

区块链简介及其对会计工作的影响

(来源: ISACA 公众号, 2019-12-23)

区块链技术是比特币和以太坊等加密货币的基础,能够存储具有显著实用特征的数据,尤其是会计数据。一般认为区块链技术比谷歌文档更为安全,虽可与多人共享,但更改是安全的:

利用区块链作为存储机制的去中心化存档可提供一个无争议空间,可以通过这个空间来访问记录。即使用于获取文档和数据集的应用程序不起作用,区块链也能使其生效。鉴于区块链的这种去中心化存档,任何人,包括竞争对手、第三方甚至政府部门都不能进行删除或修改。这就是区块链与其他形式的数据时间戳和身份验证的不同之处……这项技术为社会——或者至少是社会内部的某些群体——提供了一种保存记录的手段,并保证这些记录的不可侵犯性和持久性,而这在以前是不可能实现的。

目前,人们密切关注几乎任何与区块链技术有关的事物,也为此投入了大量金钱。深入研究区块链意义重大,但首先,应对区块链技术有一个更好的了解,随后再探究区块链对会计和审计工作有何影响。对于一个有经验的实践人员来说,区块链可能会给人一种似曾相识的感觉,让人回想起 20 世纪 90 年代初大肆宣传万维网时令人激动万分的情景。不少人亲眼见证了源源不断的资源涌向万维网,人人都致力于开发最佳创意。目前,区块链技术的发展虽然还处于早期阶段,经历了种种失败,但几年后定会有很大不同。有了万维网之后,最初的网站固然很简陋,但现在已深深融入到了人们日常生活和经济中。因此,区块链将有可能发展成为人们日常生活和经济生活中更为普遍的

一员。

这就意味着会计数据可以通过以下方式存储和访问：

- 无争议、不可修改和经过验证的数据——数据若没有错误，还需要审计吗？

- 去中心化的数据——拥有适当授权/许可的任何人都可以使用不同的系统和软件访问会计数据，从而提高报告和其他监管披露的效率。

从广义上讲，金融系统，特别是会计系统，正从物理世界向数字世界推进。区块链技术可能会在这一转变中发挥作用。对某些人来说，区块链代表的是一种“运动”，而不是一种技术，他们还将会计系统向区块链技术靠拢这一举措描述为一种降低风险的方式，以避免技术过时。对其他人来说，区块链技术本质上是为了降低信息风险和提供会计数据方面的信任。该技术的实施涉及应对重大挑战，但不乏许多潜在优势。

解决会计工作（会计和审计）相关的区块链技术问题将能消除人们对区块链的误解，找到一些问题的答案，而最重要的是，探寻区块链技术给会计领域带来的真正价值。

区块链技术

那么，什么是区块链呢？区块链用于创建一个不可变的、公共的、分布式账本，几乎任何人都可以学习读写这个账本。值得注意的是，随着区块链的发展，这些特征可能会发生变化。下面的流程图（图 1）描述了当前执行的步骤：

