可信赖的数据：区块链技术

Data You Can Trust: Blockchain Technology

美国空军退役上校文森特·阿尔卡扎（Col Vincent Alcazar, USAF, Retired）

他们说，山雨欲来风满楼，但愿他们有时不要无风不起浪？

—奥古斯塔·艾达·金－诺尔，勒芙蕾丝伯爵夫人

变革实例

美军仍在等候网络中心战(NCW)的突破，以便能提供变革美国作战方式的技术引领和作战进步。不过，在过去 10 年里，美军获得了神器：互联网接入、便携计算、智能手机引进等等。这些技术先进的神器，通常被误认为预期的 NCW 突破。这些神器的核心是迭代式装置，以及机器生产力的提高。如果 NCW 有隐伏的弱点，就是其硬件的定向。对神器的注重引出一个问题：在这些硬件、装置、网络和相关的基础设施内传输的数据会怎么样呢？尽管技术和处理取得巨大进步，今天的软件和硬件外壳—环绕和分发数据的装置—长期以来仍然易受攻击。在历史反复的洞察中，一个军队的薄弱环节—无论是潜在的或是公认的—能成为敌人突袭行动的焦点。不过，阻碍美国作战方式的突袭无需是战略性的。面对如此环境，该怎么办呢？

在美国数据的漏洞，以及可能受到网络空间突发事件影响的背景下，战士们和战士们的领导者需要采取不同的态度，本文提出一个大胆的想法，即推广一种能减缓国防部中央数据保护模式弱点的可行技术。这个更好的（大胆）想法不应该是继续近乎完全排他式地聚焦在迭代型军用计算机的改进上。而是，这个更好的想法应该为军队的信息技术（IT）设备处理、储存和发送数据增强安全性提出一个设计纲要。这个更好的想法已经存在；它就是区块链技术。简而言之，区块链是以一种使数据不能被损坏的方式储存数据的技术，而此种功能是经由其集成数据分类帐来完成。采取区块链领先技术的原因有两个方面：避免不利的破坏风险和最大化有利的作战机会。关于不利的风险，战士们需要降低因为缺乏可信数据而产生的作战干扰和恶化，因为我们很多武器系统需要数据才能有效地发挥作用，如果真能发生作用的话。区块链的有利方面是，美军可以完全排除敌人会损毁和破坏我们数据的可能性。第一个原因很重要，第二个原因在战争中能扭转乾坤。

区块链大创意的发展，以及机器的改进，显示资源受到限制的国防部 IT 成本的巨大增加。但是，区块链已经存在，节省数百万美元的研发资金，缩短了研发项目的数年时间。从根本上说，区块链是与现有的国防部网络兼容的数据管理和数据分发技术。它的颠覆性设计保护并记录数据，使数据免遭篡改和损坏。区块链使我们的军队免于同国家和非国家行为者持续的竞争，他们作为攻击者，有强烈的动机和灵活的利用开发循环，能实现一场不公平的竞争。巨大不利和极其无效的几何结构导致这种竞争场地的不公平性，迫使必须一直保持正确的减少系统硬件

/ 软件威胁的努力，去对抗一种威胁安全环境，在这种环境中，心意已决的攻击者只需短暂成功。为了让竞争朝着有利于美军的方向发展，理想的解决办法直指结合区块链技术和美国计算机 / 系统的独创性。

问题、论点和假设

数据已成为现代军事组织的关键依赖。在实践中，缺少及时、准确的数据迫使军队及其领导人凭借主观臆想作战。一般而言，主观臆想的知觉和决策的方法会产生问题。一个骑在马背上的人俯瞰战场指挥军队很成问题。在本世纪，缺少确凿的数据可能会造成任何军队在多个领域中的重大失败。这里的悖论是，美国的分布式作战模式，只有当其大量、日益增长的数据需求经由已知安全的审查过的数据定期供给时，才能达到其全部的潜能。国防部内的数据边缘用户知道，问题不是我们机器对数据的需求，或那种需求的规模。[1] 关于现状的任何问题说明，不是简单的几句话，而是围绕着一组相互关联问题绘出的一个圆圈：在我们 IT 系统中传送的数据的可靠性，以及战士们执行战斗所需要的数据是什么？那个作战数据曾否被部分或全部篡改？那个数据是真的可靠，还是仅仅表面上可靠但实际上是由一个聪明的攻击者伪造并植入的？数据的发送者是可靠的机构，或者所谓的来源实际上是寻求造成严重破坏的系统间谍？那些问题中哪些是应该解决的问题，依次顺序是什么？事实上，战士们并不在意，但是他们从 IT 专家听到的答案是要同时处理所有这些问题。因此，每一件事要使用单独的方式在单独的空间内解决。

