonce 获得随机矩阵，这个办法还是太慢了。（还有，大矩阵需要许多伪随机数数位。）但是，在每个区块或没几个区块之间换矩阵，。。。，这个速度是足够快的。虽然表面上这样能够使整个难题更强大，作者注意到实际上保证安全性必须实现以下两者之一：1）一个更可靠的关于“高难度”矩阵密度的猜想 2）关于区块链的新分析。因为此操作会带来与 Eyal 和 Sirer 进行的扣块攻击[57] 相关的攻击，此攻击类型中挖矿机可以找到提供“便利”矩阵的区块块前缀。

作者同时注意到，若矩阵 Q 具有么正性质，光学硬件结构使得其能够进行非常复杂的矩阵乘法。不幸的是，目前大规模生产该硬件样板存在困难。然而，若这些困难在未来能被解决，作者相信能找到一个更可靠的候选难题。

最后，值得注意的是，此理论只考虑有限域的线性转换，因此较实际情况更为简单。随机线性转换的难度可高达两倍[8]。

对于任意转换 T, 选样随机矩阵 A 和 B 满足 $T = A + B$。因为 A 和 B 是边缘均匀分布矩阵，我们通过一个简单的方程分解

$$Tx = (A + B)x = Ax + Bx.$$

[8]在计算机算术（通过输出结果奇偶性来模拟 $\mathbb{F}_2$ 算术）中进行此计算的问题在于，硬件输出中只有高位数元比较可靠。

得出：绝大多数矩阵比最复杂的矩阵最多简单一个常数数量级[9]。

[9]再者，任何线性转换比随机输入最多简单一倍，因为可均匀选样 r, s 满足 $r + s = x$ 即 $Tx = T(r + s) = Tr + Ts$，两个（边缘）随机输入值的线性转换的加和。

第 4 章 oPoW 系统实践应用中的具体考量

以下部分作者讨论 oPoW 在实际情况中的运用需要的基本条件。这些讨论意于提出关键点，并非详尽。

4.1 节能目标

想要利用 oPoW 实现相对于传统 PoW 区块链的大幅度节能目标，必须满足以下两个条件：

1. 光学辅助处理器挖矿机解答每哈希函数所需成本（摊销资本支出 + 运营支出）比其他硬件低（如 ASIC，GPU）。

2. 光学辅助处理器挖矿机解答每哈希函数所需成本中资本支出/运营支出的比例必须比当今运营比特币和以太坊的硬件（如 ASIC，GPU）高出一个数量级。

在与其他研究者和光学计算硬件公司进行详尽讨论后，作者相信以当今技术的发达程度，这两个条件是完全可以实现的。oPoW 现实运用的效果可以为此提供实践考察数据。

4.2 去中心化

假设大幅度节能可以实现，挖矿产业会自然实现去中心化。以下作者简单探讨两方面问题。

4.2.1 地理位置去中心化

虽然能源成本不能降低为零因而电价低廉的区域依然能提供节约小部分成本的优势，但是能源不再是利润率的决定因素。有大量的挖矿机试图在电价昂贵但是律法对虚拟货币产业友好的国家进行挖矿（如马耳他），但如今在这些地区投资挖矿机没有潜在投资回报，因为区块奖励的价值无法补偿高运营成本。oPoW 能够民主化挖矿产业，使挖矿机能在对虚拟货币友好，政治风险低，资本成本低的司法管辖区运营。

作者预测大型挖矿公司会持续在能源成本低的地区参与传统 PoW 区块链挖矿，市场竞争也较小，然而在 oPoW 区块网络中会不断出现新竞争者加入挖矿产业。

4.2.2 硬件制造商去中心化

除了高能效性能，硅光学的优势还在于较低的一次性工程费用，因为硅光学电路的制造可利用老一代处理节点（例如，200nm SOI[58], 90nm SOI[59] vs 比特币 ASIC 使用的 7nm SOI[60]）。较低一次性工程费用能降低制造商进入市场的成本和限制，保障在长远未来 oPoW 挖矿机制造商处在一个健康的竞争环境。再者，用于 oPoW 挖矿机的光学辅助处理器构架在人工智能领域有更广泛的应用，作者预测 oPoW 挖矿机制造商会因此面