- 验证交易的有效性和来源的身份。
- “证明”包含要列入区块链中的交易的区块的完整性。

- 将交易分发至对等网络。

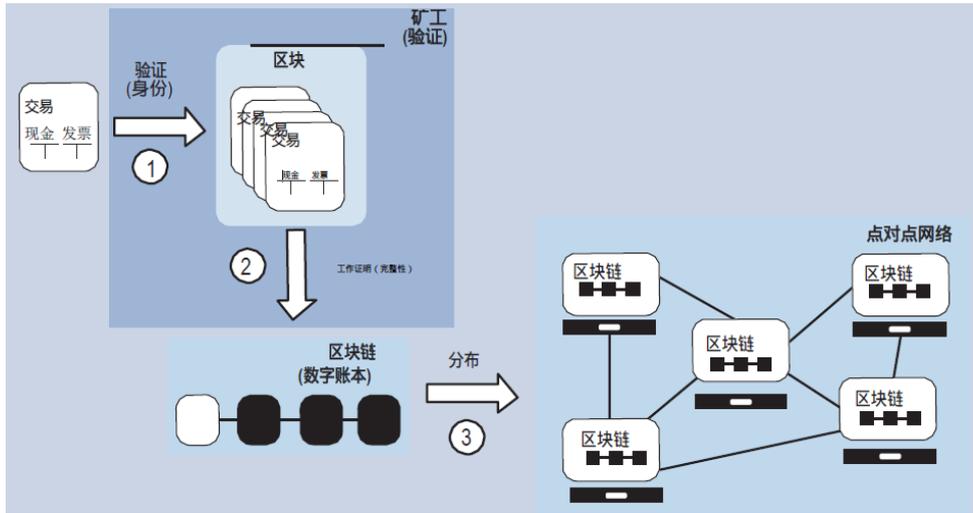


图 1 区块链流程图

截至 2018 年 6 月，GitHub 上大约有 86,034 个区块链项目，其中大约 8% 在维护中。而在 2017 年启动的项目中，有近一半（48%）以失败告终。大约 10% 为公司项目，而这些项目似乎更有可能“成功”，因为背后资源更多，且范围更窄。一个项目的平均寿命大约是一年。大多数区块链概念验证旨在实现以下三类效益之一：

- 降低成本，提高流程效率
- 创建一个信任度高于标准的生态系统
- 促进数字货币交换

	公共	私有
账本	向所有人开放	对未经授权的用户关闭
身份	匿名或伪匿名	已知
网络访问	无许可	许可
代码	开源	封闭式开发，通常是专利或专有的
信任	不信任	可信
附加到区块链	工作证明、股份证明	授权证明
示例	比特币、以太坊	瑞波、超级账本
权限/所有权	无	公司
矿工/验证者	任何人	获批节点

图 2 区块链项目：公共 vs 私有

图 2 为两类区块链项目（公共/私有）的对比。使区块链成为可

能的技术

图 3 为三种经过验证的关键遗留技术的概览，这些技术使创建、存储和共享记录的创新方式得以实现：



图 3 区块链遗留技术

1. 点对点网络（分布式账本）——目前，创建和维护账本需要利用某些第三方（即产权局、银行、法院、投票记录、借记卡、支票、合同）。账本的规则可能有些模糊，需要进一步解释，而解释可能导致不一致的情况发生。信任第三方很重要，因为企业看不到账本，账本都集中在一处，并且需要权限才能访问。而在去中心化的账本中，每个节点都可连接到所有其他节点，并且不依赖于任何中心权限。账本将“同步”至所有节点并公开。相邻节点之间相互信任，但在记录节点之前要先对交易进行验证（信任，但需验证）。这是一个分布式账本架构，是区块链的关键组件。在分布式账本架构中，交易可被读取（验证）和写入（附加）。点对点（P2P）网络易于管理，但速度慢，易受攻击（如拒绝服务（DoS）攻击）。点对点网络的使用是区块链的重要组件。点对点网络没有中心层次结构，所有节点都始终维护整个账本的副本。

2. 公钥基础设施（区块链地址）——如何信任“未知方”？ 密码学（一种算法）用于在不受信任的参与方之间的交易中创建信任。具体来说，公钥基础设施（PKI）是区块链的一个组件。区块链技术使用非对称加密（与对称加密相对，对称加密使用相同的密钥对数据进行加密和解密）来识别参与方（通过数字签名）以及交易的完整性（通过消息摘要）。

使用 PKI 之后，会生成一对密钥（公共密钥和私有密钥）。公钥自由分发，私钥则由这对密钥的所有者保存。任何东西都可用公钥加密，但只能用私钥解密。发送方的私钥也可用于对消息进行数字签名。私钥所有者必须保护好私钥，以使用相应的公钥来验证发送方的身份。如果私钥被破坏，整个系统都会受到影响。网络用户（所有节点）必须获得公钥。各方可创建一个私钥来维护钱包，并创建一个公钥来向网络提交交易请求。用户可拥有无限数量的钱包。钱包可在软件上进行在线交易，置于一个安全的驱动器中或借助于书面形式。公钥在多次迭代中散列，以创建叫做区块链地址的用户地址，从而保证了各方的匿名性。每个交易都使用不同的地址。

3. 哈希函数（矿工）——哈希函数用于整个区块链流程，保证记录不会被更改，从而确保整个系统的完整性。哈希函数接受可变长度的输入，并创建一个固定长度的输出，称为消息摘要。这是一个单向流程，意味着不能从输出中重新创建原始输入。在这个流程中，可以检查输入是否被更改。如果输入确实遭到更改，将会有不同的输出产生。

