JRC SCIENCE FOR POLICY REPORT

区块链教育

亚历山大Grech安
东尼F. Camilleri

编辑：Andreia Inamorato dos Santos

2017

Joint
Research
Centre

EUR 28778 ZH

本出版物是欧盟委员会科学和知识服务联合研究中心（JRC）的"政策科学"报告。 它旨在为欧洲决策过程提供循证科学支持。 所表达的科学成果并不意味着欧盟委员会的政策立场。 欧盟委员会和代表委员会的任何人都不对本出版物的使用负责。

联系信息
名字：Andreia Inamorato dos Santos / Yves Punie
地址：欧盟委员会JRC，Calle Inca Garcilaso，3 - 41092 Edificio EXPO - 西班牙塞维利亚
电子邮件：andreia-inamorato-dos.santos@ec.europa.eu / yves.punie@ec.europa.eu

JRC科学中心
https://ec.europa.eu/jrc/en/open-education

JRC108255 EUR

28778 ZH

PDF ISBN 978-92-79-73497-7 ISSN 1831-9424 DOI：10.2760 / 60649

卢森堡：欧盟出版办公室，2017年

如何引用本报告：Grech，A。和Camilleri，AF（2017）教育区块链。 Inamorato dos Santos，A.（编）EUR 28778 EN； DOI：10.2760 / 60649

标题
区块链教育

抽象

本报告介绍了区块链的基本原则，重点关注其在教育领域的潜力。 它解释了这种技术如何可能会破坏制度规范和授权学习者。 根据当前的技术发展和部署情况，提出了在教育背景下应用区块链的八种情景。

内容

图表

致谢

这项研究得益于整个欧洲和其他地方的利益相关方和专家的投入和合作，项目组想向他们表示感谢。 我们特别感谢：

— 麻省理工学院媒体实验室数字货币计划高级顾问Michael J. Casey
— 玛丽·卡拉汉（Mary Callahan），本科教育注册主任兼高级副院长 - 麻省理工学院
— Brian Canavan，麻省理工高级助理注册官
— CédricColle，联合创始人 - Gradbase
— Alberto De Capitani，联合创始人Gradbase
— 开放大学知识媒体研究所所长John Domingue
— Provicis首席执行官Daniel Gasteiger
— 尼科西亚大学George Giaglis
— Provicis业务发展负责人Patrick Graber
— 微软公司C + E Azure区块链工程首席项目经理Marley Gray
— Learning Machine总裁Dan Hughes
— 学习机首席执行官Chris Jagers
— Darco Jansen - EADTU
— Soulla Louca - 尼科西亚大学
— Ioannis Maghiros - JRC欧盟委员会B4单元负责人
— Theo Mensen - Stichting ePortfolio支持
— Yves Punie - JRC欧盟委员会副主任
— Digitary业务发展总监Simone Ravaioli
— Kristel Rile - 爱沙尼亚教育部
— 学习机业务发展副总裁Natalie Smolenski
— 欧洲质量保证登记处主任Colin Tuck
— 学习创新总监Philipp Schmidt - MIT媒体实验室

我们还要感谢审稿人：

— 赫尔曼 德 莱乌 - 行政人员 导向器， 格罗宁根 宣言 网络，荷兰
— 爱尔兰Digitary业务发展总监Simone Ravaioli

亚历山大·格雷奇，安东尼·卡米莱里和安德里亚·伊纳莫拉托

前言

该区块链教育研究由欧盟委员会联合研究中心（JRC）B4 - 人力资本与就业部门设计并提供支持。 这是一项位于JRC开放教育[1]研究领域内的探索性研究，有助于在开放教育框架[2]的认可维度领域进行研究。 此前的研究是对基于MOOC的学习的认可研究，其结果是OpenCred[3]报告。

进一步的研究被认为是必要的，以理解在日益数字化的世界中什么可以促进发布和认证证书的过程。 "教育区块链"报告旨在填补这一空白。 它强调了在处理自己的学习和学习组合时，越来越需要学习者授权，从而利用流程的开放性和分权化带来的好处。

本报告主要面向决策者，教育机构，教育研究人员，教师和学习者，以及任何非技术性读者有兴趣了解区块链及其教育潜力的人士。

JRC整体研究数字时代的学习和技能目的是为了向欧盟委员会提供以证据为基础的政策支持，以利用数字技术的潜力来鼓励教育和培训实践的创新；改善终身学习的机会；并传授就业，个人发展和社会包容所需的新（数字）技能和能力。 对这些问题进行了20多项重大研究，形成了120多种不同的出版物。

近期关于教育和学习数字化转型能力建设以及对技能和能力要求不断变化的工作侧重于为公民开发数字化能力框架DigComp），教育工作者（DigCompEdu），教育机构（DigCompOrg）和消费者（DigCompConsumers）。 高等教育机构开放的框架（OpenEdu）也于2016年出版，同时还有创业能力框架EntreComp）。 其中一些框架伴有（自我）评估工具。 学习分析，MOOCs（MOOCKnowledge，MOOCs4inclusion），计算思维（Computhink）和数字技术在教育中整合和创新使用的政策DigEduPol).

关于我们所有研究的更多信息可以在JRC科学中心找到：https://ec.europa.eu/jrc/en/research-topic/learning-and-skills.

Yves Punie
副部长
DG JRC股人力资本和就业
欧盟委员会

[1] https://ec.europa.eu/jrc/en/open-education

[2] bit.ly/openeduframework

[3] bit.ly/opencredreport

执行摘要

区块链是一项新兴技术，几乎每天都会公布其日常生活的适用性。 由于区块链的分散性和分散性以及区块链记录的持久性以及运行智能合约的能力等特征，被认为会为传统产品和服务提供重大的机会。 这些特点使基于区块链技术的产品或服务与以前基于互联网的商业发展显着不同，而且对教育部门特别感兴趣 – 尽管有一些小例外的教育目前在大多数国家国家区块链举措。 此外，目前教育界的利益相关者基本上不了解区块链技术的社会优势和潜力。 编写这份报告是为了弥补这个差距。

上下文

预测区块链技术会破坏任何基于所有权标题的时间戳记录的活动领域。 在教育领域，可能受区块链技术干扰的活动包括授予资格，授权和认证，管理学生档案，知识产权管理和支付。

区块链技术的主要优势

从社会角度来看，区块链技术提供了超越目前可用的可能性。 特别是，将记录移动到区块链可以允许：

— **自**主权，即用户自我认同，同时保持对个人资料存储和管理的控制权；

— **信**任，即对于一个技术基础设施，使人们有足够的信心在其业务中进行支付或发放证书等交易；

— **透**明度和出处，即用户进行交易的知识，每方都有能力进入该交易；

— **不**可移动性，即记录要永久写入和存储，不可修改；

— **去**中介，即取消中央管理当局管理交易或保存记录的需要；

— **协**作，即各方直接相互处理而无需调解第三方的能力。

主要结论

这份报告的结论是，区块链申请教育仍处于起步阶段，尽管迅速增长。 它描述了英国开放大学，尼科西亚大学，麻省理工学院和马耳他各个教育机构的实施案例研究：这些实施都处于试点阶段。 然而，即使从这些早期的飞行员也可以得出结论：区块链可能会扰乱学生信息系统的市场，并放松玩家对这个市场的控制力。

虽然区块链技术的许多应用还不能想象，但我们发现，在教育领域，以下几个方面在不久的将来会被区块链技术的采用所影响：

(a) 区块链技术将加速证书纸质系统的结束。 特别是教育机构颁发的任何证书

资质和成就记录，可以使用区块链技术进行永久和可靠的保护。 还可以使用更高级的区块链实现信用的奖励，认可和转移自动化，甚至可以存储和验证终身学习中正式和非正式成就的完整记录。

(b) 区块链技术允许用户能够直接对区块链自动验证证书的有效性，而无需联系最初发布证书的组织。 因此，这可能会消除教育机构验证证书的必要性。

这种自动发布和可靠验证证书的能力也可以应用于其他教育场景。 因此，可以设想质量保证机构颁发给学校的认证证书，或授予教育工作者的授权证书，所有这些都可以被任何用户公开获得并且可以通过区块链验证。

它也可以应用于知识产权管理，用于跟踪首次出版和引用，而不需要中央管理机构来管理这些数据库。这使得例如可以自动跟踪开放教育资源的使用和再利用。

(c) 我们发现区块链技术创建数据管理结构的能力可以大大降低教育机构的数据管理成本，以及由于数据管理问题导致的责任风险。

(d) 最后，我们发现基于区块链的加密货币很可能被用来促进一些机构的支付。 创建自定义加密货币的能力也可能意味着区块链将在许多国家的授予或以凭证为基础的教育机构中发挥重要作用。

我们进一步得出结论，只有通过开放的技术实现才能实现上述的好处。（a）利用开源软件；（b）使用开放的数据标准；（c）实施自主权的数据管理解决方案。 这就是说，区块链解决方案供应商提出的许多解决方案（其中已有数百个）至少在以下三个标准中的一个上失败，因为建立一个围绕软件，数据或标准进行控制的商业案例比较容易。 我们建议教育领域技术的进一步发展应被视为市场和公共权力的共同能力，以确保私营部门创新的适当平衡，加上维护公共利益。

为了这一切，监管和标准化将决定前进的程度和进展的速度。

主要建议

鉴于区块链技术在跨国应用时显然受益于网络效应，而且还影响到成员国专有权限的许多领域，我们认为任何与区块链相关的政策工作都应具有欧盟与会员国根据条约规定的辅助性和比例原则。

为了确保开放区块链的实施，我们建议欧盟与成员国合作，考虑制定和推广一个"开放"教育记录的标签，其中规定了接收方所有权，供应商独立性和分散式验证的原则，并且只支持或采用技术遵守这样的标签。

我们进一步建议政策制定者考虑调查和支持区块链技术在特定教育用例（如上所述）中的应用，尤其是通过组织和支持创新管道来实施。

如果没有共同认可的数字元数据标准，利用任何技术提供的与教育记录相关的创新都无法取得进展。 因此，我们建议欧洲紧急支持这一领域的标准化活动。

从研究的角度来看，我们建议组建一个专家咨询委员会，让决策者了解事态发展及其对政策的影响，同时为具体实施和/或项目提供资金。

区块链技术在教育领域的主要受益者可能是教育组织和学习者的网络。 为此，我们建议与网络接触，以帮助他们了解区块链技术的优势，并将技术背后的原理融入到学习者的数字能力教育中。

相关和未来的JRC工作

JRC的OpenCred[4]报告曾经探讨过对非正式MOOC学习的认识。 这个Blockchain in Education报告也认可了学习，但是从正式和非正式学习的认证和认证角度来看，并且认为全球各国政府，企业和初创企业正在探索区块链技术/市场的适合性各种各样的用例以及广泛的需求和监管要求。 然而，对于基于可信区块链的系统的发展仍然有许多未知之处。 需要进一步的研究来提高我们关于如何创建基于区块链的系统的知识，以及如何创建基于区块链的系统将按需要工作的证据。