要打赢保护和控制我们 IT 系统的战斗，需要巨大的资源支出。但是，如果我们转移答案的重点，把他们建议的上述所有疑问和问题搁置一旁，情况会如何呢？如果我们不问能对 IT 系统重新做点什么，而是我们能对数据本身重新做点什么呢？由此引入区块链，它侧重数据的问题和答案。有鉴于此，本文的论点是，如果国防部部署区块链——一种新型和截然不同的数据管理技术——那么，今天的数据攻击破坏性就要小很多，其主要的好处是，战士们手中的数据，由于几乎不能被毁坏，变得极为可靠。

接下来，本文的假设是，为了更好地保护美军网络中的作战数据，已知最好的数据技术解决方案是区块链。换言之，区块链能帮助战士减少我们不断经历的网络攻击，同时避免来自意料之外的、未记载的、未标明的、以及未知的 IT 硬件 / 软件漏洞被侵入的损失。

区块链概述

2008 年，一个笔名叫中本聪的人出版了目前流通甚广的白皮书，概述了比特币的概念及其生成的基本原理系统，即区块链技术。[2] 区块链可能是真正值得被称为颠覆性数据技术的第一种技术。区块链不仅是对现有数据记录和记载技术的跨代进步。它的重要性在于其具有消除我们现有网络设计关键弱点的能力：对网络信任管理政策的危害。信任管理功能，由于其在所有计算机网络中，包括在军方使用的计算机网络中发挥关键的作用，常常是攻击的目标。信任管理人员控制两个关键的功能：用户认证和存取控制。信任管理依靠一种硬件装置及其软件来发挥中间人的角色，确保用户和他们的数据交易信任可靠。[3] 攻击者通过攻击用户的认证，能进入网络，获取最终的数据目标集，达到他们攻击的目标。

缔造区块链的设计者明白网络设计模式固有的局限性，这种模式需要一个信任管理员的存在。在建立区块链的内在形式和逻辑时，他们在新的操作框架中开拓了一种技术，把今天的战士们了解的国防部基于系统计算的众多弱点抛开。下面各点概述了区块链具备何种特性和为什么能成为一种颠覆性的技术。

区块链是一种新优势来源

传统的安全网络设计将信任关系管理和守门员角色置于中心位置，在网络的层级结构中具有完全的权限。通过去除信任管理中间人角色的必要性，区块链去除对集中权力的要求。中央控制的缺席赋予一种可伸缩性，使区块链网络能够在任何规模的阈值以相同的效能和效率发挥作用；从突击小组到大规模联合特遣部队等等。区块链的另外一个优点是其分散式的结构（扁平化组织）以及不集中的逻辑（较少的由上而下）能减少延迟。更多平行、更少垂直结构克服了军事网络中的很多挑战，这种网络因失去集中的信任管理员而充满风险。换言之，让区块链更强大，不是应该对区块链做的事情，是区块链本身。

块链翻转了数据集中模式

先进持续性威胁 (APT) 和国家以及非国家行为者都对美军网络设计施加巨大影响。那些威胁迫使我们做出广泛的防御反应，把数据存储在更精心保护的高墙之内，在更多层的安全庇护之下。这种威胁、防御和反应心态带来的是，不断地增加数据存储筒仓的数量。数据的安全成为其本身的目标，从这个目标传送出意料之外的结果：数据的割据。对数据管理员来说，这种构架既正确也合适。但是，对于那些在多个领域，从越来越分布的战场阵地作战的战士们来说，筒仓把作为战争工具的数据放置的太远，而不是其在战争中应该唾手可得的位置。

区块链重塑数据防护

区块链并不能使所有可想象的行为者和威胁变得毫不相关，没有任何可负担得起的军事网络设计能够做到这些。但是，网络撷取器工作证明的区块链结构，以及其数据交易的分布式分类帐，极大地减少了数据窃取、数据毁损，以及发送方身份泄露的可能性。[4] 此外，区块链的数据加密标准，SHA-256，使得反向利用发送者信息内容的代价昂贵和费时。即使一名对手能经济划算地破解 SHA-256 的加密标准，在战时他也极不可能快速地做到，也就是说，速度快得足以左右战局。[5]