用户可将数百万个交易分为不同区块，并按顺序一次添加一个区块，以此控制试图一次发布同步的数百万个交易的添加。此流程可确

保每个人的钱包都与账本匹配。区块是区块链账本的重要组件。

每个区块头中都包含前一区块头的哈希值，区块之间就这样相互链接，也就形成了所谓的区块链。区块链上的第一个区块被称为创世区块。

在每个区块头中，默克尔根以哈希值的形式表示区块中包含的所有交易的摘要，它是区块内所有交易的唯一永久指纹。创建默克尔根要将两个记录的哈希值放在一起，生成组合哈希值，再重复进行该流程，直到区块中的所有记录都用一个哈希值表示。图 5 演示了四个交易记录（交易 1、交易 2、交易 3 和交易 4）的这一流程。

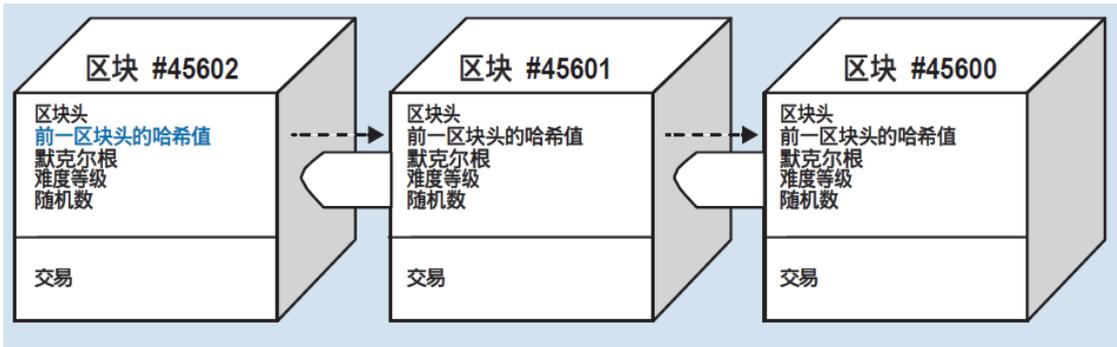


图 4 区块/区块链结构

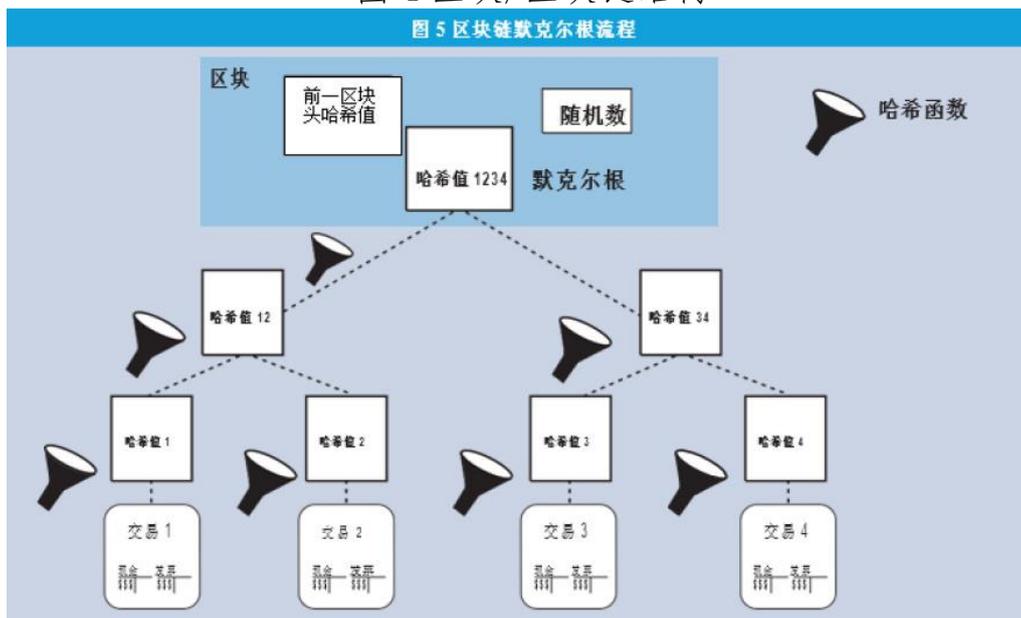


图 5 区块链默克尔根流程

资料来源：《区块链基础：揭秘可能影响一切的技术》，ISACA，美国，2017年，经许可使用。

只有交易各方协商一致，交易才可输入区块链（例如，参与投票的“节点”中，至少须有 51%同意将交易输入区块链）。矿工负责达成共识，并要求请求者以代币/硬币形式支付报酬。只有一些节点有矿工身份。工作量证明算法（是最初用于打击垃圾邮件的哈希现金（Hashcash）工作量证明算法的派生算法）运用的是蛮力攻击。矿工计算区块头的哈希值，创建一个随机数摘要。随机数是每个区块唯一的数据项，可增加以找到满足所需模式的结果（例如，生成的哈希值带有一定数量的前导零）。