[4]bit.ly/opencredreport

1 介绍

本研究探讨了区块链技术[5]在教育领域的可行性，挑战，收益和风险，重点介绍了区块链在正式和非正式证书中的应用[6]。 这是一个针对决策者和非专业观众的探索性研究

区块链在教育方面的应用是非常新的 – 很少有同行评审发表的文献在该地区。 这项研究代表了对区块链教育的探索性回顾，重点关注欧洲领域的最新技术。 其主要目标受众是政策制定者，教育者，战略家和研究人员，他们有兴趣确保：

a) 一个新的数字基础设施的基础知识，在专业和技术媒体上被广泛吹捧，因为它有可能破坏已建立的部门；

b) 对那些最有可能受到欧盟成员国和目前正在试验该技术的教育机构采用该技术影响的领域的务实了解。

因此，该研究必须将案头研究与对该领域早期推动者的评估挂钩，同时铭记在技术采用初期设计的结果将决定未来的基础和脆弱性。

(5) 在本报告中，当提到区块链的概念时，我们使用"区块链技术"和"区块链"，当谈到写信息到特定区块链的具体用例时。

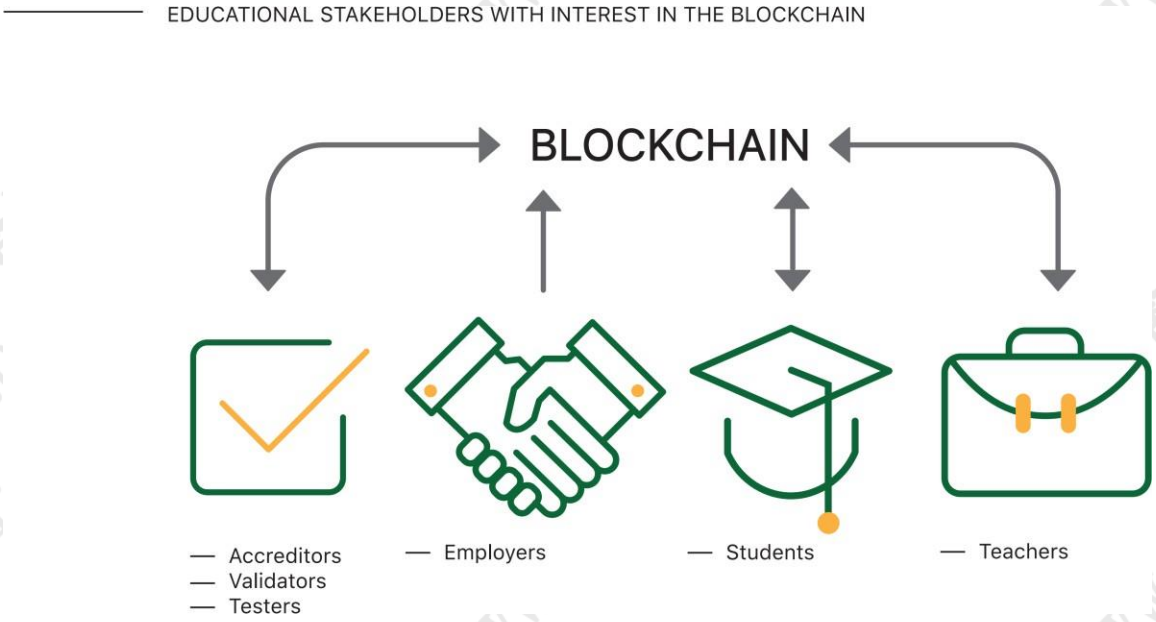
(6) 承认非正规学习和新的认证模式是2012年理事会关于验证非正式和非正式学习的建议的关键目标，要求成员国在国家安排进行验证。

2 目的，范围和目标

区块链技术是欧洲及其他地区许多行业和大学越来越感兴趣的领域。 作为计算机科学相对较新的一项创新，区块链是一种全球性的跨行业和颠覆性技术，预计将在未来几十年推动全球经济的增长[7]。

这项探索性研究涉及分散式分类帐的价值，特别是基于区块链的分类账可能会带给教育部门的利益相关者，特别关注其个人和学术学习数字认证的潜力。

图1：可能利用区块链技术的教育利益相关者



本研究侧重于区块链适用于正规和非正规教育证书的可行性，挑战，好处和风险。 欧洲需要克服许多教育证书方面的挑战，涉及到：

a) 持续专业发展和重新培训员工的需求；

b) 促进基于个人投资组合的非正规学习的认可 – 这对开放的学习者和移民来说尤为重要；和

c) 认证发放和认证过程的标准化和规模化，以及有关方面的获取。

从这个意义上说，区块链也代表了第三方（如雇主）独立和私下验证共享记录是否真实无损的机会。 这项研究探讨了一些反映与这个主题相关的社会政治和技术景观快速变化的领域。

(7) 世界经济论坛（2015年）估计，到2025年，全球GDP至少有10%（100万亿美元）将通过区块链技术进行管理，其中一半将以加密货币的形式进行管理。

此外，本研究还考察了区块链技术对知识产权管理（特别是开放教育资源）的影响，教育补助金的管理以及加强对学习者对自己数据的控制。

研究的主要目标是：

1. 介绍区块链技术及其核心社会价值主张；
2. 确定并参与影响政策制定者和其他关键利益相关者考虑在区域教育领域使用区块链技术作为增值主张的关键问题；
3. 解释教育机构和学习者如何利用这项技术作为一个透明，可信赖的系统来保证，分享和验证在欧洲的学术成就；
4. 确定技术是否适合在短期内记录学术成果，如果将欧洲大学和高等教育机构作为开放标准进行部署，可能会采用这种技术；
5. 讨论区块链技术如何可以帮助学术机构在发放学历证书和个人期望最大限度地提高他们的学习投资组合时保护他们的品牌和声誉的合法需要；
6. 为高校区块链技术的应用确定了一系列明显的机遇和挑战。 该研究还涉及与技术互操作有关的问题；以及如何协调认证的集中性和区块链的分散性
7. 提出一系列可能支持欧盟努力通过最大限度发挥区块链技术潜力在成员国开展教育的建议。 该研究将推荐欧盟如何在引入区块链技术方面发挥战略作用，从而可以改善教育的正式，非正式和非正式机会；提高资质透明度；并为教育和欧洲就业部门的改善作出贡献。

这项研究主要针对欧盟和欧盟成员国的决策者，教育者和研究人员。 对于一个对新兴技术感兴趣的更一般的读者来说，它也可能是有兴趣的，并且将其部署在更广泛的社会经济背景下。

3 方法

本研究以定性研究方法为基础，运用案头研究，文献综述，访谈和案例研究等方法进行研究。 随着区块链等新兴技术的出现，几乎每天都有专业媒体发布行业公告和帖子，定性方法的使用目前代表了一个在研究这个问题处于萌芽阶段时与这个问题交往的实用方法，涉及区块链和教育的案例研究是探索性和/或试点举措。

为此，我们的研究方法包括：

任何已发表文献的文献综述：区块链技术在教育中的应用

区块链技术的非金融应用更普遍

存储，保护，分享和核实学历证书的数字方法

书桌研究利用主要来源涵盖：

主要区块链实施技术规范，特别是比特币和以太坊

供应商提供的产品技术规格，提供基于区块链技术构建的产品，以及其治理结构，运营和知识产权安排。

访问区块链和教育领域相关利益相关方的研究人员，专家，行业代表，教育工作者，认证人员，测试人员和学习者样本。

3.1 研究的局限性

这项研究受制于一些早期阶段，即探索性研究领域的局限性。

1. 区块链技术正在全球范围内得到积极的发展，最近的进展可能会影响我们的研究结果。 为了缓解这种情况，我们通过监控国际技术会议，发表的学术论文和灰色文献（如白皮书和博客），努力跟踪区块链技术的进步。
2. 我们只使用了少量的用例。 这是本研究采用的总体探索性，定性方法的考虑因素。 我们不会根据有关用例人群的统计证据提出索赔。
3. 所选用例可能不足以代表对区块链教育的最佳方法。 我们已经广泛使用我们的专业网络来保证与行业领导者以及研究人员和专家的面谈。 用例研究被确定和发展为这个迭代过程的直接结果。
4. 我们用例的候选人对区块链技术在教育领域发展的贡献可能不是最佳的。 有可能存在替代案例研究，更好地解决相关用例研究的动态背景和要求。 我们通过从文献和行业内部人士和政策制定者的采访中寻求广泛的投入来减轻风险。 我们相信，我们已经获得足够的相关第一手资料用于评估风险和机遇区块链系统提供了一系列可能影响教育行业主要利益相关方决策和行为的领域和这项研究的目标读者。
5. 我们所进行的设计分析可能不够有效，相关或严格，因为它们尚未被区块链系统广泛识别，使用和研究。 但是，我们相信我们采用的高水平定性方法以前曾被用于各种其他技术领域，因此我们认为使用它们来支持我们研究中的指示性定性研究结果是合理的。 我们认为，我们研究的结论和建议基于区块链技术发展阶段的适当分析以及教育利益相关者的非常有限的接受程度；而这又反过来揭示了区块链技术发展初期可能经常遇到的风险和机遇。
6. 我们对区块链技术的技术描述被有意简化，以便非技术人员理解。 因此，本文没有讨论支持区块链技术的密码技术，也没有讨论不同区块链采用的一致性验证和挖掘机制。

4 区块链 – 介绍

"区块链"正在迅速成为技术白话的一部分，但仍然非常被误解。 以下高级定义[8]提供了对该主题的快速介绍：

> 简而言之，区块链是一种分布式账本，它提供了一种信息被社区记录和共享的方式。
>
> 在这个社区中，每个成员都维护他或她自己的信息副本，所有成员必须集体验证任何更新。
>
> 这些信息可以代表交易，合同，资产，身份或实际上可以用数字形式描述的任何其他信息。
>
> 条目是永久的，透明的和可搜索的，这使得社区成员可以全面查看交易历史。
>
> 每个更新都是一个新的"块"添加到"链"的末尾。
>
> 协议管理如何发起，验证，记录和分发新的编辑或条目。 通过区块链，密码学取代了第三方中介作为信任的保管者，所有区块链参与者运行复杂的算法来证明整体的完整性。

自20世纪90年代初以来，已经进行了区块链实验，但是直到2008年，以中本聪本人[9]的个人或团体的个人或团体发布白皮书，区块链才被广泛采用。 第一个众所周知的区块链是比特币区块链，也是第一个被广泛使用的分散式加密货币[10]的名称。 "比特币"也指加密货币的网络协议。 就流行的白话而言，比特币区块链在实践中自动与"区块链"相关联，还有其他区块链具有重要意义，比如以太坊区块链（参见附件3中的主要区块链概述。

4.1 分类账

分类账是可以在任何时间点确定资产所有者的工具。 他们通过作为有关资产转移的中央权威清单履行这一职能。

> 在同意使用分类账来确定特定资产所有权的系统或社会中，所有在双方之间转移所有权所需要的是在分类账中输入一个表明已经发生的事情。

从技术角度来看，分类账只是一系列按时间顺序排列的交易，结构如下：

---

(8) 改编自Piscini等。 （2016）。

(9) 最初的白皮书"比特币：对等电子现金系统"于2008年10月31日发布。它描述了比特币网络协议及其分布式体系结构，随后在一年后提供参考实施。 这些文件成为比特币加密货币的基础。

(10) 本研究报告简要概述了该技术，确保参考而不是重复2015年JRC研究报告"关于虚拟和加密货币：从技术层面到财务影响的总体概述"。 另见https://blockgeeks.com/guides/what-is-cryptocurrency 以便快速指导加密货币的起源和基本原理。

图2：典型分类帐条目

TRANSACTION NO.	DATE & TIME	SENDER	ASSET	RECEIVER
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2

这个保存资产转移权威列表的简单概念，使得资本的系统转移和积累成为资本主义成为可能的关键技术（Windjum，1978；Yamey，1949）。

实体拥有或控制公共分类帐（包括分类账所在的服务器，在线公共分类帐的情况下）的人或组织处于重要的权力和影响力的位置。 具体而言，分类帐的所有者可以：

— 决定是否记录一笔交易，这又使这个人有能力：
  - 强加条件让个人记录交易；和
  - 决定适用的控制制度，检查这些交易的准确性；
— 修改或删除分类账中已有的交易；
— 完全摧毁总账，或者让其被销毁。

由于在这样一种制度下，在分类账中编写，修改或删除交易也改变了对象的所有权，控制这种分类账的人或组织也通过有效地控制谁拥有什么 – 仅仅是作为名单的管理者的交易。

传统上，分配精确账本的责任一直被分配到各种机构：政府通过控制财产账户控制土地所有权； 银行通过持有货币的分类账来控制世界的货币体系； 而股票交易所通过持有商业所有权的分类账来控制商业界的大部分股份。 由于资本主义社会是围绕着销售和所有权（资本的转移和积累）的概念而建立起来的，因此与分类账的管理有很大的责任。

具体而言，这些中央政府相信：

提供证人 – 即证明身份并确保登记在账本上的人是他们所说的人，并确保被转移的资产存在；

在所有交易中保持诚实和透明 – 即不要通过创建虚假交易或在创建后非法修改交易来剥离用户的资产；

保证安全 – 即确保未经授权的第三方不能读取或写入分类账（黑客）；

不要滥用垄断地位，为他们的服务施加不公平/特殊的成本；

允许人们进行交易 – 也就是说，让每个有合法利益的人通过列入账目进行交易。

由此推论，这些机构可能单独或集体地造成重大的伤害甚至社会混乱，滥用信任，以准确地保存和维护这些分类帐。 推论是，这些机构有权使用或滥用对分类账的控制权，并对其直接职权范围内的个人和社会施加重大控制。

