GeNeDis 稿件编号（由编辑填写）

移动健康应用中的区块链

利用 GPU 计算加速

GeorgiosDrakopoulos · Michail Marountas · Xenophon Liapakis · Giannis Tzimas · Phivos Mylonas · SpyrosSioutas

arXiv:2301.04725v1 [cs.CR] 11 Jan 2023

收稿日期：日期 / 接受日期：日期

摘要 区块链是一种线性链接、分布式且极为稳健的数据结构。最初，它作为比特币分布式技术栈的一部分被提出，后来在众多领域得到应用，尤其是智能合约、社交媒体、安全物联网和加密货币挖矿。它通过将经过强加密的数据分散存储在高度冗余的片段中，确保数据完整性。每次新增数据都需要经过区块链多数用户的验证和批准。加密和验证都是计算密集型任务，无法由普通的现成中央处理器完成。因此，科学界重新对安全的分布式通信和协调协议产生了浓厚兴趣。移动医疗应用日益普及，其一大优势是能够及时诊断某些病症。然而，由于移动医疗应用默认可以访问高度敏感的个人数据，人们对其隐私问题提出了担忧。本章简要介绍如何将区块链应用于移动医疗应用，以增强隐私保护。

关键词 区块链 · 数字健康 · 边缘计算 · 移动计算 ·移动应用 · 多数协议 · GPU 计算

数学主题分类（2010）65Y05 · 68Q05 · 68Q10 · 68W10

G. Drakopoulos 和 P.Mylonas 信息学系，爱奥尼亚大学，希腊 电子邮件：{c16drak, fmylonas}@ionio.gr X. Liapakis Interamerican SA，希腊 电子邮件：liapakisx@interamerican.gr G. Tzimas 西希腊技术与教育学院，安蒂里奥校区，希腊 电子邮件：tzimas@teimes.gr M. Marountas 和 S. Sioutas 计算机工程与信息学系，帕特雷大学，希腊 电子邮件：{marounta, sioutas}@ceid.upatras.gr

1 引言

近年来，分布式计算和数据结构领域中最受关注的新兴技术或许就是区块链。区块链可充当公有或私有账本；从结构上看，它是一种线性、分布式且健壮的数据结构。其新数据的插入不仅需要获得利益相关者的特别许可——他们大多是对某一区块链拥有合法既得利益的普通网民，但不一定都是如此，而这项许可是通过专门设计的共识协议获得的；此外，参与特定区块链的网民真实身份及其中包含的数据也都经过了强加密，通常采用 SHA-256 等公钥方案。此外，数据插入的确切位置由安全哈希函数决定。最后，当参与区块链的网民数量很大（通常达数千人）时，区块链就很难被入侵或操纵，因为任何恶意更改几乎都会立即显现。

凭借上述计算特性，区块链是一种出色的数据结构，可用于安全存储海量信息，适用于范围极广的用途，包括但不限于智能合约、数字健康信息、智慧城市和智能基础设施的状态信息、金融宏交易，以及游戏和社交媒体中的微交易，还有保险信息。事实上，作为一种数据结构，区块链最初是比特币技术栈的一部分，如 Nakamoto（2008）所述；此后也在加密货币综述中得到探讨，例如 Antonopoulos（2014）和 Antonopoulos（2017）。然而，自那以后，区块链逐渐独立发展，众多参与方都为各自的目的开发了某种基于原始区块链的版本。

区块链并非近年来唯一一种计算密集型的发展。数值计算和分布式深度学习等领域（例如训练多层卷积神经网络和循环神经网络）、复杂系统仿真（例如脑网络和蛋白质相互作用网络），以及大规模社交网络分析，都以迅速扩展而闻名。为满足额外计算能力的需求，一种应对方式是开发旨在实现大规模并行的硬件，例如专用图形处理器，并配套开发能够利用此类专用硬件、协调适当计算步骤序列以得出所需结果的软件。Google TensorFlow 是此类框架之一。正如 Abadi 等人（2016）等人所述，这是一种低级框架，其基本运算单元是张量，即多维数组。

本章的主要目标是聚焦并简要介绍 TensorFlow 和 GPU 计算如何与区块链结合，为数字健康和保险市场领域的应用赋能。次要目标是分析 TensorFlow 的计算能力及其数据流模型。

表 1 本章符号说明。

符号	含义
$\triangleq$	定义或按定义相等
$\langle s_k \rangle$	含有元素 s_k 的序列
$\lvert\langle s_k \rangle\rvert$	序列基数