作为编织网的区块链数据

在目前美军数据管理的愿景中，数据在数据接收器中聚合。数据存储库存在的本身就招致攻击。如果某人创建一个数据结构，其数据是黄金，这个人就置那堆数据于经常的危险之中。区块链位于数据存储的顶端。的确，数据仍然为王，但是，在每个数据块被加入到区块链网络分类账中时，区块链在其数据块排列中将数据隔离封存。在一个完整的区块被加入全部网络分类账后，篡改每个区块包含的数据是不可能的。

区块链的分散结构与分布式战争相辅相成

当撷取器暂时同其本地区块链网络断开时，它们并没有失去能力，只是在它们等候下一个数据交易时空转。[6] 当一个区块链网络同整体网络重新连接时，就会出现一个工作同步认证区块。所有完成的数据区块被输出到每个分类账。设计这个程序是确保，当一个网络撷取器和相关机器重启时，它们一致地作用于相同的新数据交易。这种区块链的设计，对于战士们来说至关重要。这些战士们知道，这不是如果连接受阻，而是何时连接受阻的问题。

区块链，管理作战对象网络的一个选项

区块链的结构适用于管理概念化作战对象网（BNO）—这是民间物联网的军事名称。集中的、自上而下的模式对象连接一个区块链网络中数以千计的其它 BNO 装置，发送和接收数据，而不是在 BNO 为每个对象设立一个谨慎的指挥通道。当被解密后，模式数据被加入到每个对象分类账中，或许加入到容

宿一群相关 BNO 装置分类账的主机中。不管其规模多大，区块链成为一个网络中 BNO 装置的同步化机制。区块链减轻战士们在一个充满网络对象的战场中要保持高度感知的负担；反而，使用区块链，每个 BNO 装置都了解战场。

区块链—控制装置集群的选项

区块链的分布形式，结合将被纳入集群装置的算法，释放出可靠的集群行为，因此实现了更完整的军事化潜力。区块链能在两个方面完成这种潜力：首先，提供一个集群内存来组成集群行动的基石，第二，提供集群与集群之间连接和通讯的途径。或许最令人振奋的是，区块链技术能达成各种不同层面的人—机器人互动。区块链能通过如上文所述的集群内存以及出现的动态（集群自我组织）来完成此项功能；二者都能提升集群感知。由于感知提升，集群能获得高度的自主性，在直接操作员控制不切实际，或者当操作员与集群连接受到干扰的战术情景中，这一特性非常有用。[7]

区块链如何运作?

区块链的首次互联网公开展示版本，在不同时间，不同地点登场，时间从 2008 年末到 2009 年初。[8] 区块链网络有各种规模，其特点是被称为撷取器的相互链接的计算机、分类账主机，以及同其他网络相连的连接点。撷取器是计算机，它的工作是计算复杂方程式的解决方案。[9] 椭圆曲线数字签名算法（ECDSA）是区块链的一种算法。非对称密钥加密，是发送者和接收者使用匹配的公开 / 私下密钥方法对数据交易加密和解密的方法。[10] 一旦撷取器成功确定 ECDSA 的解决方案，它被一种算法转换成 256 个字节长的数据串。[11] 这个数据串就是区块链区块技术所要求的任何给定数据交易的载荷。随着交易在网络中从 A 点移动到 B 点，作为接收方的撷取器使用各自的计算能力，反复计算公式，直到其解决方案输出数据字符串匹配发送者数据交易的数据字符串，以此来解决交易的 ECDSA 公式。一旦匹配完成，数据块几乎完成，将迅速符合条件加入到每个网络撷取器和分类主机的分类账中，即所有完成的交易记录。[12] 配对的公开 / 私下密钥技术保护解决方案，使得攻击者不能窃取或毁坏网络内的解决方案数据。我们不必是计算机科学工程师、网络管理员，或国家安全局密码破译专家才能理解区块链的作用：以简单方法使用复杂理念来生成比单纯数据更重要的东西。