4.1.1区块链作为公共账本

最广为人知的区块链应用是作为加密货币交易的公共账本，比如比特币和以太网。 与其他公共分类账一样，区块链分类账记录了资产所有权的来源和转移。 区块链协议的交易结构不仅便于加密货币的转移，而且便于其他数字资产的转移。 资产可以是有形的，如房屋，汽车，现金，土地，或像知识产权这样的无形资产，如专利，版权或品牌。 事实上，任何有价值的东西都可以在区块链网络上进行追踪和交易，从而降低所有涉及的风险和成本（Gupta，2017）。 由于它们被设计用于记录和保存交易，因此所有区块链传统上都有一种与之相关的数字货币，作为跨网络交易的最基本的资产。 这也激励了通过向自己的加密货币支付网络贡献者来采用该区块链协议。

区块链因此是记录交易组的交易记录，否则称为块，它们以线性时间序列密码链接在一起。 与区块链相关的其他关键属性 – 安全性，不变性，可编程性 – 取决于区块链的架构以及区块链运行的共识协议的特性。 一些区块链被构造成促进跨非节点的节点之间的点对点事务；这被称为"分布式"网络结构。 一些区块链，比如比特币区块链，也通过其独特的共识协议确保分类账的不变性。

为了确定谁拥有一个特定的资产，一方只需要查阅分类账，以检查最近的所有者是谁。

在描述区块链时，重要的是理解支撑其核心思想和哲学（其"社会价值主张"）的一套社会原则，以及支持其社会效用（其"技术特征"）。 以下章节解决了这些重要的考虑事项。

4.2 区块链的社会价值主张

在区块链这样的主题领域，首先要关注数字中断，数字经济，知识产业和创新体系等问题。 这使我们能够了解数字中断的背景。 但是，通常不仅数字技术是重要的：社会经济

创造技术需求的驱动因素（或者对其作出的改变）可能同样重要，如果不是更重要的话。 最有效的数字商业模式首先理解人，数字技术第二（Christensen，Clayton M 2003）。

在Byrne（2017），Gupta（2017），Hanson et。 al（2017），Morabito（2017）和Piscini等人（2016年），可以提出一套支持区块链技术[11]的社会价值主张的原则，作为了解区块链技术对教育部门具体功能的启示。

4.2.1 自主主义与认同

关于区块链的早期文献经常提到"自我主权"，以及个人在网上拥有和控制自己的身份的能力（Lilic，2015；Allen，2016；Smolenski，2016b）。 根据Au（2017）和Lewis（2017）的说法，公开链通过让个人有能力成为谁可以访问和使用他们的数据和个人信息的最终仲裁者来促进自主权。 在教育背景下，这个术语正在逐渐成为赋予个人学习者权力以拥有，管理和分享其证书细节的同义词，而不需要呼吁教育机构作为可信中介。

这也可以被认为是公民通过在线共享个人数据和身份的方式获得重要的"自我授权"，并且能够选择将其全部或部分释放以获得他们想要的服务 - 而不需要不断求助于第三方中间人来验证这些数据或身份。

> *身份是公众和政府之间相互信任和相互信任的基础；它是服务提供，安全，隐私和公共安全活动的关键推动者；它是公共行政和大多数政府业务流程的核心。 如何收集，使用，管理和保护身份信息是公共部门领导人关心的重点"（加拿大政府）*

身份是公民和需要验证身份的复杂领域：验证个人属性，个人历史，关系和/或交易历史[12]的评估。 数字身份接近人权。 然而，还没有一种安全的方法来处理互联网的缺陷之一 - 在网上识别人员或机器[13]。当公民有义务或者同意泄露他们的在线身份时，就会产生新的问题，比如使用私有算法来最大化社交媒体上用户个人数据的商业用途。

技术从根本上改变了我们代表自己的能力。 同时，我们互联世界的本质正在改变我们对身份和信任的看法。

---

(11) 不同的区块链实现以不同的方式和不同的程度来解决这些原则。 并非所有区块链和/或不同类型区块链的应用都将包含基于区块链技术社会价值主张的全部原则。 关于哪一个是最可能的区块链来体现整套原则存在争议；然而，一个强有力的例子是，作为一个高度分散的共识协议的公共区块链，比特币区块链位居榜首。

(12) 根据汉森等人。 al（2017）对身份的评估用于最大限度地减少任何感知的信任差距。 这种差距与风险的度量成正比，这反映了对身份和潜在损失的看法。 权衡通常是隐私的损失，以换取高价值交易。 其缺点一直是私密性的丧失，在交易不对称的情况下，对被审查的个人进行中等程度的最小限度的价值，而对另一方提供的风险进行比较。 为了验证他们身份的某些属性来完成交易，他们还公开了他们可能不想公开的身份的其他属性。 本披露将其所有属性放在该文档上，有可能进一步不必要的泄露或非法使用。

(13) 看到https://qz.com/989761/microsoft-msft-thinks-blockchain-tech-could-solve-one-of-the-internets-最困难的 - 问题 - 数字身份/

以区块链技术为核心的密码技术有助于解决身份漏洞问题，并将个人数据的所有权和控制权"搏斗"回个人用户。 人员，企业和机构可以将自己的身份数据存储在自己的设备上，并将其有效地提供给需要验证的人员，而不依赖于身份数据的中央存储库。 区块链技术不仅提供了一种数字化具有内在价值的纸张的新方法，例如我们的凭证 - 它为我们提供了在线控制我们的身份并适当管理的手段（参见第5 了解有关Blockchain授权和认证功能的更多信息）。

事实上，一些人认为，完全的数字自我主权可能最终背离分享永久性的"身份"之类的东西，而是成为一种核实索赔的制度。 换句话说，查询方不是索取无关的信息，而只是要求立即与手头交易相关的信息：18岁以上的个人？ 他们是否从麻省理工学院获得了神经科学博士学位？ 他们是意大利公民吗？ 一旦得到满意的验证，索赔就可以被撤回[14]。

4.2.2 相信

一项有影响力的英国政府研究[15]表明，信任是两个或两个以上的人，组织或国家之间的风险判断； 在网络空间中，这是基于两个关键的要求：

a) 认*证 - 向我证明你就是你说的那个人；*

b) 授*权 - 向我证明您有权执行您所要求的权限。*

如果其中一方对答复不满意，他们仍然可以选择允许另一方进行，但是会带来风险。 但是，除非各方相互信任，否则没有可行的关系。 从这个意义上讲，在社会上值得信任就好像是有信誉的。

这个信任的基本概念在数字化的世界中保持不变，我们必须依靠许多我们永远不会遇见的行为者，以诚信和为我们行事：信任通常只被授予一个特定的应用，上下文以及一段时间。 在全球数字经济中，维持信任的挑战 - 随之而来的制约和平衡 - 正在变得越来越昂贵，耗时且效率低下[16]。

区块链技术可能为当前建立制度化信任所需的程序，组织和技术基础设施提供一个可行的替代方案。 利益相关者之间的信任关系的改善与分散式公共账本的使用以及加密算法有关，这些加密算法可以保证经批准的交易在经过验证后不能被改变。 分布式账本通过在给定的时间点建立一个事实来进行信任，这个事实可以被信任。 他们通过自动化信任的第三方的三个角色来实现这一点：a）验证； b）安全防范交易；和c）然后保存它们。

我们希望，就像互联网重塑沟通和影响社会行为一样，区块链也可以帮助解决目前交易，合同和信任方面的缺陷 - 这是企业，政府和社会的关键支柱。

---

(14)请参阅"ADISummit：自主主义认同小组"中的Andreas Antonopolous。
https://www.youtube.com/watch?v=DZbyiJqKT8c

(15) 英国政府科学办公室（2016）

(16) Piscini et。 al（2016）

4.2.3 透明度和出处

易于共享和可见性是区块链的基本特征；目前系统中缺乏这些功能往往是区块链采用的主要驱动力。 它们在不止一个组织进行区块链交易的交易中变得尤为重要。

区块链使参与者了解每个资产或记录的来源以及其所有权随着时间的变化。 但是，这种透明度只有在区块链交易链接到标识符时才起作用。 如果没有公共标识符（如链接文档或序列号），区块链交易将无法解码和跟踪。 这样，区块链甚至"公开"区块链默认是私有的，但也可以通过链接的"链外"数据跟踪特定个体的交易。

区块链技术为验证交易数据在特定时间存在提供了无可争议的机制。 此外，由于链中的每个块都包含有关前一个块的信息，因此每个块的历史，位置和所有权都被自动验证，并且不能被更改。 单一的共享分类账提供了一个确定资产所有权或完成交易的地方。

4.2.4 不变性

不可变的记录是一个不可改变的记录，其状态在创建后不能被修改。

不变性与安全性以及其机密性，完整性和可用性的经典属性相互关联。 不变性也与韧性和不可逆性有关。区块链数据不能轻易改变，因为它在不同地点不断复制。 作为区块链底层协议的一部分，使用私钥和公钥加密技术，事务安全性和机密性变得几乎无懈可击。

区块链的不变性意味着一旦建立就不可能做出改变：这反过来又增加了对数据完整性的信心并减少了欺诈的机会。 对于区块链上的交易被认为是有效的，交易中的所有参与者必须就其有效性节点达成一致，否则运行区块链协议的"同伴"必须就交易的有效性达成一致。 发生这种情况的机制不同于区块链到区块链，但通常在一定程度上分布，这意味着没有一个参与者可以成为网络中的真理仲裁者。

没有参与者在记录到分类帐后可以篡改交易。 如果某个交易出现错误，则必须使用新的交易来纠正错误，并且这两个交易在分类帐中都可见。 区块链弹性源于其结构，因为它被设计成一个分布式的节点网络，其中每个节点都存储整个链的副本。 因此，当交易由参与节点验证和批准时，实际上不可能有人改变或改变交易的数据。 尝试在一个地点更改数据将被解释为欺诈行为，并对其他参与者的完整性进行攻击，结果将被拒绝。

4.2.5 非中介

通过用数学替代中间商，区块链也可以走向维持信任（Piscini et al。2016）。 区块链上的参与者在一个市场上连接在一起，他们可以以透明的方式进行交易和转让有价值的资产的所有权，而无需协助

第三方调解员或中间人的介入。 一个价值网络没有一个明确的中央权威机构。

利用区块链技术，点对点共识算法能够在没有第三方的情况下透明地记录和验证交易 – 可能会降低甚至消除成本，延迟和一般复杂性。 例如，区块链可以在各方直接相互交换资产时降低间接费用，或者迅速证明信息的所有权或作者身份 – 如果没有中央当局或公正的调解人，目前几乎是不可能的。 此外，区块链能够跨越机构界限保证真实性，可能有助于各方将注意力集中到以新的方式验证记录，内容和交易的新方法。 互联网越来越分散化将会把更多的控制权交给用户（或者更具体的说是用户的设备），而不是依靠谷歌或者亚马逊这样的云平台。

4. 3存储在区块链上的记录类型

区块链通常用于存储以下记录：

1. 资产交易；
2. 智能合约；
3. 数字签名和证书。

4.3.1 资产交易

资产交易记录通常有两种形式：

— 货币，以货币为单位表示：同一货币的每一单位在任何时间都具有与其他单一单位相同的价值。货币也可以兑换率内部兑换。 使用区块链技术构建的货币最常见的形式是比特币。

— 所有权的文件证据，合法地称为地契。 这些通常用来表示土地等不动产或知识产权等无形财产。

4.3.2 智能合约

智能合约实际上是存储在区块链中的小型计算机程序，其将在特定条件下执行交易。 因此，智能合约通常是诸如"如果Z发生时将X转移到Y"的声明。 与达成协议后的正式合同不同的是，各方必须签署合同才能进行合同，而智能合同是自动执行的 – 也就是说，一旦指令写入区块链，交易将在适当时自动进行条件被检测到，交易双方或其他第三方不需要进一步的行动。

以智能合约为代表的承诺是，在一个行业重要的数字记录可以被验证之后，一个全新的技术自动化生态系统将开始发展，形成一个新的社会结构，实现公民效率，个人移动性和制度转型。 因此，在这种情况下，智能合约代表了对未来的自动化看法[17]。

(17) 另见https://github.com/Azure/azure-blockchain- 项目/斑点/主/布莱切利/ AnatomyofASmartContract.md