临更激烈的竞争。市场上不仅有许多商业生产人工智能光学辅助处理器的公司，也有对其他模拟向量矩阵乘法计算法的研究，比如忆组器交叉阵列和其他类脑电子结构，这些最终都会发展成新的矿机竞争对手进入市场。从一个更广义的角度思考：用于 SHA256 哈希函数的硬件在虚拟货币之外并没有太高的计算能力价值，然而硅光学处理器除了应用于虚拟货币系统有更广泛的应用领域。前者硬件市场较后者更容易孕育垄断制造商。

4.2.3 实现最大能效性所需容错性

光学辅助处理器上数模转换和模数转换过程，散粒噪声，温度浮动及其他因素都是产生噪声的源头，这说明追求高准确性必须牺牲能效性[41]。为了最大程度实现光学模拟计算的能效性，oPoW 算法必须具备容错性（牺牲准确性）。

假设一矩阵大小为 256×256[1]，第三部分中提议的重型哈希函数便是不切实际的，因为其输出向量中每四位元值中最低有效位得错误率[2]高达 10^{-3}。该错误率在商业用途中的光学硬件中是可行的，然而在此算法的未来版本中，作者希望能完成将容错性提升到容忍最低有效位 10^{-1} 错误率的长远目标。这个目标数值与深度神经网络提供的数值相符，错误率大于等于此数值时元件不再有耐噪性[41,61]，因此作者理性推断用于 MAC 计算的光学辅助处理器不会在更高噪音环境下工作（无论是否存在更低能耗的可能性）。

[1]对于此论文中参考的商业光学辅助处理器结构，此数值是一个合理的中间目标。提升矩阵大小超过 512×512 是很难做到的，因为用来调整参数的控制电路数量提升是矩阵大小提升的二次元，在某些结构中，矩阵增加的每一行需要令增加复合波（multiplexed wavelength）。

[2]矩阵向量乘积输出的所有 256 个数值都不存在 LSB 错误的概率是 $0.999^{256} = 77.4\%$，也就是说 22.6% 的试验结果会被浪费，这是可以接受的。

第 5 章 展望长远未来

虚拟货币过去五年内虚拟货币从一个概念发展到早期商业化阶段。尽管我们很难真正预测虚拟货币技术的长远未来，但该技术显然为加强全球金融系统运作效率和公平性提供了一个机会。虚拟货币市场可作为危机情况下的安全阀门这一点我们已在现实中见证：津巴布韦，委内瑞拉等国法定货币系统的崩溃拉动了当地国民对比特币的需求。随着虚拟货币越来越稳定，实用，易操作，它将在越来越广的范围内与传统金融系统竞争。

硅光学辅助处理器光学行业希望能复制硅光学技术在数据交流应用中的成功于计算应用中。用光学代替电子进行计算带来的巨大优势是显而易见的，然而，想要实现光学计算的广泛运用，我们必须首先解决许多现实工程难题。采用硅光学技术让我们可以直接利用已有的标准化半导体生产链，这解决了最主要的工程难题，但是还有许多问题尚未解决，例如缺乏硅镭射源[1]。人工智能领域内，能与半导体兼容的非线性光学组件是一个活跃的研究对象，但其利用还未被商业化。再者，硅光学电路组件之间的制造差异通常是通过微型加热器[2]来调整的，这提高了光学电路的整体耗能。作者预测 oPoW 应用的简单性（硬件只需进行为光学计算定制设计的强力计算，几乎没有内存要求）将迈出光学辅助处理器技术进入主流商业规模的第一步。