这一流程分为以下两步：

- 第一步——计算区块头的哈希值，包括随机数。
- 第二步——根据目标值（难度级别）检查在第一步中计算的哈希值。

如果结果大于或等于目标值（模式），则增加随机数，并重新计算哈希值。如果结果小于目标值（模式），则代表计算出的哈希值解决了证明问题，并将该区块添加到区块链中。

2009年，人们可用个人家用电脑挖出 200 个比特币。到了 2015 年，使用个人家用电脑挖出 1 个比特币大约需要 98 年的时间。而在 2018 年，用于挖掘加密货币的电量足可为一个家庭供暖。按总耗电量计算，区块链挖矿的耗电量将与世界第七大电力消耗国不相上下。矿工不能改变过去的记录，这些记录具有永久性质，因此，只能添加未来的条目。

区块链带来的变化

通过区块链，不受信任的各方之间无需中心授权，就可安全地将

经验证的交易写入分布式账本，为每个节点创造不可否认的历史和价值，并为这些交易增加价值（信任）。

区块链会计

有了区块链技术，用户可将会计与业务活动融为一体，而非将其分开。这一点可通过三式记账系统实现，该系统基本上同时维护三个账本，每个账本由卖方、买方和一组公开的（加密授权的）记录组成。公开记录实则代表了交易的证据，且无可辩驳。

区块链技术也可应用于业务流程中的其他领域，包括贷款/抵押、资产来源（如“冲突钻石”）、银行间和跨境结算、私人债务/股权发行以及一些“智能”合约，这些合约可在预定的“触发”事件发生时自动执行程序。需要注意的是，组织可控制数据访问权，包括谁可以访问数据以及可以访问哪些数据。

“有了区块链技术，用户可将会计与业务活动融为一体，而非将其分开。”

区块链审计

审计师查看公共和私有企业的财务报表，并对其进行审计，以向用户保证这些报表公平地反映了公司的财务状况和经营成果。

区块链代表了一种确定交易数据有效的独特方式，也提供了一种独特方式来存储和访问这些信息：

一般而言，区块链技术指的是一个完全分布式系统，用于加密捕获和存储网络参与者之间交易的不可变、线性事件日志。在功能上类似于分布式账本，由参与网络内所有交易的各方一致保存、更新和验证。在这样一个网络中，区块链技术提高了透明度，并保证最终在整个系统范围内就整个交易历史的有效性达成共识。

优点：区块链技术的一个主要优点是，不能伪造数据，也不能修改数据。使用区块链之后，伪造数据几乎不可能发生，因为一旦创建了记录，就无法修改，只能进行补充。不过这种方法本身也带来了一定挑战（下一节将对此进行详细说明）。以下是采用区块链技术的

潜在优势：

- **三重验证**——三重验证限制了在会计数据输入之前或输入之时伪造数据的可能。截至 2018 年，已开发了双重验证系统，交易双方的记录中均有交易信息。

- **不可变记录**——很多人认为，区块链技术的最大优势之一是记录不可变。这就意味着数据输入之后就无法更改记录，且始终可信任记录包含有效数据。如此一来，试图通过修改会计记录进行欺诈将再无可能。

- **公开**——关于公开是区块链技术的优点还是缺点，尚存在争议。尽管公开可能会使审计工作的某些部分变得更容易，但很多组织不愿披露敏感数据（如工资单）。

- **资产（投资）管理**——区块链技术可用于提高记录的透明度、准确性和及时性，并为基金经理和经销平台提供直接联系。这些改进可能会促使证券结算、过户代理和基金估值验证发生改变。区块链技术还可帮助满足有关“了解您的客户”政策（KyC 或客户引导）的管理要求，以及对客户数据和交易的持续监控。

- **税收和税收计划**——区块链技术提供的透明性和可验证性在税收合规审计方面具有明显优势。区块链技术在间接税、转让定价和交易税（例如增值税，预扣税，印花税和保险费税）方面可能尤为有用。