安全是区块链的基石。区块链中的数字密码术非常强劲，需要单一的桌面工作站很长时间来计算所有的可能性，才能破解发送者的数据串。[13] 区块链加密的复杂性可被调整，也就是说，上调或下调复杂性。[14] 对于军事区块链的应用，这种变阻器的特性，在提供远征行动灵活性方面证明是有帮助的；有时需要更多的加密复杂性，其他时候，少些复杂性更合适。在例行实践中，现有一代的区块链网络撷取器需要平均 10 分钟才能解开标准的 SHA-256 加密方程式。[15] 但是，新的区块链技术能将计算时间减少至 3 分钟。随着下一代芯片的速度和量子芯片的商业化，可以预见，即使今天最快的计算速度都能够再被降低一个数量级（6-8 秒）。在目前 10 分钟的计算期末尾，网络执行相当于一个整体同步过程，在这个过程中，所有的网络分类账都一致更新。一个完成的区块链数据块，来自首先解决方程和匹配数据串的撷取器—被称为工作证明—作为备份被输出到各个网络机，并加入到每个分类账中—这里记录了开始以来所有的网络数据交易。想象一下运行中的区块链网络；在我们继续对数字化的追求中，区块链是一种强化我们战争方式的技术，而不使其欠灵活和更加脆弱。

在当今的网络中，当数据块完成时会发生什么，就是区块链的独特所在，超越其他数据管理办法一筹的地方。回想一下，一个网络信任管理功能的损坏，能给网络用户和数据带来问题。但是，一旦区块链区块完成，该区块的内容被密封，其数据载荷变得无法被损坏。这个过程的机制很简单：一个完成的区块是整体向每个网络主机的分类账发布。至于攻击，归根结底是，攻击者没有简易的方法损坏交易数据，所以他的手段就是攻击整个网络。但是，除了彻底摧毁那个网络以外，最坏的情况是短期受阻碍，不是长期被打败。

在军事应用中，区块链撷取器计算机可能会以不同的速度，在不同的交易中运行，在不同的时间和不同的频率断开并重新连接其网络。这样做的原因可能是计算机计算性能差异，通讯不稳定，发射控制措施，或网络遭受攻击的后果。在其中任何一种情况下，有可能发展多种区块链—能够与单一区块链竞争的多个区块链。由于可能在网络数据分类账中形成相互矛盾的数据交易，多种链本身不能持续下去。缓解这个问题的方法很简单：撷取器和参与的网络主机找出最长区块链，并且争取把未来的区块只加入到那个链中。鉴于区块链网络中进行的大量数据处理，撷取器能使用逻辑工具使区块链保持在一个事先确定的长度。随着区块链的加长，这种工具减轻主机对内存的要求。使用这种工具帮助确保军事行动中的区块链数据交易流动率维持在最可能高的速度上。[16] 结论是，区块链不仅加固数据，而且对网络性能很敏感。

区块链的用途

下列精选的例子展示区块链的根本设计将如何应用于广泛的军事任务集：

作战命令和计划文件。就数据而论，区块链的分散化示意着网络某种程度的民主化。对战场中的战士们，没有什么比必须要了解作战计划，并且随时掌握情况变化更民主和更急迫的。让作战人员掌握作战计划的相关方面，是准备和执行计划的目标之一。区块链的大飞跃在于其独特技术，它确保数据，此处指的是作战要点，能水平地传发出去；数据被保存在象石块一般的数据区块里。如果网络的某个部分同总部的网络连接出现中断，那个上级网络只需要把数据区块传递给一个从属网络的单一撷取器。在那种情况下，那个接收撷取器将按要求把那个区块和其他区块传给那个区块链网络的每个数据分类账。情况又怎么样？是作战态势感知更新、士气大振，任务继续进行下去 。

装置集群控制。设计者在研制集群装置的运输系统，这种作战方式已吸引美军的注意，工程师们正在找出集群装置的应用。集群部署的最大挑战不是装置设计或包装，而是控制。[17] 控制一个集群中数百、甚至数千个装置的一个主要局限，是专家们所说的全局知识。换言之，不仅要感知临近的装置，而是整个集群中所有装置之间共享的感知。[18] 区块链网络公开、分布的设计得以管理和协调编入每个装置内的简单操作程序，综合起来，可使一个集群感知的一切同时让所有装置知道和了解。其结果是，一个集群具有作为一个单一整体行动的能力。区块链技术解开集群的军事可能性。