oPoW 体系想要扩大比特币及其他价值储藏虚拟货币的规模，使其满足全球需求量，技术创新和社会创新两者缺一不可。许多研究员和技术发展人士正努力通过链下发展，如闪电网络[3]，或通过区块链创新技术，如 MimbleWimble/大零币 Zcash/门罗币 Monero（隐私性）和 DAGs（可扩展性），来提升系统性能。企业家正努力拉动新用户加入网络以及改良非技术性使用者的用户体验。然而，除了使用可在生能源进行比特币挖矿的尝试和努力（尽管仍然来自中心化集团），PoW 在 2012 年比特币挖矿 ASICs 的出现后并没有见证更多创新。

PoWx 的目标是利用新一代计算技术的优势改变此现状。去中心化价值储藏系统的规模若要扩展到一个新的数量级，PoW 生态系统需要经历一个从根本上的转化。oPoW 只需对现存 PoW 算法机制进行极小的修改，因而保留 PoW 的优良安全性能，同时能解决比特币和其他虚拟货币面临的一些根本问题。oPoW 能够打破虚拟货币对发电站的依赖，使挖矿在地理位置上去中心化，因而提高整体系统安全性。同时，oPoW 能够改善哈希率相对虚拟货币价值的敏感性，民主化货币发行。oPoW 的应用还能够促进高能效光学辅助处理器的发展，成为该技术进入更广泛应用的踏脚石。

[1] 混合型硅 III-V 镭射[62-63] 以及其他与硅镭射有关的尝试[64-65] 都已经获得不小的成功。

[2] 有许多想要取代微型加热器的尝试，比如非易失性相变材料调节[66]。

[3] 闪电网络是为提高比特币网络系统每秒交易量设计的网络系统，其在链下渠道记录交易，然后把帐目记录结合起来一次性记录在比特币区块链上。

致谢

作者感谢 PoWx 公司提供的部分资金资助。作者感谢 Sunil Pai（斯坦福）帮助设计芯片样板, Mustafa Hamood, Stephen Lin, Jaspreet Joha (SiEPIC/University of British Columbia) 帮助制造和测试芯片样本。作者还要感谢 Guy Corem (Beam), Bram Cohen (Chia), Tom Brand (Starkware), Yichen Shen (Lightelligence), Mitchell Nahmias (Luminous Computing), Yonatan Sampolinsky (DAGlabs), John Tromp (Grin) 在研究进程讨论中提供宝贵的意见和反馈。

参考文献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[M/OL]. Working Paper, 2008. https://bitcoin.org/bitcoin.pdf.

[2] BACK A. Hashcash-a denial of service counter-measure[EB/OL]. 2002. http://www.hashcash.org/papers/hashcash.pdf.

[3] LAMPORT L, SHOSTAK R E, PEASE M C. The byzantine generals problem[J]. ACM Trans. Program. Lang. Syst., 1982, 4(3): 382-401.

[4] DWORK C, NAOR M. Pricing via processing or combating junk mail[C]//Lecture Notes in Computer Science: volume 740 CRYPTO. [S.l.]: Springer, 1992: 139-147.

[5] Ethereum wiki[J/OL]. GitHub. https://github.com/ethereum/wiki/wiki/Ethash.

[6] BENTOV I, HUBÁČEK P, MORAN T, et al. Tortoise and hares consensus: the meshcash framework for incentive-compatible, scalable cryptocurrencies[J]. IACR Cryptology ePrint Archive, 2017, 2017: 300.

[7] SOMPOLINSKY Y. Phantom , ghostdag : Two scalable blockdag protocols[Z]. [S.l.: s.n.], 2018.

[8] Cambridge bitcoin energy index[J/OL]. CBECI. https://www.cbeci.org/.

[9] IEA. IEA energy statistics[J/OL]. IEA. www.iea.org/statistics/electricity.

[10] TORPEY K. Blockstream reveals massive mining operation[J/OL]. Forbes. https://www.forbes.com.