“有些区块链应用程序的处理速度太慢，无法支持业务运营。”

缺点：会计从业人员经常对财务记录进行调整，包括在数据可用时将其与之前的数据融合（例如，考虑到后续事件或针对不足/过度应用的开销进行调整）。复式记账系统之所以在现代世界得以应用，很重要的一点正是因其有进行此类调整的能力。而区块链否定了这一能力，使得证明不如支持者宣传的那般有益。此外，仅仅因为交易不能被修改，并不能保证交易最初的输入是正确的。

与任何新的、相对未经测试的技术一样，各组织应彻查区块链技术应用过程中的潜在风险和挑战。其中一些挑战包括（但不限于）：

- **公开**——很多组织不愿以任何公开方式存储会计、客户或员工数据。存在丧失竞争优势的风险，组织可能不愿采用此技术。

- **延迟**——有些区块链应用程序的处理速度太慢，无法支持业务运营。据估计，每秒钟会产生超过 1 万笔支付卡交易，而区块链无法达到这个速度。

- **可扩展性**——可扩展性严重限制了区块链的效用。目前，这项技术太慢、太繁琐，用处不大。一些理论认为，区块链系统“……每秒最多能记录 7 笔交易……而比特币验证一笔交易的平均时间是 43 分钟。因此，很容易看出，暂且不论处理一家大型公司甚至同时处理多家公司的交易，区块链连处理一家中型公司的要求都无法满足。”

- **标准化**——目前存在多种分布式账本工具，而这些工具是由不同的组织根据不同的标准开发的。

- **可行性/遗留系统**——很多组织在将数据迁移至任何类型的区块链（分布式账本）系统之前，仍依赖于需要更新的旧（遗留）系统。组织中有经验的成员将会意识到系统升级涉及一定的技术和行为挑

战。

- **组织声誉**——技术一旦实施失败，可能会损害整个组织的声誉，而经理们倾向于规避此类风险。

- **电力消耗**——区块链也产生了电力消耗问题。“比特币的用电量相当于整个爱尔兰的用电量。”如此大规模的电力消耗使得技术的使用成本异常高昂。

- **易受黑客攻击**——与任何计算机技术一样，区块链技术可能易受黑客攻击和网络攻击，比如最近的 7,900 万美元加密货币被盗事件。

- **数据消耗**——数据成本也是一个问题。“如果某集团公司的交易总数为 N，那么公司需要计算和网络资源来捕获 2 N 笔交易。”况且这个数字仅考虑了公司的公开信息，而公司也很可能需要存储更多的私人数据。

- **无调整分录的交易对手方**——区块链技术旨在支持（加密货币的）现金流，其中货币被兑换成了有价值的东西。区块链技术并非为权责发生制（例如，公认会计原则[GAAP]）会计系统所需的调整分录而设计的。没有交易对手方，就没有三式记账，相应地，就会产生可验证性、信任等方面的损失。

- **合作/竞争**——利益方/受影响方需要合作和共享信息，以支持技术有效实施。但很多这些环境的特征都是竞争，而非合作，使得潜在的参与者不愿意实施此技术。

- **互操作性/融合**——为了实现区块链技术的全部优点，必须就数据和策略达成一致标准。但目前还没有这样的标准。

- **错误**——目前该技术中还没有规定能确保交易在一开始就得到正确处理，交易双方之间仅有一项协议可起作用，所以记录中仍然

可能会出现错误。

- **串通**——目前该技术中还没有防止交易双方串通进行财务欺诈的条款。

区块链的未来

是否需要新的法规和/或会计准则？目前，监管者似乎在走一条老生常谈的谨慎乐观之路，让私营部门自由创新。然而值得注意的是，很多政府和监管机构（如国际货币基金组织、英格兰银行、金融稳定委员会、金融行为管理局和欧洲议会经济和货币事务委员会）正在对区块链技术的威胁和机遇进行研究。一些政府也在研究区块链技术能如何帮助政府更好地为其选民服务。爱沙尼亚正在公共部门服务的各个领域试验区块链，洪都拉斯也有土地登记试点计划。

区块链技术有潜力成为一种实用的工具。但在组织环境中，应对其实用性和可实施性持怀疑态度。很多组织可能不愿意在公共区块链上共享敏感数据（例如合同信息、工资单），并在就区块链的性质及其未来用途提出一些重要问题。与传统系统相比，区块链数据需求会很大，那么如果区块链要得到广泛应用，这是一个需要解决的问题。不少企业可能会尝试使用这项新技术并以此创造价值，不过很多还处于起步阶段，会成功还是失败还有待观察。