后勤。由于军队和民间供应者之间交换的后勤供求数据如此之多，确保数据真实而没有被篡改至关重要。区块链的分类账逻辑确保，由可信的发送者传递的数据，以及由授权的接收者收到的数据，本质上可以被信任。考虑到其合同、协议、订货单、请购文件等，区块链在后勤方面使用的效果极好。无论这些后勤文件是否由计算机生成，区块链内在的逻辑确保每个文件都可靠，可以提取，不能损坏。

区块链的一些制约

人们已经意识到并且解决在早期实验室实验中发现的弱点；其中之一是自私的撷取器。自私的撷取器问题基于这样一种情况，一群撷取器相互串通，为了他们的利益阻止或转移交易；这是一些民用区块链环境中面临的一个挑战。自私撷取器最糟糕的例子是，一小撮无赖撷取器设法招募其他撷取器，逐渐占据上风，最终控制一个网络。研究人员发现这种现象的两个方面：首先，自私的撷取器问题有一个上限，无赖们借此最终控制网络，使其成为被彻底改造的网络。第二个发现是，对区块链逻辑进行简单的编码修改，就可从一开始排除自私的撷取器发作。[19]

工程师们发现了另外一个漏洞：女巫攻击。当一个行为者向一个网络的少数区块加入无赖的撷取器时，不是去加速解方程，而是引导那个网络区块中诚实的撷取器离开解决某种交易时，就导致这种女巫攻击。女巫攻击的影响是双重的：它降低网络的集体计算能力，放慢网络分类账的更新。修改单一的最长区块链撷取器的偏好行为，就能主动清除女巫攻击的弱点；其逻辑是，迫使撷取器把分类账区块仅加入到现存最长的链中。在某些与正常操作逻辑相矛盾的例子中，女巫攻击的矫正方法是划分撷取器群体，这样所有的撷取器输出区块都被分离成两个分开的链，直到其中一个作为最长的链出现，通常是一个单一区块。当这个单一链出现时，女巫攻击停止，较短的链被抛弃，撷取器群体恢复正常运作。

回应区块链局限性

为了让区块链更好地适用于军事应用，研发人员将回到从区块链初期汲取的见解。人工智能（AI）的进步能交叉利用，以遏制并抑制自私的撷取器，以此作为修改区块链逻辑的替代。AI 演算的另外一个用途，在于找到不规则的撷取器行为，例如早期形成的自私撷取器群组。

区块链作为一种技术继续在发展，产生新的类型和潜在的用途。一个这种创新的例子，替代区块链，是一个建立区块链网络的变体，它只寻找并处理特定的数据交易类型。另外一个区块链变体是侧链，这种特别的撷取器集群解决特定用途网络内的特殊类型交易。在军事用途中，替代区块链可能在传递情报数据交易的网络中有效用。AI、撷取器和主机可以联手过滤替代区块链网络中不同保密层次的交易。为扩展这种观点，情报区块链网络将向在同一网络中使用访问权限的用户提供数据，而不是为授权使用不同层次和计划的用户提供并行的单独网络。新增的安全特性是匿名的浏览器，它掩盖用户信息和其他相关资料的数据。[20]

在野战条件下，区块侧链可能具有重大作用。例如，执行数据传输和交换功能的任务化网络，支持特定任务，如突袭、占领、高价值目标打击等。但是，必须要做一个重要对照：目前的国防部网络向下传到战术层面（集中的，自上而下）。区块链则不同；它是分散的（水平的）。攻击者知道如何战胜集中的网络，削弱军事使命，但那是今天的问题。区块链消除了那个问题，确保任务不会由于数据安全问题而受到危及。

未来的发展，区块链 2.0 版，几年前已经出现，催生了 10 多个新的商业区块链提供者，每家公司定制的区块链技术，在依靠各种区块链类型的特定商业应用中发挥作用。其中一家这样的公司，ADEPT，是国际商用机器公司和以太坊基金会联合开发。这家公司在发展用于民用物联网应用程序的区块链。[21] 以太坊基金会的区块链变体将彻底改变互联网，从其目前的状态，转变成一个替代状态，其中的记录、契约文件与合同等等不再被第三方政府或商业实体储存和拥有。从这个角度看，