[11] DOFFMAN Z. Putin signs 'russian internet law' to disconnect russia from the world wide web[J/OL]. Forbes, 2019. https://www.forbes.com.

[12] GOH B. China wants to ban bitcoin mining[J/OL]. Reuters, 2019. https://www.reuters.com.

[13] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking bitcoin: Routing attacks on cryptocurrencies[C]//2017 IEEE Symposium on Security and Privacy (SP). [S.l.]: IEEE, 2017: 375-392.

[14] GAZI P, KIAYIAS A, RUSSELL A. Stake-bleeding attacks on proof-of-stake blockchains [C]//CVCBT. [S.l.]: IEEE, 2018: 85-92.

[15] ABUSALAH H, ALWEN J, COHEN B, et al. Beyond hellman's time-memory trade-offs with applications to proofs of space[C]//Lecture Notes in Computer Science: volume 10625 ASIACRYPT (2). [S.l.]: Springer, 2017: 357-379.

[16] MORAN T, ORLOV I. Simple proofs of space-time and rational proofs of storage[C]// Lecture Notes in Computer Science: volume 11692 CRYPTO (1). [S.l.]: Springer, 2019: 381-409.

[17] TROMP J. Cuckoo cycle: A memory bound graph-theoretic proof-of-work[J/OL]. Financial Cryptography and Data Security Lecture Notes in Computer Science, 2015: 49–62. DOI: 10.1007/978-3-662-48051-9_4.

[18] AMODEI D. AI and compute[J/OL]. OpenAI, 2019. https://openai.com/blog/ai-and-compute/.

[19] Marr B, Degnan B, Hasler P, et al. Scaling energy per operation via an asynchronous pipeline[J/OL]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2013, 21(1): 147-151. DOI: 10.1109/TVLSI.2011.2178126.

[20] TAIT A, De Lima T, ZHOU E, et al. Neuromorphic photonic networks using silicon photonic weight banks[J/OL]. Scientific Reports, 2017, 7(1). DOI: 10.1038/s41598-017-07754-z.

[21] SHEN Y, HARRIS N C, SKIRLO S, et al. Deep learning with coherent nanophotonic circuits[J/OL]. 2017 IEEE Photonics Society Summer Topical Meeting Series (SUM), 2017. DOI: 10.1109/phosst.2017.8012714.

[22] CARTWRIGHT S. New optical matrix–vector multiplier[J/OL]. Applied Optics, 1984. DOI: 10.1364/ao.23.001683.

[23] JAEGER H. The "echo state" approach to analysing and training recurrent neural networks[J]. German National Research Center for Information Technology GMD Technical Report, 2001, 148:34.

[24] MAASS W, NATSCHLÄGER T, MARKRAM H. Real-time computing without stable states: a new framework for neural computation based on perturbations.[J/OL]. Neural Comput, 2002, 14: 2531-2560. http://dx.doi.org/10.1162/089976602760407955.

[25] DOMINEY P F. Complex sensory-motor sequence learning based on recurrent state representation and reinforcement learning[J]. Biological Cybernetics, 1995, 73: 265-274.

[26] ILIES I, JAEGER H, KOSUCHINAS O, et al. Stepping forward through echoes of the past: forecasting with echo state networks[R]. [S.l.]: Jacobs University, 2007.

[27] JALALVAND A, WALLENDAEL G V, WALLE R V D. Real-time Reservoir Computing Network-based Systems for Detection Tasks on Visual Contents[J/OL]. 7th International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), 2015: 146-151. DOI: 10.1109/CICSyN.2015.35.

[28] FERNANDO C, SOJAKKA S. Pattern recognition in a bucket[C]//Lecture Notes in Computer Science: volume 2801 ECAL. [S.l.]: Springer, 2003: 588-597.

[29] LARGER L, BAYLÓN-FUENTES A, MARTINENGHI R, et al. High-Speed Photonic Reservoir Computing Using a Time-Delay-Based Architecture: Million Words per Second Classification[J/OL]. Physical Review X, 2017, 7(1): 011015. DOI: 10.1103/PhysRevX.7.011015.