4.3.3 证书和数字签名

从**最基本的形式来看，认证就是一方向另一方声明一定事实是真实的问题（见第一节）6).**

签名证明声明是由上述各方发布的。

区块链可用于存储证书的密码散列（"数字指纹"），或存储声明本身[18]。 因此，区块链可以承担公共证书注册管理机构的职能。

4.4 区块链架构的高层概述

区块链是连接连续的"块"交易的分类账，其中：

— 每个希望通过私人或公共网络交易任何资产的人都需要访问网络。 这种访问通过在用户和区块链之间进行调解的软件应用程序来实现。 软件应用程序（通常称为"钱包"）可以直接安装在设备上，也可以通过网络浏览器访问。 根据设计的方式，区块链钱包可用于发送和/或接收数字资产。 有些钱包可以在没有调解的第三方的情况下进行直接交易，而其他的钱包则由第三方管理，第三方代表他们管理用户的数字资产。

— 希望参与通过共识验证交易的用户通常必须在其设备上安装区块链软件。 这用于写入分类账，存储整个分类账的整个副本，并保持分类账的所有副本完全同步。 由于公共区块链允许任何人安装软件并拥有整个分类帐的副本，任何人都可以直接在网络中的区块链上进行交易，并且没有任何第三方可以强制访问条件。 在经过许可的区块链中，中央管理机构确定谁有权访问运行节点并参与共识流程。

— 区块链中的交易记录或区块以加密方式链接在一起，使其具有防篡改功能。 与数字数据库中可以更改的记录不同，一旦在区块链上记录了交易记录并加上了时间戳，就不可能对其进行更改或删除。

— 区块链记录交易的事实，即已经转移的事物，涉及的当事方，以及与交易相关的结构化信息（元数据）和交易内容的密码散列（"数字指纹"）。 这个独特的签名用于稍后验证交易：如果某人更改了交易内容，则其唯一代码不再匹配链上的版本，区块链软件将突出显示该差异。

— 参与交易的所有参与方，只有那些参与方必须在新的交易记录被添加到网络之前提供他们的共识。网络中的所有其他节点将只验证双方是否有适当的能力进入交易。 因此，只要一方同意发送资产，并且另一方同意接收资产，并且节点验证每个方都有能力进行交易，那么就完成了。

— 网络中的所有计算机不断地和数学地验证它们的区块链副本与网络上的所有其他副本相同。 在大多数计算机上运行的版本被认为是"真正的"版本，所以"记录"记录的唯一方法是控制网络上一半以上的计算机。 对于运行数千个（甚至是在中）的区块链

[18]如果索赔可以用令牌来表示，例如获得信贷，那么情况尤其如此

未来，数以百万计）的电脑，像比特币和以太坊这样的公共链，这将是一个几乎不可能完成的任务。 完全摧毁分类帐将需要删除世界上的每一个副本。

5 证明

5.1 什么是认证？

一般来说，认证描述证书颁发的任何过程，作为对权利要求的验证。

在教育中，许多情况下使用认证，例如，作为以下证据：

- 学习成果的实现，不管学习的形式如何；
- 教师的能力；
- 一个学习者进行的学习过程，不管学习的形式如何；
- 符合一定质量标准的教育组织或课程；
- 认可机构被授权发布认证。

正如Schmidt（2017a）所观察到的，过时的证书制度限制了我们创造教育新途径的能力，特别是对那些缺乏获取途径和最需要的人。 没有受过正规教育的人面临的一个挑战是把他们的学习转化为工作，因为他们往往缺乏肯定他们的技能和经验的证书。 此外，现有的证件制度大大有利于正规教育而不是其他学习经验，使得开展有价值的课余和下班后教育项目变得更加困难 - 尽管终身学习和非正规和非正规教育有明显的优点。

斯摩棱斯基补充说："证书已经成为一种跨国，跨学科的能力和技能信号，在其他特征 - 语言，国籍，宗教身份 - 不能被预设的环境中出现"（Smolenski，2017）。 凭证不仅决定谁可以传递知识，还能帮助我们识别具有某种技能的社区成员（Schmidt，2017b）。

5.2 认证的本体论

5.2.1 认证的组成部分

认证是最基本的形式，是从一方到另一方声明一定事实是真实的。 因此，任何认证都涉及以下要素：

1. 声称 - "这一系列事实是真实的"。 教育背景下的例子可能包括："学习者获得技能"，"教师有足够的知识来教授"，或者"学生已经完成任务"。
2. 发行人 - 一个已经核实和确认事实的机构，并且证明索赔是真实的
3. 支持索赔的证据通常包括索赔被核实的程序和关于索赔的一些额外信息。 因此，例如，如果一个机构证明学生已经收到了1个ECTS学习价值，那么ECTS手册就会说明如何验证这个索赔的组成部分和程序。 在这个例子中，程序涉及测试学生实现一组指定的学习成果，这已经通过大约25个小时的学习
4. 接受者 - 接受要求的人 - 学习者获得技能，具有足够知识的教师或完成作业的学生
5. 证书 - 证明发行人身份的文件，收件人的身份，索赔，并在必要时提交证据。

6. 证书将包括一个签名，这是一个唯一的标志，印章，图像或代码，只能由发行人加盖，从而确认其身份。

5.2.2 涉及认证的过程

认证涉及三个不同的过程：

1. **签**发：这是将索赔，签发人，证据，收件人和签名记录在证书上的过程。 通常，这些数据被记录下来：

- 在一个集中的索赔数据库中；
- 在颁发用户证书上。

2. **验**证：这是第三方验证证书真实性的过程。 有三种模式可以做到这一点：

a) 使用内置于证书本身的安全功能进行验证：这可能包括检查封条的真实性，特殊安全性文件，签名等措施。

b) 与原始发行人核实证书，由第三方联系原发行人，询问他们是否确实签发了证书。 （这里原发行人可能会咨询他们的集权索赔数据库，或检查自己的证书内置的安全功能）；

c) 通过与索赔集中数据库进行比较核实。 在这里，发行人可能已经列出了在第三方数据库中发布的所有证书，这将允许任何人查阅这个数据库来查看所有发放的证书的副本，并比较这两个证书。

3. **共**享：这是证书收件人与第三方共享该证书的过程。 共享证书有三种方式：

a) 直接将证书（或证书的副本）转让给第三方，
例如通过电子邮件发送，或者亲自向第三方展示；

b) 把证书存放在一个托管人的手里，这个托管人有权按你的要求只与某些人分享（例如，在私人遗嘱的情况下，公证人只能在受害人死后与受益人分享遗嘱内容）；

c) 发布证书，把它放在公共的注册表或商店里，每个人都可以查阅。

5.3 可信赖的认证系统的推动者

任何人都可以向任何其他人颁发证书，证明任何事情，证书制度的目标是证书被第三方广泛接受。 这要求第三方对系统及其流程有重大的信任。

通过以下方法和过程创建认证范围内的信任：

5.3.1 身份验证的方法

这涉及通过验证谁参与交易来创建信任。 由于证书涉及从一方到另一方的陈述，所以能够核实发行人和合格证持有人的身份是非常重要的。 身份通常使用身份证件进行验证，身份证件本身就是证明个人身份的证书。

在验证身份证明文件可能很复杂的情况下，通常涉及第三方来验证双方的身份。

5.3.2 发行和认证的标准化流程

单独了解交易双方的身份意味着第三方需要对前者有完全的信任。 由于这些情况很少出现，所以还必须相信发放证书的方式，特别是通过显示发行人已经达到了权利要求中所述结论的方法。

还有必要确保系统内的所有证书都是可预测和公平地发放的，即一旦符合某一套标准，只有符合这一套标准，证书才会发给任何人。 这就要求将这种方法记录在所有发行人都遵守的标准[19]中。

如果一个认证体系有多个发行人，而且每个发行人都采用个人或专有标准发放证书，那么不可避免的结果就是创建了多个子系统。 这些反过来又需要被单独和独立地理解和验证，以建立信任。 因此，在一个有多个发行人的系统中，整个网络的标准化水平越高，认证系统固有的信任水平就越高。

5.3.3 监管和保证机制

一旦建立了一套标准化的证书制度，就必须相信系统中的每一方真诚地行事，并按照他们的要求来执行这些标准。 因此，一个包含验证双方真诚行事的机制的证书制度，以及揭露（并可能消除）没有达成的各方，从而提高整个系统的信任度。

5.3.4 安全功能

希望验证证书中索赔真实性的第三方必须能够确保此证书不被伪造。 有两种方法可以防止这种伪造：

— 通过身份防伪机制，如签名，水印，特殊设计纳入证书本身，确保只有发行人可以提出具体的证书；

— 通过由发行人或称为登记处的中央数据库持有的已发出债权的数据库，借此第三方可以检查确实已经发出债权。

5.3.5 无障碍

信任证书的最后一个要素是要求方便访问。 这意味着：

— 证书的接收者应该能够持有证书的副本；

— 需要获得证书的第三方应该由持有人，发行人或注册管理机构轻松地批准；

— 证书应包含如何核实索赔的信息，以及用于提出索赔和签发证书的标准和程序；

— 证书中的信息应该清晰，易读，易于使用。 如何做到这一点包括：

- 规范证书本身的内容；
- 确保证书是机器可读的。

([19]) 标准可能是开放的，专有的或法定的。

5.4 教育认证的使用

5.4.1 学习者使用的证书

证书在整个教育中广泛使用，用于各种目的。 证书通常发给学习者认识：

— 完成一个具体的学习经历。 这方面的例子可能包括正式教育的离校证书，出席/参加非正规教育的证书或证明移动经验的证书；

— 在特定领域取得的全部学习，例如颁发学位证书的证明；

— 离散的学习单元，通过实现具体的学习目标，例如通过在高等教育中授予ECTS学分；

— 有助于学习的具体经验，如证明学徒完成的证书或另一种工作经验；

— 具体技能的获得，例如通过在承认先前学习的程序中颁发的证书；

— 达到某些卓越标准，例如赢得某些成就奖，或者以"荣誉"毕业。

— 通过颁发考试证书或等级卡在特定领域取得具体的能力水平。

通常，向学习者颁发的证书由对个人学习证据感兴趣的利益相关者使用。 例如：教育机构对此感兴趣，以确定个人是否适合升读另一级教育； 招聘人员和潜在的雇主有兴趣确定候选人是否适合开放就业机会。

文献还指出认证在教育中作为激励工具的用途，通过授予证书以实现具体的中级学习目标（Gibson等，2015； Abramovich，Schunn，&Higashi，2013），通过学习的游戏化。 这种正在进行的形成性评估和认证已被证明可以提高注意力，回忆和总体学习成果。

5.4.2 使用认证证书

认证是权威机构正式承认一个机构或个人有能力执行具体任务的程序（ISO / IEC 18009：1999）。 认证通常通过证书进行证明。 教育中使用多种形式的认证：