区块链储存和提取应用程序成为二十一世纪首选数据储存地点。[22] 对于战士们来说，所有这些意味着，区块链已经呈现新的形式，足以发展成为军队定制的应用程序，支持我们各种各样的使命。

区块链撷取器要求大量的计算能力。支撑宿主撷取器的足够大设施，最可能设在稳定状态的基地，港口和枢纽。如果要把撷取器向前线部署，靠近作战部队，军事化的撷取器设计必须耗电低，占用空间少并适当加固。要让区块链部件部署就绪，还有一些工作要做。

采纳更好的新技术

区块链是早已存在的密码学技术，不过以新应用程序概念来表达，它主要的效益是确保作战人员对他们从国防部网络中获取数据的真实性和安全性的高度信任。归根结底，区块链给予作战人员他们需要的东西—可靠的数据。作为一个好处，可靠的数据解决了战斗人员的担忧—其他人不能破坏的数据。把这个概念变成实际用语：在作战中，我能信任数据帮助降低网络漏洞，并且保持作战势头吗?

美国军方在大刀阔斧地推动区块链开发吗？没有。原因是对这种新想法和不明确的发展道路抱持的并非根深蒂固的怀疑。尽管国防部迷恋创新，但一种经常“不是在这里发明”的态度，对挑战现状规范的想法和事物不予考虑并关闭大门。想想托马斯·库恩撰写的《科学革命的结构》，还有其他国防部的批评者发现一个避开新思想的原因，因为乍一看这些新想法还不成熟；雷达或喷气推进技术在他们首次横空出世时也是一样。当然，这种洞察力是，有时候必须要超越眼前的约束，放眼未来，才能看到某个技术的最终成果。除此之外，更好地保护国防部数据的想法，或至少更多的数据，并不被看作如同向美国庞大的军事数据企业硬件方面增加注入数十亿美元那么可信。

最后，有一件事我们能直截了当地说：为军事应用获取数据很重要；保护这些数据是关键。开发区块链，然后进行部署，以此提升数据安全，并增强国防部接触的每个武器系统的作战效绩。★

注释:

1. 边缘用户包括静态指挥控制节点外的所有用户，它强调战术用户—在远征环境下的战士。
2. Satoshi Nakamoto,“Bitcoin: A Peer-to-Peer Electronic Cash System,” accessed 1 September 2016, http://www.bitcoin.org/bitcoin.pdf.“比特币：点对点电子现金系统”。
3. Michael Crosby, et al., Blockchain Technology, Sutardja Center for Entrepreneurship and Technology, 16 October 2015, 3.“区块链技术”，2015 年 10 月 16 日，加州大学周秀文创业科技中心。在网络系统操作员之外，很多用户几乎并不识别网络的信任活动。克罗斯比等人引用熟悉的活动作为网络中间人信任活动的产品：核实某人的电子邮件被投递到收件箱中，脸书查证某人的帖子只同加入朋友的联系人分享等。
4. 在这篇文章中，真实性指的是确证一个特定用户的身份。
5. 安全散列算法 (SHA)-256 标准包含高度信任的数字序列，长达 256 个字节。SHA 方法根植于 NSA 工作中，以改进经由信息协议传输的数据串的完整性。使用长度 256 个字节的数据串，等于是 2256 个可能的数据变体，一个信息接收能运行考虑在传输前 / 后特定文档的 SHA-256 数据串的简单例行程序。SHA-256 标准的能力是 2256 的运算能力。为了把处理时间降低到几分钟，网络的撷取器相互竞争，但最终相互合作，汇集他们的运算能力，获得正确的匹配 -- 解决方案。未来的军事区块链应用可能利用甚至是更强大的 SHA 数据串，如 512，1064 等。
6. 区块链撷取器是为特殊目的而设计的机器，具有强大的处理能力，计算每个 SHA-256 交易数据串的独特解法。

7. Blockchain will not cause devices to operate as a swarm; rather, blockchain is the means by which the swarm can attain the global knowledge within machines innate to swarming creatures in nature. 区块链不会导致装置作为一个集群来运行，区块链是集群能在具备自然界集群生物固有特性的机器内获得全局知识的一种途径。

8. Crosby, 5. 克罗斯比。

9. Erik Rykwalder, "The Math behind Bitcoin," Next World with Michio Kaku, 19 October 2014, http://www.coindesk.com/math-behind-bitcoin/. "比特币背后的数学"，