[30] SHOJI T. Low loss mode size converter from 0.3 μm square si wire waveguides to singlemode fibres[J/OL]. Electronics Letters, 2002, 38: 1669-1670(1). https://digital-library.theiet.org/content/journals/10.1049/el_20021185.

[31] XU Q, SCHMIDT B, PRADHAN S, et al. Micrometre-scale silicon electro-optic modulator[J/OL]. Nature, 2005, 435(7040): 325–327. DOI: 10.1038/nature03569.

[32] CHEN L, LIPSON M. Ultra-low capacitance and high speed germanium photodetectors on silicon[J/OL]. Opt. Express, 2009, 17(10): 7901-7906. http://www.opticsexpress.org/abstract.cfm?URI=oe-17-10-7901. DOI: 10.1364/OE.17.007901.

[33] CHROSTOWSKI L, HOCHBERG M E. Silicon photonics design[M]. [S.l.]: Cambridge University Press, 2015.

[34] Silicon photonics reaches tipping point, with transceivers shipping in volume[J/OL]. Semiconductor Today. http://www.semiconductor-today.com/news_items/2018/jan/yole_220118.shtml.

[35] SAADE A, CALTAGIRONE F, CARRON I, et al. Random projections through multiple optical scattering: Approximating Kernels at the speed of light[C/OL]//ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings: 2016-May. 2016: 6215-6219. DOI: 10.1109/ICASSP.2016.7472872.

[36] BUENO J, MAKTOOBI S, FROEHLY L, et al. Reinforcement learning in a large-scale photonic recurrent neural network[J/OL]. Optica, 2018, 5(6): 756. DOI: 10.1364/optica.5.000756.

[37] PRUCNAL M N, Paul R., SHASTRI B J. Neuromorphic photonics[M]. [S.l.]: CRC Press, 2017.

[38] WIGGERS K. Lightelligence releases prototype of its optical ai accelerator chip[J/OL]. VentureBeat, 2019. https://venturebeat.com.

[39] LTD S E. Lightmatter lands 33m dollars to marry photonics with ai[J/OL]. Optics.org. http://optics.org/news/10/2/32.

[40] Bill gates, neo, gigafund backing luminous in photonics supercomputer moonshot [EB/OL]. 2019. https://techcrunch.com.

[41] NAHMIAS M A, LIMA T F D, TAIT A N, et al. Photonic multiply-accumulate operations for neural networks[J/OL]. IEEE Journal of Selected Topics in Quantum Electronics, 2019: 1–1. DOI: 10.1109/jstqe.2019.2941485.

[42] MILLER D A B. Attojoule optoelectronics for low-energy information processing and communications[J/OL]. Journal of Lightwave Technology, 2017, 35(3): 346–396. DOI: 10.1109/jlt.2017.2647779.

[43] BANGARI V, MARQUEZ B A, MILLER H B, et al. Digital electronics and analog photonics for convolutional neural networks (DEAP-CNNs)[J]. arXiv preprint arXiv:1907.01525, 2019.

[44] DE LIMA T F, PENG H T, TAIT A N, et al. Machine learning with neuromorphic photonics[J/OL]. J. Lightwave Technol., 2019, 37(5): 1515-1534. http://jlt.osa.org/abstract.cfm?URI=jlt-37-5-1515.

[45] VORICK D. The state of cryptocurrency mining by david vorick[J/OL]. Sia Blog. https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b.

[46] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030.

[47] HEILMAN E, NARULA N, DRYJA T, et al. Iota vulnerability report: Cryptanalysis of the curl hash function enabling practical signature forgery attacks on the iota cryptocurrency [R]. [S.l.]: MIT Media Lab, 2017.