— 教育机构被认可，被授权经营。 这种认证的例子包括政府颁发给大学或学校的认证；和软件公司颁发给培训中心的认证，以教授特定的软件包；

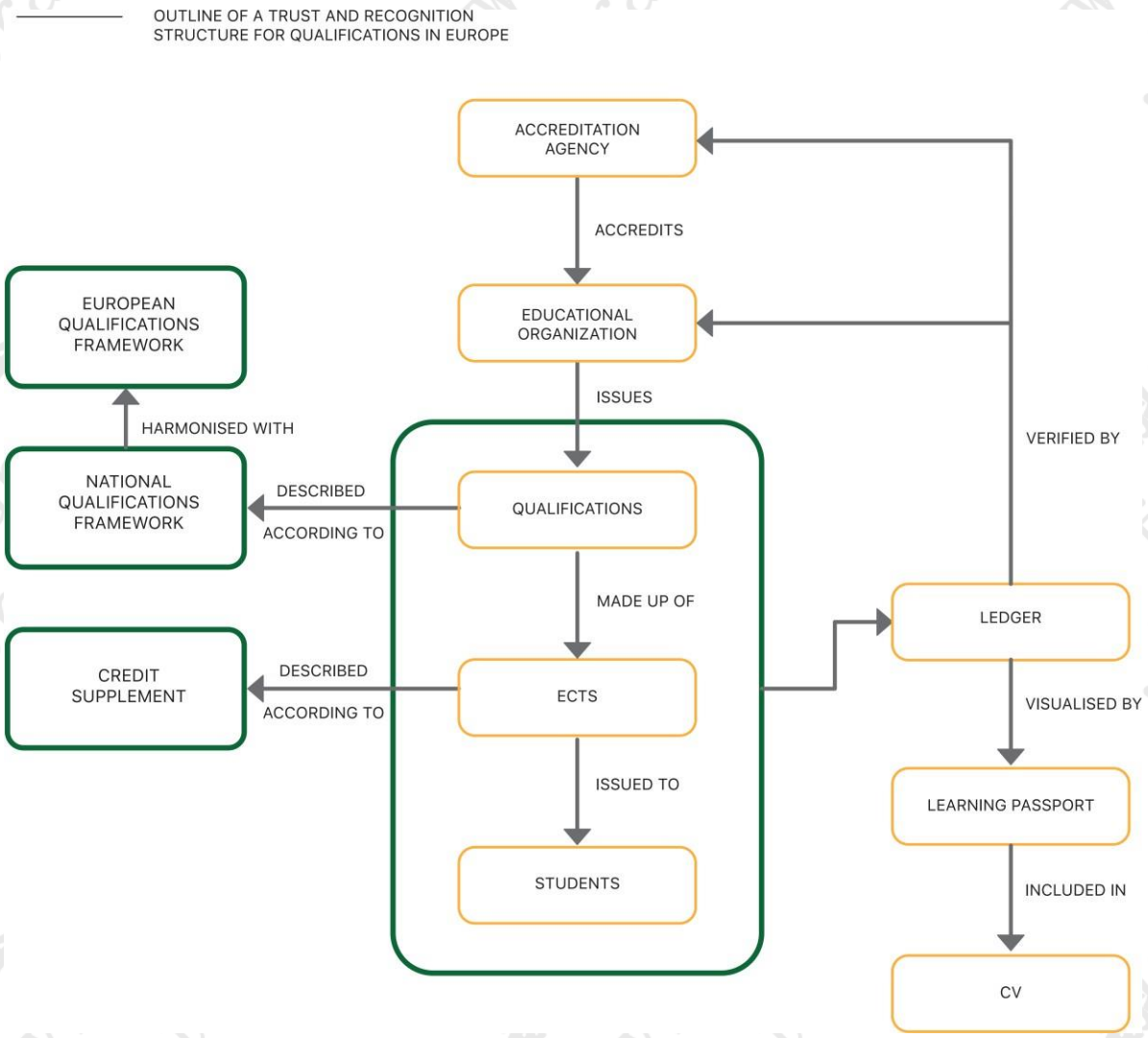
— 具体的教育计划获得认可，允许在认可的教育机构内进行教学；

— 教师经常被认定为具有特定的技能，被允许声称自己是教师，并在具体的学校任教；

— 授权学校和教师的机构本身是由高级监督机构认可的，这确保了他们按照既定的规则进行认证。这种认证的例子是由欧洲质量保证登记（EQAR）颁发的。

许多这些证书和认证通常与认证链相关。 因此，例如，一名学生只有在颁发认证课程后才能获得证明其学位证书的证书，而该认证课程又由认可的大学颁发，而认可的大学则由认可的质量保证机构认可。欧洲高等教育的典型认证结构如下：

图3：欧洲资质信任和认可结构概述



资料来源：安东尼（Camilleri），安东尼（2017）：欧洲资历认可结构概述。 看到 https://doi.org/10.6084/m9.figshare.5372758.v1

5.4.3 证书跟踪知识产权的使用

注册和跟踪知识产权是所有学术体系的重要组成部分。 知识产权创造价值，反过来它的使用可能会产生成本。

为此，一大批中央机关用来管理各种知识产权。 尤其是：

— 研究期刊证明一项研究是新的，研究是按照严格的科学标准进行的 – 这些信息被用来确定科学的真相；

— 数据公司证明了一个研究或开放教育资源（OER）已被使用的次数。 这是用来确定研究或OER的重要性，往往相应地补偿作者；

— 专利局对一项发明的第一个发明人进行了认证，并授予他们垄断权，从中获得了这项发明多年的利益。

5.4.4 财务事宜证明书的使用

证书也广泛用于财务原因，包括跟踪：

— 付款收据；

— 学生资助奖励；

— 学生贷款奖励；

— 放弃和/或修改学生贷款。

5.5 证书的限制

虽然政府和行业的数字化努力正在世界各地进行（Cheng等，2016），但大多数记录仍然以纸件或其他物理格式发行。 证书没有"完美格式"，许多国家使用混合证书，凭证由数字数据库备份。

然而，每个系统的重大限制清楚地表明需要更好，更强大的认证技术。

5.5.1 纸质证书的限制

纸质证书在很多方面仍然是最安全的认证形式，因为它们是：

— 由于证书本身内置的安全功能，难以伪造；

— （通常）由收件人直接持有，由此完全控制其证书；

— 相对容易长时间安全地存放，例如将它们放在安全的地方；

— 他们可以由任何地方的接收者，任何人出于任何目的。 但纸质证书也有明显的缺点：

— 虽然很难伪造，但没有证书是免于伪造风险的。 因此，发行人有义务保留可用于验证证书真实性的已颁发证书的中央注册表；

— 证书注册管理机构是单点故障：虽然证书可以保持有效，但验证它们的能力将会丢失；

— 保存这种索赔登记册并回答关于证书有效性的查询是一个手工过程，需要大量的人力资源；

— 物理证书中的安全特征完全来源于创建文档所需的难度级别和专业知识。 证书越安全，生产成本就越高。 一次性安全证书，例如护照，一般需要20至150欧元；

— 对发行人欺诈性陈述证书的时间戳或其他细节的能力没有限制；

— 一旦签发，没有办法吊销证书，不让业主放弃对其的控制；

— 如果第三方需要使用证书，例如验证简历中的声明，他们需要单独和手动读取和验证每个证书，这是一个耗时的过程。

5.5.2 （非区块链）数字证书的局限性

数字证书比纸质证书有许多优点：

— 他们所需要的资源要少得多，因为：

  - 证书的真实性可以自动在注册表中检查，无需人工干预；
  - 如果第三方需要使用这些证书，那么如果这些证书是以标准格式发布的，则可以自动整理，验证甚至总结；
  - 证书的安全性来源于密码协议的安全性，这确保了证书的生产成本低廉，但是除了发行者之外的任何人都可以复制成本极高的证书；

— 证书可以由发行人撤销；

— 根据系统的设计，某些类型的发行者欺诈（如更改时间戳或更改证书序列）可能变得不可能

但是，数字证书也有明显的缺点，即：

— 没有使用数字签名，他们是非常容易伪造；

— 在使用数字签名的情况下，这需要第三方证书提供者的参与来保证交易的完整性 – 这些第三方对认证和验证过程的每个方面都有重大的控制权，可以被滥用；

— 在许多国家，数字签名没有普遍使用的开放标准，导致证书只能在特定的软件生态系统的环境下得到验证；

— 销毁电子记录更容易 – 保持安全性需要复杂的多层备份系统，容易出错；

— 如果注册管理机构失败，证书本身变得毫无价值，因为不像纸质证书，没有注册管理机构，它们就没有内在价值。

— 数字证书注册管理机构容易发生大规模的数据泄露。

5.6 使用区块链技术的数字证书

区块链技术是保证，分享和验证学习成果的新基础架构的理想选择（Smolenski，2016）。 在认证的情况下，区块链可以保存每个证书的发行者和接收者的列表，以及公共数据库（区块链）中的文档签名（哈希），该数据库存储在世界各地的数千台计算机上。 在区块链上保护的数字证书比"常规"数字证书具有明显的优势，其中：

— 他们不能被伪造 – 可以确定地证实该证书最初由证书中所指明的同一人签发并由其接收[20]；

[20]请注意，尽管这允许证书与发行人或收款人明确匹配，但它不能防止发行人或收件人冒充他人或机构。 防止身份欺诈可能需要公钥注册管理机构作为经过验证的列表，哪些人拥有哪些公钥，这些公钥可能由供应商和公共机构作为服务来维护。

— 任何可以访问区块链的人都可以通过简单的开源软件进行证书的验证 – 不需要任何中间人；

— 由于不需要中间人对证书进行验证，即使发布该证书的组织不再存在或不再存取已发布的记录，该证书仍然可以被验证。

— 只有在托管该软件的世界上的每台计算机上的每个副本都被销毁的情况下，才能销毁在区块链上签发和接收的证书的记录；

— 散列仅仅是创建用户持有的原始文档的"链接"的一种方式。 这意味着上述机制允许发布文档的签名，而不需要发布文档本身，从而保护文档的隐私。

5.6.1 接受者的理想特征

从接收者的角度来看，区块链满足以下理想的证书要求：

— **独**立性：接收方拥有凭证，在收到凭证后不要求发卡机构或验证第三方参与；

— **所**有权：收件人可证明所有权凭证；

— **控**制：收件人控制他们如何管理自己拥有的凭据。 他们可能会选择将证书与他们自己拥有的已建立的个人资料相关联，

— **可验证性：证书** 可以通过第三方验证 各方，如雇主，招生委员会和核查组织；

— **永**久性：凭证是永久记录（受10.3中讨论的限制）

5.6.2 发行人的理想特征

区块链从发行者的角度来满足证书的以下理想要求：

— 发行人可以证明他们已经出具了证件；

— 发行人可以在凭证上设置到期时间；

— 发行人可以吊销凭证；

— 资格认证系统是安全的，并且承受最小的持续负担。

5.6.3 其他特点

为使实际证书具有意义和实用性，必须确信证书的真实性，第三方验证者（例如接收凭证作为应用程序的一部分的机构）必须确信。 以下是标准要求：

— **诚**信：内容没有被篡改；也就是说，它与发行人最初的目标相符。

— **真**实性：相信发行人是谁的证书要求，并没有被伪造。

5.7使用区块链验证身份

从技术角度来看，一个人的身份是由他们所有的个人身份信息（PII）组成的。

当一个人希望向另一个人或机构确认他们的身份时，他们将分享许多个人身份信息。 因此，例如，未来的学生可以通过提供他们的姓名，地址，政府身份证号码，性别和年级来确认他们的身份。 通常情况下，招生办公室将所有这些数据保存在一个集中的数据库中，要求用户信任他们关心数据的安全性。 但是，由于这些数据的价值，它最容易受到诸如滥用，欺诈和盗窃等风险的影响，最近一大批来自世界各地政府和企业的高调大数据泄露就证明了这一点。 目前，每当一个人需要与新的人或组织进行交易时，他们又需要交出数据，并且再次控制数据的保护和共享。

区块链技术实现了自我主权认同的新概念，即用户将自己的个人身份识别信息存储在智能手机等个人设备上，并仅在必要时与第三方共享。 这是将您的纸质证书保存在家中的安全数字证书，并将其显示给第三方以证明您的身份，但要确保这些第三方是否可以复制这些文件。 区块链技术还允许用户认证他们的身份，而不需要共享构成该身份的底层数据。

5.7.1使用认证的自主标识

一旦一个人拥有完全自主的身份：

— 他们的个人数据被数字化地存储在一个只有他们有权访问的设备上，并且被他们控制，例如设备级别的钱包；

— 无论是由声明还是数字文档组成的数据的散列都可以存储在区块链中；

— 该数据的真实性由第三方认证，例如发证或验证机构，证书也是：

  - 与该人的其余数据一起存储在安全设备上；
  - 散列在区块链上。

有了这些要素，只要证明他们是与证书索赔相关联的公钥的所有者，并且不需要共享任何个人可识别的内容，就可以向任何也信任验证机构的任何一方安全地识别自己信息 – 甚至没有他们的名字。

因此，继续我们的例子，一旦大学的学生获得奖学金，他们可能需要将自己确定为大学其他部分的奖学金获得者。 例如，他们可能有权从大学书店免费书籍。 传统上，大学书店需要持有哪些学生有资格获得奖学金和免费书籍的数据才能够提供这项服务。 因此，为了获得免费的书籍，学生需要允许书店持有非常敏感的信息，从中可以推断学生的经济状况和他们的家庭情况。 经过验证的自主主义身份，书店不需要任何数据。 学生只需出示"奖学金获得者"声明（存储在他们的电话或其他设备上），然后通过输入密码或在手机上扫描指纹来证明他们是该证书声明的所有者。 由于书店所有者相信证书发行者（即招生办公室）已经适当地验证了身份，并且由于区块链的安全性和不变性而可以信任证书，所以他们可以给学生书本，而不需要存储任何一个片段关于学生的任何信息。

5.8直接使用区块链发布证书

只要证书具有可衡量的价值，就可以将其表示为令牌，并直接在自定义区块链上进行交易。 因此，例如在以下区块链上：

— 学校毕业证书，单一的证书可以被视为一个令牌；

— 教育学分，1 ECTS等于一个标志；

— 跟踪期刊论文的参考，一个参考可能等于一个标记。

因此，证书可以从一个人转移到另一个人，只需在区块链上转移一个标记即可。 有关证书的更多信息可以存储在：

— 直接在区块链上；要么

— 通过从区块链条目链接到它。

因此，有可能设计一个数据库，其中一些信息将是私人的，由用户持有，而其他信息将在区块链上公开。

直接在区块链上签发证书的好处是，证书本身，而不仅仅是签名的证明，变得不可变和永久。

缺点是这种方式使用的任何通用区块链的大小都会大大增加，这意味着会导致性能低下和资源使用率高。因此，这种模式只能作为一个私人/许可区块链来实现（关于区块链的资源使用情况，请参见第10.2节）。