区块链是否会使审计工作丧失其必要性或者改变审计的性质？区块链对审计的影响似乎不那么明显。审计师会继续审计交易还是改为审计区块链本身？

- **审计交易**——区块链技术似乎无需验证基础交易。如前所述，该技术中没有任何规定来确保交易在一开始就能得到正确处理，也没有规定可以避免共谋。值得注意的是，审计单笔交易只是审计中很小

的一部分。此外，对于存储在区块链之外的任何数据，仍然需要进行传统的审计工作，而目前区块链中的数据仍然绝大多数都是交易数据。此外应注意的是，调整分录很大程度上是依赖于会计和审计师的判断，不太可能存储在区块链中，通常只出现在审计工作纸质文件中。或许未来的审计工作将会更加精简，更加注重内部控制和治理，从而有可能使审计师进一步向价值链上游发展。

• **审计区块链本身**——2018年，普华永道（PwC）宣布推出区块链审计服务。除此之外，区块链交易可能仍然具有未经授权、非法、欺诈性、在关联方之间执行的性质，且与佣金或其他计划有关，或者会在财务报表中遭到错误分类。

尽管审计工作将一如既往地变化着，但其在可预见的未来仍然很可能继续存在。区块链不太可能使审计工作丧失其存在的必要性。

结论

图 6 区块链项目：公共 vs. 私有

	公证通	Tieron	Stampery	TaxToken	天秤币	Audit Chain
种类：						
附加区块链		✓	✓	✓		
完整区块链	✓				✓	✓
特征：						
数据安全存储	✓	✓		✓		
数据验证		✓		✓	✓	✓
审计追踪	✓	✓	✓		✓	✓
所有权证明	✓		✓			
存在证明	✓		✓			
完整性证明	✓	✓	✓			
收据证明			✓			
不可变记录	✓	✓	✓	✓	✓	✓
电子收据	✓				✓	✓
原产地：						
美国	✓	✓		✓	✓	
爱沙尼亚			✓			
瑞士						✓

图 6 目前市场上尝试使用区块链技术的一些产品

区块链代表的是机遇，而非威胁，未来的会计和审计服务可能会考虑使用区块链技术。尽管区块链技术正迅速发展，可能会对会计和审计工作产生影响，但仍有人对其潜在优点和易于实施的特征持怀疑态度。就目前而言，人们可能夸大了其优点，而低估了成本和实施难度。

区块链现在仍是一项相对较新的技术，软件也还在不断发展之中。图 6 列出并简要描述了目前市场上尝试使用区块链技术的一些产品。

作者介绍：

帕斯卡·A·比扎罗 (Pascal A. Bizarro)，博士、国际信息系统审计师；美国俄亥俄州博林格林州立大学会计和管理信息系统系会计专业副教授；曾在《国际信息系统审计期刊》、《会计师期刊》、《内部审计师》等权威期刊发表多篇论文；博林格林州立大学信息系统审计与控制本科和研究生项目的主要顾问，项目与国际信息系统审计协会模型课程一致，并发布于 www.isaca.org。

安迪·加西亚 (Andy Garcia)，博士，注册会计师；美国俄亥俄州博林格林州立大学会计与管理信息系统系会计专业副教授；美国科罗拉多州的注册会计师；曾就职于普华永道，曾在某财富 500 强公司担任国际审计师，在北美、南美、东南亚和大洋洲拥有审计经验；曾在《国际信息系统审计期刊》、《会计师期刊》和《内部审计师》发表多篇文章。

扎卡里·摩尔 (Zachary Moore)，美国俄亥俄州博林格林州立大学会计与财务规划专业本科生；曾在校园组织中担任会计类职务（财务主管），目前在当地一家房地产投资信托公司实习；曾获多项荣誉，包括博林格林州立大学本科生中心研究和奖学金补助金、朱利安·费桑会计和管理信息系统奖学金和建设财务管理协会奖学金；将于 2019-2020 学年期间注册学习博林格林州立大学会计硕士课程，并于 2020 年参加注册会计师和注册理财规划师考试。

原文链接：<https://mp.weixin.qq.com/s/mT0SQpv3IGgtlx-p65Np8g>，
转载请注明。