[48] PAI S, BARTLETT B, SOLGAARD O, et al. Matrix optimization on universal unitary photonic devices[J]. Physical Review Applied, 2019, 11(6): 064044.

[49] RECK M, ZEILINGER A, BERNSTEIN H J, et al. Experimental realization of any discrete unitary operator[J/OL]. Physical Review Letters, 1994, 73(1): 58–61. DOI: 10.1103/physrevlett.73.58.

[50] RUSSELL N J, CHAKHMAKHCHYAN L, O' BRIEN J L, et al. Direct dialling of haar random unitary matrices[J/OL]. New Journal of Physics, 2017, 19(3): 033007. DOI: 10.1088/1367-2630/aa60ed.

[51] Pai S, Williamson I A D, Hughes T W, et al. Parallel fault-tolerant programming of an arbitrary feedforward photonic network[J]. arXiv e-prints, 2019: arXiv:1909.06179.

[52] Bitcoin hashrate vs. price in usd chart[J/OL]. BitInfoCharts. https://bitinfocharts.com/comparison/hashrate-price-btc.html.

[53] HUILLET M. China: Bitcoin mining behemoth bitmain releases new 7nm antminer hardware[J/OL]. Cointelegraph, 2019. https://cointelegraph.com.

[54] BELLARE M, ROGAWAY P. Random oracles are practical: A paradigm for designing efficient protocols[C/OL]//DENNING D E, PYLE R, GANESAN R, et al. CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993. ACM, 1993: 62-73. https://doi.org/10.1145/168588.168596.

[55] JOUPPI N P, YOUNG C, PATIL N, et al. In-datacenter performance analysis of a tensor processing unit[C]//ISCA. [S.l.]: ACM, 2017: 1-12.

[56] JOHNSON J. Making floating point math highly efficient for AI hardware[J/OL]. Facebook AI Blog. https://ai.facebook.com/blog/making-floating-point-math-highly-efficient-for-ai-hardware/.

[57] EYAL I, SIRER E G. Majority is not enough: bitcoin mining is vulnerable[J]. Commun. ACM, 2018, 61(7): 95-102.

[58] Aim photonics foundry[EB/OL]. 2019. http://www.aimphotonics.com/.

[59] Global Foundries. Global foundries silicon photonics[EB/OL]. 2019. https://www.globalfoundries.com/technology-solutions/silicon-photonics.

[60] NEWS B. Bitmain announces new 7nm bitcoin mining chip with 29 percent more efficiency[EB/OL]. 2019. https://news.bitcoin.com.

[61] Reagen B, Gupta U, Pentecost L, et al. Ares: A framework for quantifying the resilience of deep neural networks[C/OL]//2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC). 2018: 1-6. DOI: 10.1109/DAC.2018.8465834.

[62] Sun X, Liu J, Kimerling L C, et al. Toward a germanium laser for integrated silicon photonics[J/OL]. IEEE Journal of Selected Topics in Quantum Electronics, 2010, 16(1): 124-131. DOI: 10.1109/JSTQE.2009.2027445.

[63] FANG A W, COHEN O, JONES R, et al. Electrically pumped hybrid algainas-silicon evanescent laser[J/OL]. Optics Express, 2006. https://www.osapublishing.org/oe/abstract.cfm?uri=oe-14-20-9203.

[64] OTTERSTROM N T, BEHUNIN R O, KITTLAUS E A, et al. A silicon brillouin laser[J]. Science, 2018, 360(6393): 1113-1116.

[65] RONG H, LIU A, JONES R, et al. An all-silicon raman laser[J]. Nature, 2005, 433(7023): 292.

[66] ZHANG Y, CHOU J B, SHALAGINOV M, et al. Reshaping light: reconfigurable photonics enabled by broadband low-loss optical phase change materials[C/OL]//GEORGE T, ISLAM M S. Micro- and Nanotechnology Sensors, Systems, and Applications XI: volume 10982. SPIE, 2019: 98 - 105. https://doi.org/10.1117/12.2513385.