在区块链上发布文凭补充

从实际的角度讲，学位证书只能提供很少的信息。 它包含日期，颁发机构，获奖者和学位的名称。因此，马耳他大学可能会在15日2017年6月向Jane Doe颁发科学学士学位（荣誉）。这是很少量的信息可以很好地存储在分类帐中，链条上的小空间。 因此，它可以在区块链上发布：

- 如果目的是建立一个公开获取的学位数据库，
- 作为证书的散列（使用诸如Blockcerts之类的系统），目的是为了保证颁发给学生的数字证书。

欧洲高等教育区的毕业生有权获得文凭
补充其资格，另外说明：

- 其资格的水平和功能；
- 获得的内容和结果；
- 补充证明；
- 有关国家高等教育系统的细节；
- 任何额外的相关信息。

这些信息可以分成几个页面，而且很适合存储在一个

数据库，它不太适合存储在分类帐中。 此外，将这一级别的信息直接存储在区块链上的成本过高。因此，资格连同文凭补充可以在区块链上发布：

- 在明文中包括时间戳，授予机构，获奖者，学位的名称，并链接到文章补充的全文链接在外链
- 作为证书的散列[21]（使用Blockcerts等系统）的目的是为了保证颁发给学生的数字证书。

[21]请记住，无论文档的长度如何，文档的散列总是相同的长度。

6 区块链技术的技术特点

本章介绍区块链技术的技术基础。 希望了解区块链技术如何完成上一章所述权利要求的读者应该阅读。 对于那些希望在面值的情况下采取这些声明的人，我们建议跳过这一章。

6.1 区块链的原则

6.1.1 从集权到分配

集中式分类帐是交易记录的单一权威列表。 这方面的一个例子可能包括国家土地登记处。 以计算机术语来说，集中式数据库被存储并在单个中央节点上执行。

集中式分类账的一个变种，有一个分配要素，涉及多个当事方分担单个权威分类账的不同部分的责任。 因此，考虑由区域办事处管理的国家土地登记处，每个办事处只在其管辖范围内处理和储存交易 – 但所有这些都最终构成一个单一的国家土地交易数据库。 在这个计算机化的实现中，每个节点只存储其数据库的一部分并执行其部分代码。

如果中央计算机（服务器）停机，则防止访问其账本。

分权和分配一个分类帐涉及到完全通过建立一个系统来取消中央控制权：

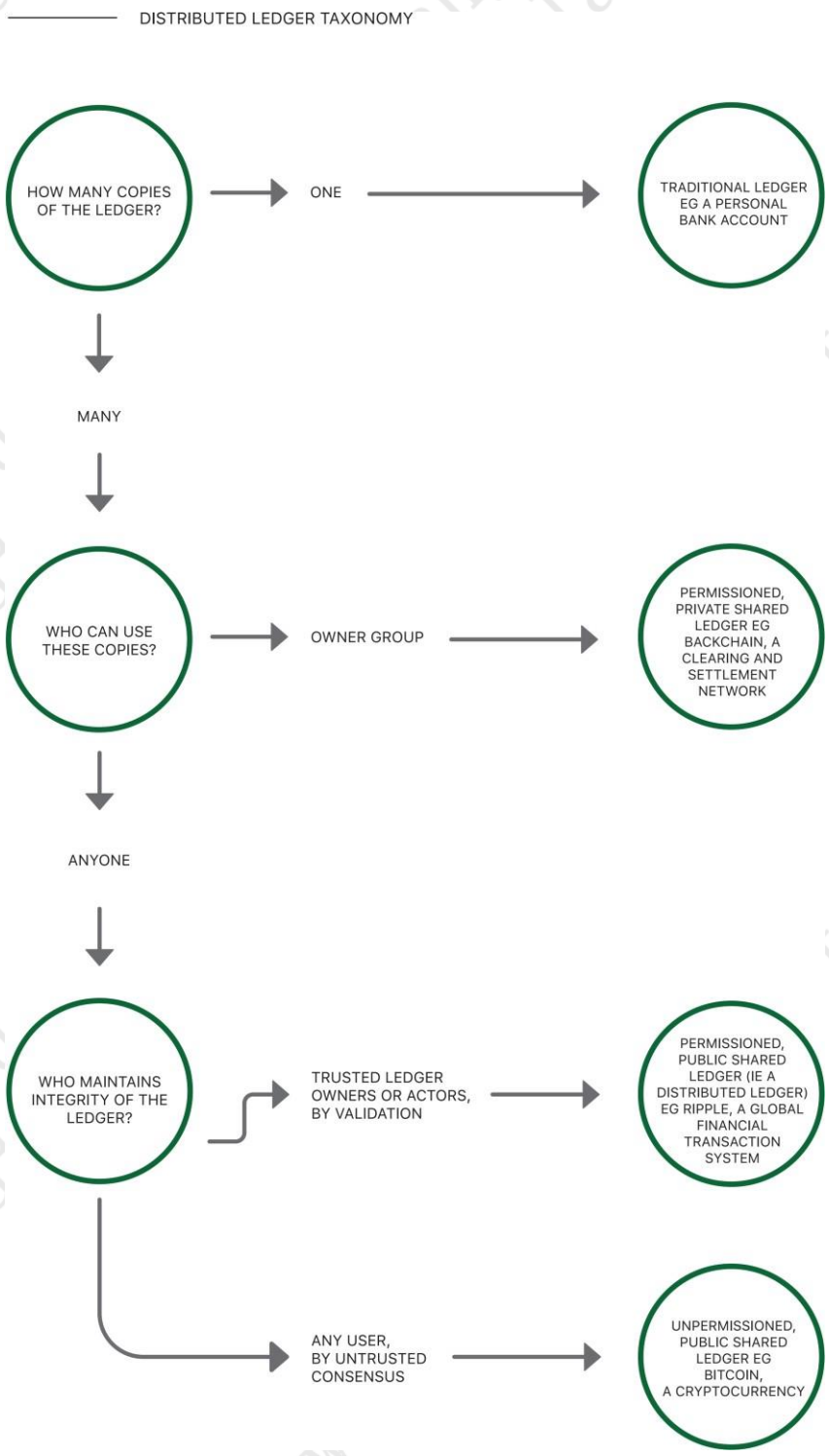
— 有几个人保留整个分类帐的副本；

— 编写或修改分类帐需要有副本的人的共识；

— 每一项增加或更改都记录在分类账的每个副本中，因此每个副本都具有同等的权威性（Peters& Panayi，2016）。

一个分布式的，分散的网络只会在每个单个节点关闭的情况下下降，使其几乎总是可用。

图4：分布式分类账分类



来源：改编自分布式账本技术。 超越区块链：英国政府首席科学顾问的报告

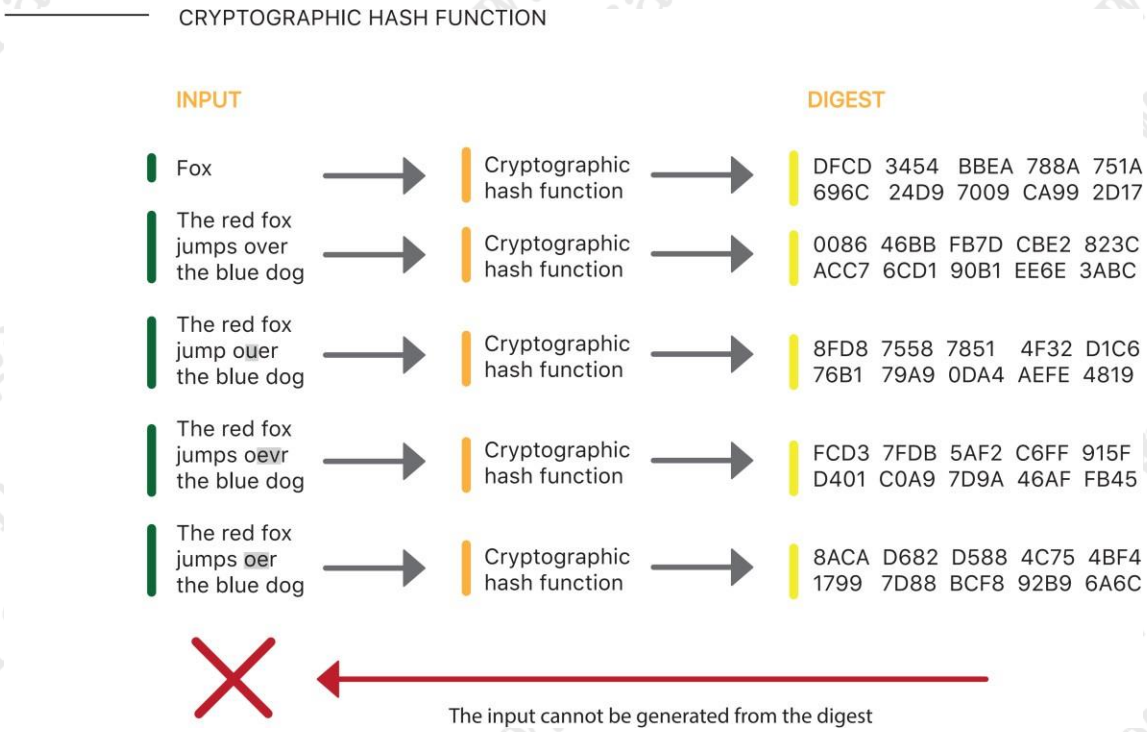
6.1.2 哈希

散列是定义长度的短代码，用作数字文档的指纹。 被称为哈希生成器的程序允许用户上传任何文本字符串

并创建一个唯一的ID。 每次通过哈希生成器运行相同的文本字符串时，它将给出相同的文档ID。 哈希作为防翻译设备的贡献是显着的：如果文档中的单个字母被改变，它将自动生成完全不同的ID。

哈希是单向的。 这意味着哈希生成器可以用来从文档生成哈希，但从数学上不可能从哈希生成文档。

图5：加密哈希函数



来源：改编自：https://commons.wikimedia.org/wiki/File:Hash_function.svg

在区块链中，每个交易块都通过包含信息块的散列以及前一个块的方式来保证安全，从而允许所有各方保证没有交易被修改或篡改。

6.1.3 公钥和私钥

公共密钥实际上是可用于识别个人的公开可用的ID号码。

私**钥实际上是一个密码，它已经在数学上与公钥相关联。**

当使用公钥/私钥对时，用户可以通过将他们的私钥详细信息输入到软件中来验证他们确实是公钥的所有者；这将会依次检查两个键是否真正数学关联。

这个函数实际上不能反向运行 – 也就是说，如果只有关于公钥的信息，则几乎不可能产生私钥

6.2 区块链的体系结构

6.2.1 分散交易资产的数字网络

作为面向网络的软件实现，区块链将代码执行和数据存储的风险和责任从集中式机器转移到分散式网络。

区块链用于记录数字资产的交易。 交易被建立在大多数区块链协议运作中的最基本的资产是以令牌形式（比如比特币，以太币，莱特币等）的加密货币。 但是，它们也可以用来交换其他资产，例如土地所有权或身份证明文件（请参阅章节4.3).