本文其余部分的结构如下：第 2 节简要回顾有关区块链、GPU 计算及其应用的相关科学文献。第 3 节介绍区块链和 TensorFlow 的特性，第 4 节则探讨区块链在数字健康和保险领域的应用。第 5 节陈述本章的主要发现以及未来可能的研究方向。最后，表 1 总结了本文使用的符号。

2 先前研究

Nakamoto（2008）在开创性的比特币研究中正式提出了区块链。Barber 等人（2012）和 Cachin（2016）等人探讨了区块链的技术创新及其成为颠覆性技术的潜力。Miller（2018）重点研究了区块链与物联网的结合、其在主流工业领域的应用，以及与工业4.0即将带来的数字化转型之间的关系。Zyskind 等人（2015）展示了在物联网和边缘计算环境中实现区块链的实用方法及相关挑战。许多研究探讨了比特币的财富积累前景，以及比特币相对于传统法定货币的特性，例如 Antonopoulos（2014）、Antonopoulos（2017）、Kosba 等人（2016）、Swan（2015）和 B¨ohme 等人（2015）的研究。Abbas 等人（2018）和 Pass 等人（2017）讨论了区块链的分布式实现，而 Puthal 等人（2018）则探讨了区块链的安全问题。Underwood（2016）介绍了比特币体系之外的众多区块链。

自 Abadi 等人（2016）和 Abadi（2016）首次公开介绍 TensorFlow 以来，它便在深度学习领域得到广泛采用。Matthews 等人（2017）详细介绍了一种采用基础 TensorFlow 运算实现的高斯过程生成器。有关一种基于路径的新型图韧性度量，请参阅 Drakopoulos 等人（2018b），其思路与 Kanavos 等人（2017）的正则化方法相似。Wongsuphasawat 等人（2018）介绍了 TensorFlow 计算的优势及其可视化方法。关于张量在社交网络分析中的应用，例如多路数字影响力估计，请参阅 Drakopoulos 等人（2017）；关于社区结构发现，请参阅 Drakopoulos 等人（2018a）；关于基于图的 k 均值初始化，请参阅 Drakopoulos 等人（2016）。最后，关于一种用于聚类包含语言数据和空间数据的张量的遗传算法，请参阅 Drakopoulos 等人（2019）。

3 并行性与区块链

3.1 区块链

顾名思义，从结构上看，区块链通常由非常长的、线性链接的节点构成。每个节点都包含数据结构中部分经过标记的信息，以及一些管理信息。区块链中存储的数据永远无法删除，但只要所有相关方同意，就可以对其进行更新。因此，原始数据和更新后的数据都会被存储，从而提高审计效率。

除了提高安全性之外，选择区块链方案最重要的优势或许包括以下几点：

– 区块链支持海量交易。由于其固有的分布式特性，这些交易几乎可以同时进行。因此，利益相关者可以在合理的时间内执行任意数量的交易，无须担心确切的交易执行时间；在某些情况下，交易执行时间可能会影响交易成本。– 特定区块链的利益相关者几乎可以实时了解该区块链的全局状态。因此，他们不仅可以进行交易，还能几乎立即知晓交易结果，或至少在交易实际执行时得知结果。 – 无论是公有区块链还是私有区块链，都具有完全的透明度，因为任何参与者都可以自由验证该区块链上发生的任何交易。此外，验证协议经过精心设计，即使计算资源有限的网民（例如使用智能手机或平板电脑的网民）也能轻松完成验证。这增强了人们对妥善实施和管理的区块链的信任。 – 发生灾难性损失时，妥善实施的区块链至少可以利用存储在利益相关者计算机中的数据片段部分重建自身。区块链中更高的冗余使这一点成为可能。 – 从软件工程的角度来看，每个区块链节点的结构都相对简单，因此只需很少甚至无需人工干预即可管理。因此，区块链管理员只需管理数据结构中的少数几个关键部分，使区块链易于维护且维护成本低廉。 – 最后但同样重要的是，不再需要任何第三方或中介。相关各方可以直接沟通，并相互获取当前报价或其他重要信息。

请注意，区块链并不能免受各种复杂攻击，尽管此类攻击通常需要大量资源，而如今这些资源已完全在专门的黑客组织或政府机构的能力范围之内。除非掌握了私钥的相关信息，否则直接攻击加密协议或许并非明智之举，而利用零日漏洞则是另一种选择。