10. 同上。注：在区块链中使用的 ECDSA，同其他椭圆曲线密码算法相关。ECDSA 的原理很简单：声音密码学取决于抗侵入数学工作的原理。由于区块链需要公开和私人密钥来完成数据信息（交易），才使用 ECDSA。在区块链中，解决方法是对独特解决方法的识别，但是信息交易在解决方法同发送者加密的解决方法串匹配后才得以完成。这种完成，直到数据块被标记上时间，才算完成。一个完整的区块符合加入到那个撷取器本身分类账的条件；一旦完成后，在该区块被加入全部那个特定网络分类账后，才验证撷取器的工作证明。

11. 在区块链中，其原理是：在 SHA-256 算法中处理的数字对象（ECDSA 计算）其产生的结果几乎是独特数据输出，这被称为散列 -- 原始对象的数字指纹。

12. Ibid., 6. 同上。

13. 同上。8-11。在一个 32 字节的 20 兆赫兹时钟速度工作台芯片（大约 224 散列 / 秒）上，估计单一的机器将需要 13 万 9461 年的时间才能匹配 256 个字节的输入 / 输出数据串。更强大芯片的计算功能，能产生更短的输入 / 输出间隔。军事化的任务是在轻微集群的装置中，在 SHA 加密的鲁棒性和规模经济芯片性能之间取得平衡。已经"更轻的"区块链技术在商业上是可行的，其计算间隔从 10 分钟减少到 3 分钟。

14. 支持比特币的基本区块链加密标准，是安全散列算法 (SHA)，其长度是 32 字节（256 二进制数字）。

15. 在支付行业的区块链系统中，与这种同步化周期相关的是合成的。在军事应用中，时间可以增加或减少。莱特币使用 2.5 分钟的同步周期。

16. 这种逻辑工具被称为默克尔树。要恢复使用过的计算机磁盘空间 -- 用于此前计算的内存 -- 当计算链达到一个给定的长度时，撷取器内置的长度限制器开始工作，从旧的数据块中削减数据链。这里运行着一个更深的关系，与在底部跟数据块固有的散列码有关一削剪链从这里开始。随着每个资料撷取器节点的计算能力的增加，在各自默克尔树能够被保留的链的数量，与其他撷取器内存不同；但是，从内存中移除的区块数量，从不超过确保不受干扰网络运行所需的最低数量。

17. Peter Coy and Olga Karif, "This Is Your Company on Blockchain," Bloomberg Businessweek, 25 April 2016, 8, accessed 2 September 2016, http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain. "这是区块链中的你们公司"。

18. Eduardo Castell ó Ferrer, "The Blockchain: A New Framework for Robotic Swarm Systems," (Cambridge, MA.: MIT Lab, 3 August 2016), 3, https://www.researchgate.net/publication/305807446_The_blockchain_a_new_framework_for_robotic_swarm_systems. "区块链：机器人集群体系统新框架"。

19. 通过减少实现网络共识所需撷取器的数量来完成该修复。在这种情况下，整体阈值降低，这作为一种工具，防止自私的撷取器共谋。

20. The TOR anonymizing browser is one such example. 洋葱路由器匿名浏览器就是这样一个例子。

21. Ethereum is a Swiss nonprofit organization, www.ethereum.org. 以太坊是瑞士的一个非政府组织。

22. Cellabz, "Blockchain and Beyond," Cellabz, Inc., Paris, France, November 2015, Version 1.0, 16. "区块链及未来"。

文森特·阿尔卡扎，空军退役上校（Col Vincent Alcazar, USAF, Retired），于 2014 年 12 月自现役空军退役。在他的军旅生涯中，曾担任拥有 3,800 小时飞行各型战斗机经验的资深战斗机飞行员，联合专业本科飞行员训练计划飞行教官，F-15 正规训练单位飞行教官，及乔治亚州慕迪空军基地第 479 飞行训练大队和第 479 作战支援中队指挥官。上校曾参与"沙漠风暴行动"战斗使命和部署"伊拉克自由行动"，并任前驻伊拉克空军武官。他也曾作为空军领衔代表参与空海一体战计划，并在空军总部担任参谋规划官和战略官。上校现居北弗吉尼亚州。