每个区块链网络对于交易的资产类型以及交易发生的条件都有不同的规定。 这些规则被编码到它的软件中。

运行区块链软件的每个设备都称为节点，并连接到运行该软件的节点网络。 当任何人可以建立一个节点并直接与网络上的任何其他节点进行交易时，这就是所谓的公共区块链网络。

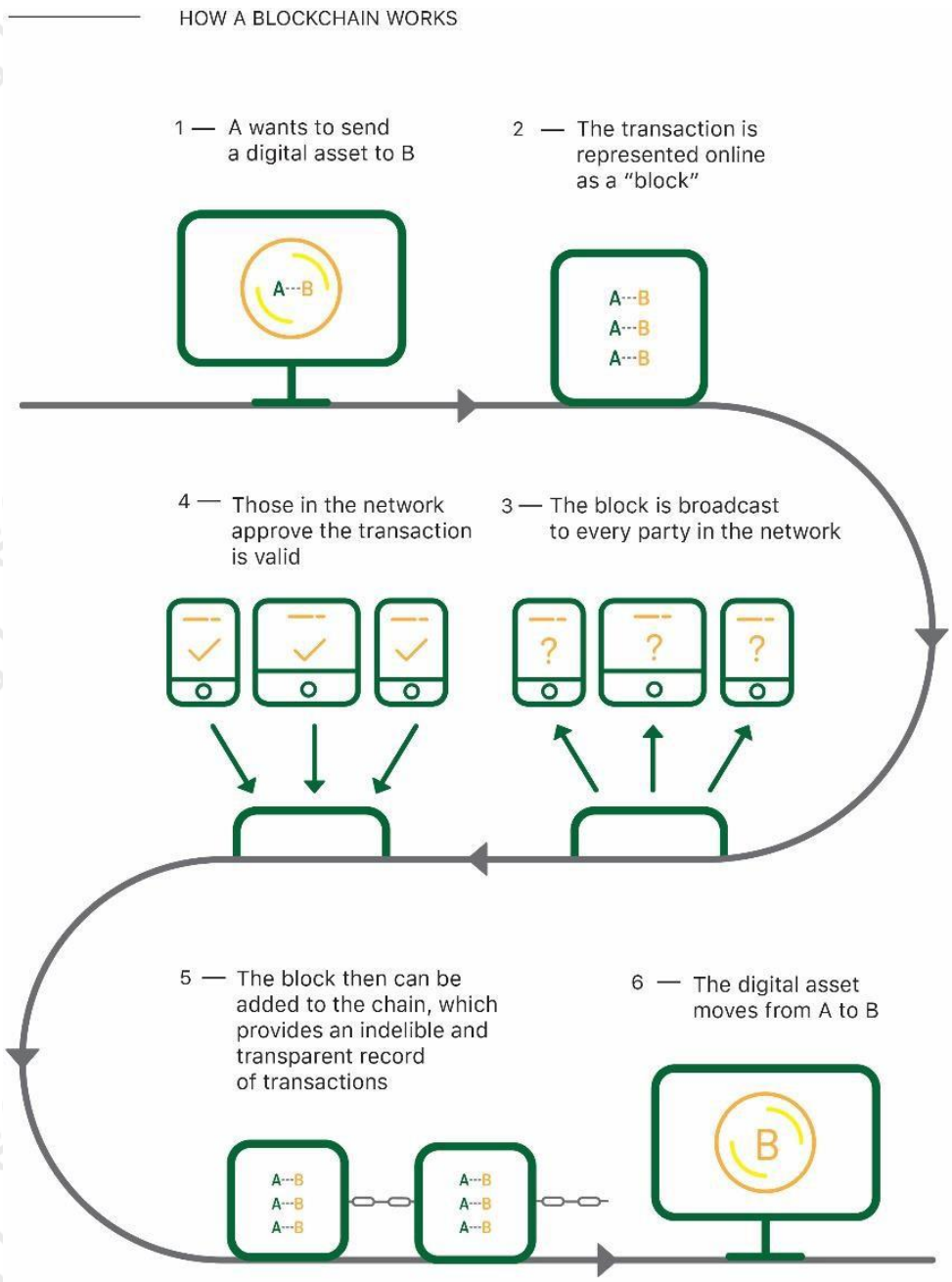
但是，如果设备连接到内部网络，即只有特定设备才能访问的专用网络，则可以在已被授权访问该网络的一组人员之间进行交易。 这被称为私人区块链网络。

区块链软件的体系结构确保只有区块链软件的相同副本可以相互交互[22]。 因此，如果有人更改软件的副本，他们有效地创建一个全新的区块链。 这就是所谓的“分叉”。自从2009年推出比特币协议以来，区块链软件已经存在多种分支：2017年8月，比特币区块链被分成一个叫做比特币现金（Bitcoin Cash）的新区块链。

协议身份确保网络中的所有设备在完全相同的条件下进行交易，而不需要中央机构验证规则是否被遵守。

(22) 这是通过哈希程序的整个软件代码来完成的。 如果软件的两个版本的单个代码字不同，哈希将不匹配，程序将拒绝相互通信。

图6：比特币区块链的工作原理



改编自瑞安（2017）

6.2.2 分散的分布式账本

区块链的核心是一个透明和自主的分散式分类账。 区块链软件的每个副本：

— 存储分类账的完整副本；

— 在收到来自网络其他部分的共识时，将新的条目写入分类帐；

— 将其用户所做的交易广播到网络的其余部分，以便通过共识和记录进行验证；

— 定期检查其分类帐的副本是否与网络其余部分的副本相同。

6.2.3 匿名验证身份和所有权的系统

交易按以下方式在区块链上列出：

图7：区块链上的交易

区块链软件可以发行一个人，该人拥有一个链接到其唯一公钥的比特币地址以及与其密码链接的私钥。

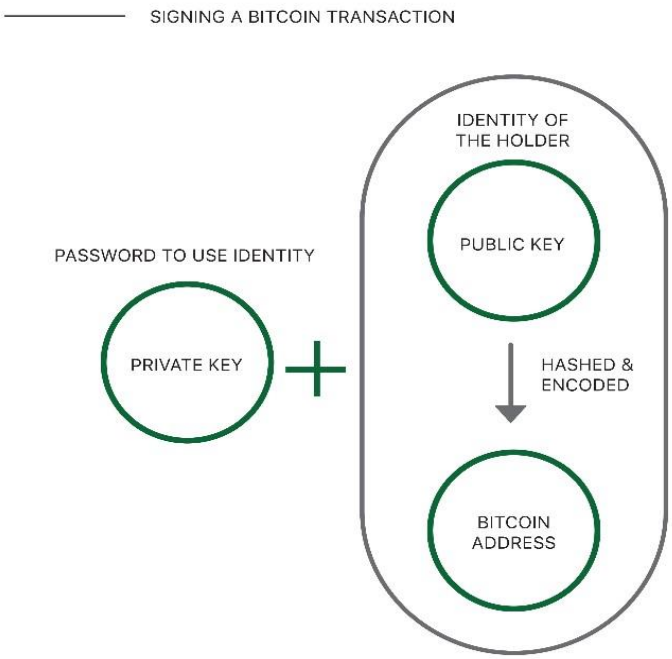
要向区块链写入新的交易 – 即传输与比特币地址相关联的资产 – 用户必须输入与创建时发给他们的公钥/比特币地址相关联的私有私钥。