与任何新技术一样，区块链管理软件绝非毫无错误。不过，迄今为止已知的大多数攻击都采用了截然不同的方式，类似于暴力攻击：依靠大型僵尸网络来控制小型或中型区块链。

攻击区块链的另一种整体性方法，是运用控制理论的概念。攻击者以任何方式估算出的大型区块链当前状态，可表示为控制向量 $\mathbf{x}[\mathrm{n}]$。然后，通常会建立如下线性状态空间模型：

$$\begin{aligned} \mathbf{x}[n+1] &\triangleq \mathbf{A}\mathbf{x}[n] + \mathbf{b}u[n] \\ \mathbf{y}[n+1] &\triangleq \mathbf{c}^T\mathbf{x}[n+1] + du[n] \end{aligned} \tag{1}$$

如果攻击者能够插入适当的输入序列 $\langle \mathrm{u}_k \rangle$，那么根据模型的准确性，他可能会使整个系统进入不理想的状态。当然，这样的序列可能并不存在，或者其基数 $|\langle \mathrm{u}_k \rangle|$ 可能趋于无穷大。

3.2 TensorFlow

Google TensorFlow 是一个基于数据流编程范式、并以张量（即多维数组）作为主要数据结构的低级编程框架。它最初是为模拟脑网络而开发的，是一种强大的深度学习工具。它提供适用于 Python 和 C++ 的官方应用程序接口，同时也有人正在为多种成熟的编程语言开发非官方应用程序接口。此外，它还为中央处理器、图形处理器和张量处理器提供计算内核。

除了支持克罗内克积和哈达玛张量乘积、查找最小值位置、张量重塑等基本操作，以及克鲁斯卡尔分解和塔克分解等张量分解方法外，TensorFlow 还提供了许多深度学习中常用的数值优化器，例如 AdaGrad。此外，TensorFlow 还支持检查点，因此可以提前终止训练过程。

在区块链环境中，TensorFlow 可以加速哈希或加密所需的数值计算。此外，它还可用于训练神经网络，无论是循环神经网络、卷积神经网络、自编码网络还是其他类型的网络，都能预测近期的交易量，从而更好地在各个区块链节点之间均衡突发的交易负载。此外，还可以构建类似的网络，预测哪个区块链用户将是下一个生成数据块或请求交易验证的用户，同样以实现负载均衡。最后，理论上可以部署大型深度学习网络，对特定区块链所使用的加密协议发起攻击；但据作者所知，目前尚无此类用例的记录。

4 应用

区块链作为一种账本结构，无论是公有还是私有，凭借其安全、分布式的设计，都可用于存储敏感数据，例如健康状况和金融交易数据。此外，如前所述，所有中介至少在较高层面上都被消除了。因此，理论上，所有费用和保费（如税款或银行手续费）也会自动消失。

在数字健康领域，基于区块链的应用具有巨大的潜力。以下列出了一些最突出的应用。
– 网民的医疗记录可以安全地存储在区块链上，只有为该网民提供治疗的认证医疗专业人员才能调取这些记录，无论其身处何地，也无论此前是否为该网民提供过治疗。– 区块链可以助力智能手机自动监测选定的生物标志物，并将测量结果与个性化基线进行比较。– 网民可以更好地控制自己的个人记录，并且可以在更加透明、明确的条件下征得他们的同意。– 网民可以使用小额支付或移动支付来购买药品

，

从而进一步保护他们的隐私。

随着保险市场不断发展，基于区块链的应用也有很大的发展空间。以下是一些典型应用：
– 网民可以更轻松地搜索有吸引力的保险方案，并直接联系保险代理人，以商谈更优惠的方案。也可以通过配置为查找特定方案或条款的软件代理来完成。– 网民和保险代理人可以在区块链上签订智能合约，例如财产和车辆的电子购买合同。之后，如果有需要，只要相关各方达成一致，就可以直接重新商定合同条款，并将其记录在区块链上。– 智能合约记录完成后，可以在区块链上运行普通的浅层学习或深度学习算法，以识别可能的欺诈案件。– 区块链大幅简化了支付流程，甚至可以与移动支付结合。支付记录保持不可篡改，可作为支付确实在所示时间发生的证明。– 连接到区块链的智能手机及其他个人设备可以自动核验理赔申请，从而减轻行政负担和管理开销。

还应注意，除上述优势外，第 3 节所述的一般优势同样适用。

5 结论

本章聚焦于两个核心主题：区块链在数字健康和保险市场领域的应用，以及作为一种面向计算密集型应用的底层计算框架，谷歌 TensorFlow 如何用于加速相关计算。

区块链在医疗保健和保险领域有着诸多应用。此外，它还能强化隐私和透明度要求，从而有助于建立一个可行且可扩展的市场。

未来的研究方向包括开发经过广泛测试的区块链管理系统，以消除大多数（如果不是全部）零日漏洞利用。此外，鉴于量子计算近期取得的进展使大规模暴力破解攻击成为可能，应寻求更强的密码方案，以保护存储在区块链中的敏感个人数据。

致谢 我们衷心感谢 NVIDIA Corporation 捐赠用于本研究的 Titan Xp 图形处理器。

参考文献

Abadi M（2016）TensorFlow：大规模学习函数。《ACM SIGPLAN Notices》51(9):1–1 Abadi M 等（2016）TensorFlow：大规模机器学习系统。载于：OSDI，第 16 卷，第 265–283 页 Abbas N、Zhang Y、Taherkordi A、Skeie T（2018）移动边缘计算：综述。IEEE Internet of Things Journal 5(1):450–465 Antonopoulos AM（2014）精通比特币：解锁数字加密货币。O'Reilly Media, Inc. Antonopoulos AM（2017）精通比特币：编程开放区块链。O'Reilly Media, Inc. Barber S、Boyen X、Shi E、Uzun E（2012）由劣变优——如何让比特币成为更好的货币。载于：国际金融密码学与数据安全会议，Springer，第 399–414 页 B¨ohme R、Christin N、Edelman B、Moore T（2015）比特币：经济学、技术与治理。Journal of Economic Perspectives 29(2):213–38 Cachin C（2016）Hyperledger 区块链 Fabric 的架构。载于：分布式加密货币与共识账本研讨会，第 310 卷 Drakopoulos G、Gourgaris P、Kanavos A、Makris C（2016）用于初始化 k 均值的模糊图框架。IJAIT 25(6):1–21 Drakopoulos G、Kanavos A、Mylonas P、Sioutas S（2017）定义并评估 Twitter 影响力指标：一种高阶方法。Neo4j 中的实现。SNAM 71(1) Drakopoulos G、Gourgaris P、Kanavos A（2018a）Neo4j 中的图社区：四种算法的应用。Evolving Systems DOI 10.1007/s12530-018-9244-x DrakopoulosG、Liapakis X、Tzimas G、Mylonas P（2018b）基于路径的图韧性度量：借助图形处理器进行高阶分析。载于：ICTAI，IEEE Drakopoulos G、Stathopoulou F、Kanavos A、Paraskevas M、Tzimas G、Mylonas P、Iliadis L（2019）用于时空社会张量聚类的遗传算法：发挥 TensorFlow 的潜力。Evolving Systems DOI 10.1007/s12530-019-09267-8

Kanavos A、Drakopoulos G、Tsakalidis A（2017）Neo4j 中的图社区发现算法及其基于正则化的评估指标。载于：WEBIST Kosba A、Miller A、Shi E、Wen Z、Papamanthou C（2016）Hawk：密码学与隐私保护智能合约的区块链模型。载于：IEEE 安全与隐私研讨会，IEEE，第 839–858 页 Matthews DG 等（2017）GPflow：使用 TensorFlow 的高斯过程库。《机器学习研究杂志》18(1):1299–1304 Miller D（2018）工业领域中的区块链与物联网。《IT Professional》20(3):15–18 Nakamoto S（2008）比特币：点对点电子现金系统 Pass R、Seeman L、Shelat A（2017）异步网络中的区块链协议分析。载于：密码学理论与应用年度国际会议，Springer，第 643–673 页 Puthal D、Malik N、Mohanty SP、Kougianos E、Yang C（2018）区块链作为去中心化安全框架。《IEEE消费电子杂志》7(2):18–21 Swan M（2015）区块链：新经济蓝图。O'Reilly Media, Inc. Underwood S（2016）比特币之外的区块链。《ACM通讯》59(11):15–17 Wongsuphasawat K 等（2018）TensorFlow 深度学习模型的数据流图可视化。《可视化与计算机图形学汇刊》24(1):1–12 Zyskind G、Nathan O 等（2015）隐私去中心化：利用区块链保护个人数据。载于：SPW，IEEE，第 180–184 页