已经转移到特定比特币地址/公钥的资产的所有权通过了解私钥进行验证。

因此，交易双方和公众都可以看到交易已经发生，并且可以在不知道交易双方身份的情况下识别谁拥有什么（Nakamoto，2013）。

交易中的每一方都可以通过简单地将他们的私钥输入到比特币软件中来使用他们的资产，而不需要向任何第三方或中间人证明或暴露他们的身份。

图8：在区块链上签署交易

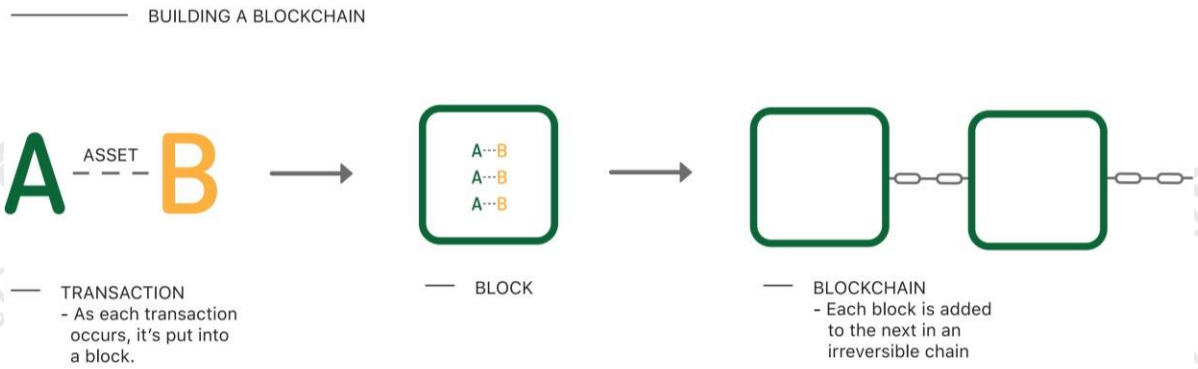


6.2.4 一个确保永久不可毁灭的记录的系统

比特币区块链中的分类账是"仅追加" - 这意味着交易只能被添加，并且不能被编辑或删除。

因此，每个新的事务都被添加到一个块中，而每个块被链接到前一个块形成一个链（见图10）。

图9：构建区块链



如图10所示，使用两组哈希来保证链的完整性：

— 块中的所有事务都被压缩，并通过使用称为Merkle根的特殊哈希函数来锚定到块。 该散列包含在该块的标题中。

— 每个块的头部还包括前一个块中所有信息的散列。

如果有人试图编辑链中的一个事务，它会立即使每个后续块的散列无效。

因此，对链条进行黑客攻击不仅需要改变事务，而且还要重新计算和更改自事务之后创建的每个数据块的头信息，并且对网络上一半以上的计算机这样做是非常不切实际的命题。

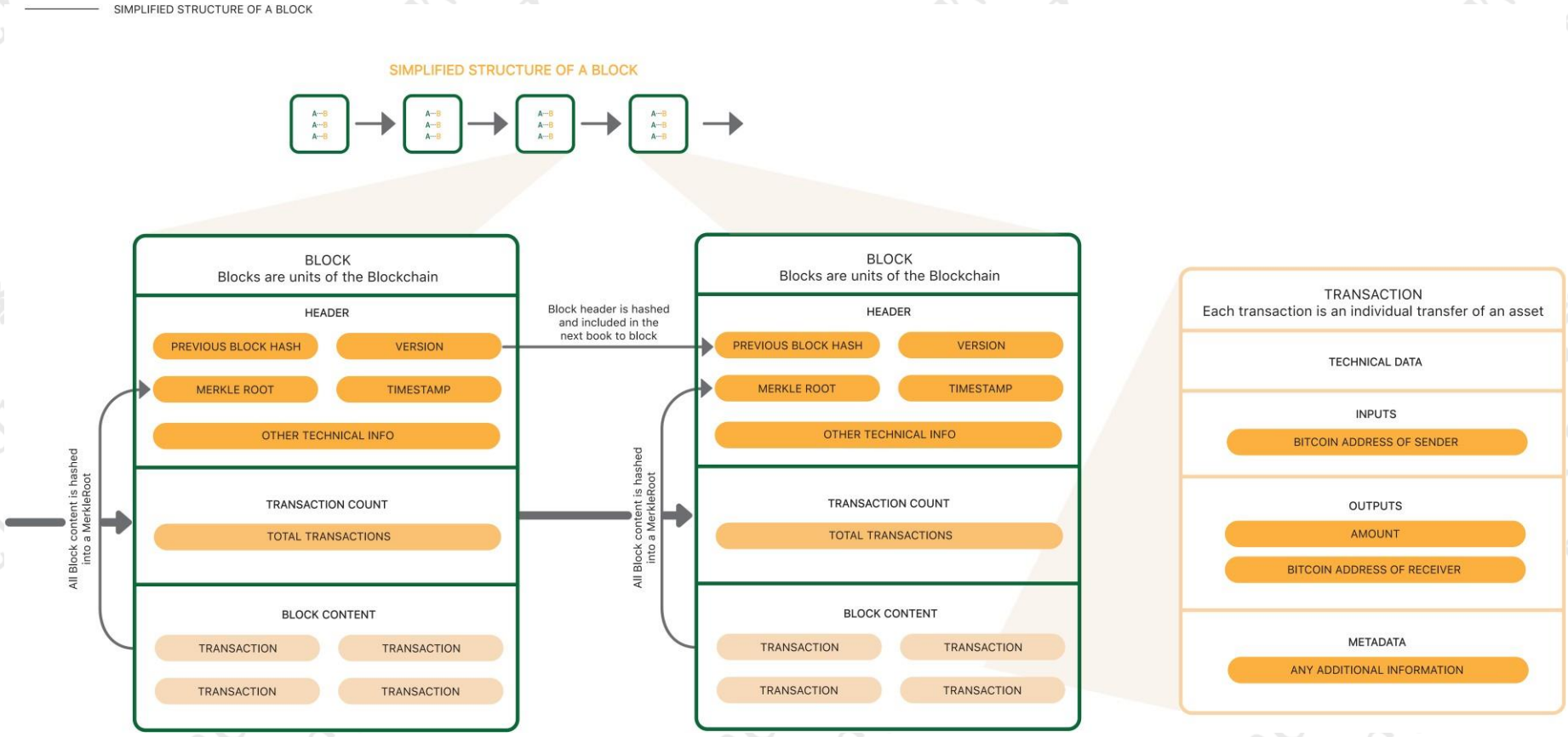
对于较大的区块链，实际上不可能改变任何交易，因为：

a) 这将需要不切实际的大量计算机处理能力；和

b) 随着链上的块数不断增加，进行这种改变所需的计算能力也总是在增加。

这是一个重要的考虑因素：计算能力的提高不会突然危及或使区块链的安全性过时。

图10：区块链的简化结构



来源：改编自https://www.slideshare.net/arcatomia/anatomy-of-a-blockchain/7

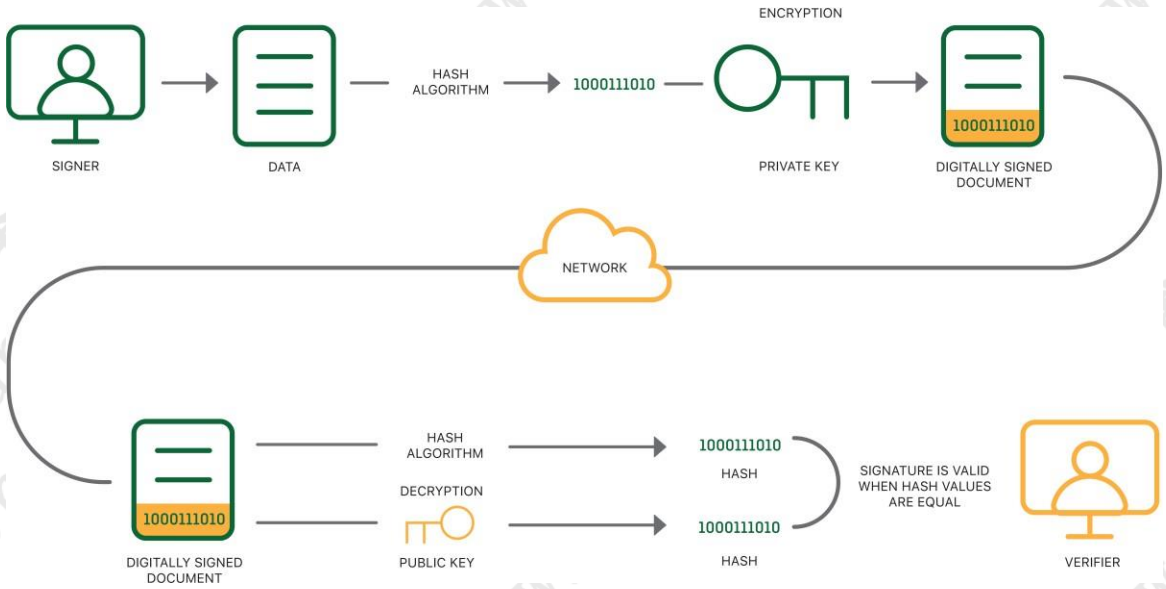
6.3 使用数字签名颁发证书

所有数字认证解决方案都使用数字签名系统来颁发证书。

数字签名与电子签名不同，电子签名只是在电子文档（例如用电子笔）上绘制的传统签名或扫描的物理签名。 电子签名容易复制或伪造，不提供验证或标准化的机制。

另一方面，可以使用数字签名来验证特定文件是否确实由特定人员签名。

图11：数字签名文档的剖析



改编自：https：//www.docusign.com/how-it-works/electronic-signature/digital- 签名/数字签名的常见问题解答

数字签名提供了一种通过允许一个人发放证书的方式：

— 用一个只有他们能产生的印章来标记文件

— 确保文件签名后不能被篡改。

为了使数字签名正常工作，他们要求签署文件的每个人都有一个身份号码（一个公钥）和一个链接的密码（一个私钥）。

6.3.1 数字签名的组成部分

数字签名由四个部分组成：

a) 一个SHA-256散列，它是一种散列函数（见5.2.1节）；

b) 公钥；

c) 一个私钥；

d) 时间戳列出了证书颁发的准确时间。

6.3.2 如何数字签署文件

通过将文档的散列与个人的私钥组合来创建新的唯一代码来签署文档。

然后将生成的签名与时间戳一起"加盖"或合并到文档中。

由于签名是这两个组件的组合，它：

— 对于这个特定的文档是独一无二的，因为它是从文档的散列创建的；

— 只能由拥有私钥的人创建。 应当指出的是：

— 由于签名被盖印在数字文档中，"签名"的数字文档具有与未签名的数字文档不同的哈希值；

— 应该在签名后更改文档的单个字母，这将再次具有完全不同的散列值。

此外，签名不能被反向工程发现一个人的私钥。

6.3.3 如何验证数字签名

如果第三方希望验证数字签名，则需要知道签名人的公钥。 由于公钥实际上只是ID码，所以通常可以在公共目录中查找，类似于电话簿。

验证软件通过输入文件和公钥来工作，并检查两件事：

— **该文件上的签名与原始文件的散列相匹配；**

— **该文件的签字在数学上与声称已经用他们的私钥签署文件的人的公钥有关。**

验证软件能够做到这一点，而无需泄露私钥。

6.3.4 数字签名系统

6.3.4.1公钥基础设施

在公共密钥基础设施中，称为认证机构的可信组织通过以下方式集中管理系统：

— 发行链接的私钥和公钥；

— 运行服务器为每个签名加上时间戳；

— 运行验证软件。

通常，证书颁发机构将公钥嵌入到包含一组附加元数据的证书中以方便使用。 这提供了几个优点：

— 认证机构可以验证发给密钥的人的身份，从而将公钥与现实世界的身份联系起来；

— 每个人都可以对签名的日期有信心，因为'时钟'只能由认证机构来维护。

但是，公共密钥基础设施也是控制和失败的中心点。 最关键的是，如果验证软件的认证机构关闭（比如破产，内乱，重组等），它将会有效

通过它签名的文件无效。 这为诸如出生，婚姻或教育成就等应该持续一生的证书提供了重大的问题。 此外，验证局可能会以本节已经讨论过的任何方式滥用信任4.1.

如果私钥被泄露，则没有任何事情可以阻止攻击者发布虚假记录和回溯内容。 即使发行人公开撤销这些记录，独立核查人员也不会知道有效和无效记录之间的区别，除非有额外的权限证明交易何时发生[23]。

6.3.5 使用区块链技术的数字证书

6.3.5.1 区块链安全数字证书的增值

区块链技术是保证，分享和验证学习成果的新基础架构的理想选择（Smolenski，2016）。 在区块链中，PKI用更强大的分散网络取代中央当局。 这种分散的结构增加了网络的寿命，因为存储签名的块的重复是如此之多。 区块链的分散使其具有进一步的优势，因为没有第三方可以改变或清除存储在区块中的交易，而不必取消验证它们的工作证明要求。

除了消除对任何证书颁发机构或可信任第三方的依赖之外，区块链提供了独立的时间戳，从而带来显着的安全优势。 一个可靠的时间戳在证书到期的情况下显然是非常重要的，但是对于一个实际的原因也是至关重要的 - 发行者必须能够定期轮换发行密钥，这既是安全最佳实践的一部分，也是对于一个关键的泄漏。 当发行密钥有效时，确定特定发行人发行的记录需要知道独立的时间戳。

与许多PKI系统不同，区块链上的签名也与文件格式无关：不管其创建的（专有）标准如何，相同的软件都可以用来签署任何类型的文件（Thompson，2017）。

6.3.5.2 区块链安全数字证书的体系结构

在认证的情况下，区块链将每个证书的签发者和接收者的名单连同公共数据库（区块链）中的文档签名（哈希）一起保存在世界上数以千计的计算机上。

[23] 请参阅：https：//github.com/blockchain-certificates/cert-schema/wiki/Why-the-blockchain

图12：区块链上的数字签名文件

ISSUER OF CERTIFICATE	HASH / DOCUMENT SIGNATURE	RECEIVER OF CERTIFICATE
1CytUYMWr439wms5MYjryCg5uM-sEhNHYW7	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1EUGqyEHbzGQ7hpvkPwm4XJG-FXC3duFvAn
1LSQXVvokuvBfRQUf8Q3rdkhVajK-gwHqoZ	d2bddd4516dd51e617fbb575a8384a1444a009b86d8d5c2440a28ed8d2db3790	1CytUYMWr439wms5MYjryCg5uM-sEhNHYW7
1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8	1b3793716c610c1a521d71b2f52c37e4c435d4cd990247ac0cd90a093f5d8fc8

施密特（Schmidt，2015,2017）描述了以Blockcerts（见7.1.1节）的方式颁发证书是一个相对简单的过程：

1. 创建一个数字文件，其中包含一些基本信息，如发行者和收件人的名称，发行者的名称（MIT Media Lab），发行日期，根据IMS开放式徽章标准构建的凭证，等等

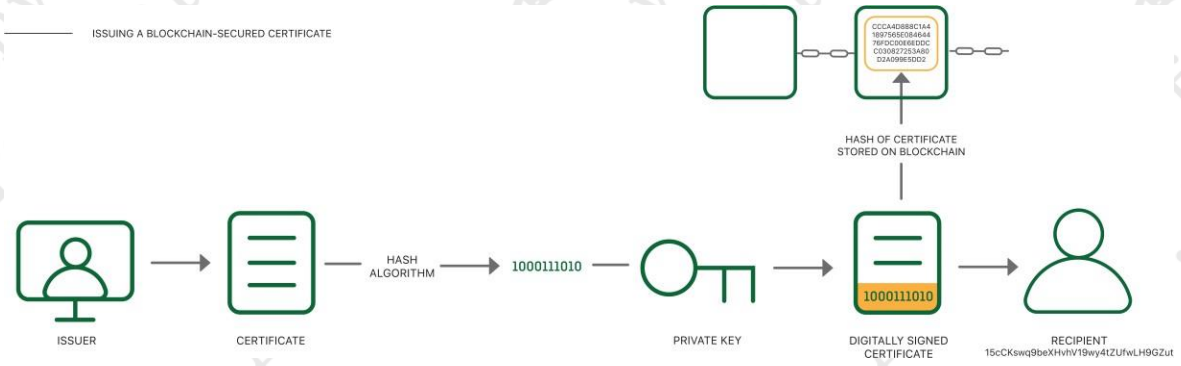
2. 发行人然后使用只有发行人有权访问的私钥对加密签名的证书内容进行签名。

3. 发行人将该签名附加到证书本身。

4. 发行人创建凭证文件的密码散列 - 可用于验证没有人篡改证书内容的字母和数字的短字符串。 如前所述，对应于数字文件的字母和数字恰好有一种可能的组合，对文件的任何改变都会导致不同的散列。

5. 最后，发行人再次使用私钥在比特币区块链上创建一个记录，说明我们在某个特定日期向某个人颁发了某个证书。

图13：发布区块链安全证书



数字凭证本身可以由用户存储在硬盘驱动器或移动钱包中，从那里他们可以很容易地与他人共享，甚至打印在纸上。 因此，用户有可能验证证书是由谁发给谁的，并验证证书本身的内容。

验证证书完整性和真实性所需的数据存储在区块链中。 因此，例如，为了验证凭证，雇主（或提供验证服务的公司）将基本上遵循上面的过程来确保散列对应于原始文件，并且发行者使用的密钥指向正确的机构。

在使用无权（或公开）区块链发行或接收证书的情况下，这意味着只要至少有一个数据库副本正在运行，任何人都可以使用区块链来确保签名和验证机制是永久可用的。 验证是通过比较被验证文档的散列和区块链上公开记录的散列来进行的。 如果它们匹配，则文件是真实的。

这还意味着，即使证书的颁发者不再存在，任何接收到在区块链上签名的证书的人都可以验证其真实性。

在使用权限（或私人）区块链的情况下，这意味着只有被允许访问特定区块链网络的人才能够在区块链上签发，接收或验证签名。

6.3.6使用区块链技术的自主标识

6.3.6.1在区块链上创建一个自主标识

> *资金交易的记录类似于授予证书的价值。 在区块链上公证的证书有时间戳，并且可以方便验证发行人和接受人的身份（ASU GSV Summit，Jagers）。*
>
> *文凭的所有权和控制权在同一个地方 - 这意味着他们在机构和学生之间平等分享。这已经是改变游戏规则了*
>
> *（灰色，2017 ASU GSV峰会）。*

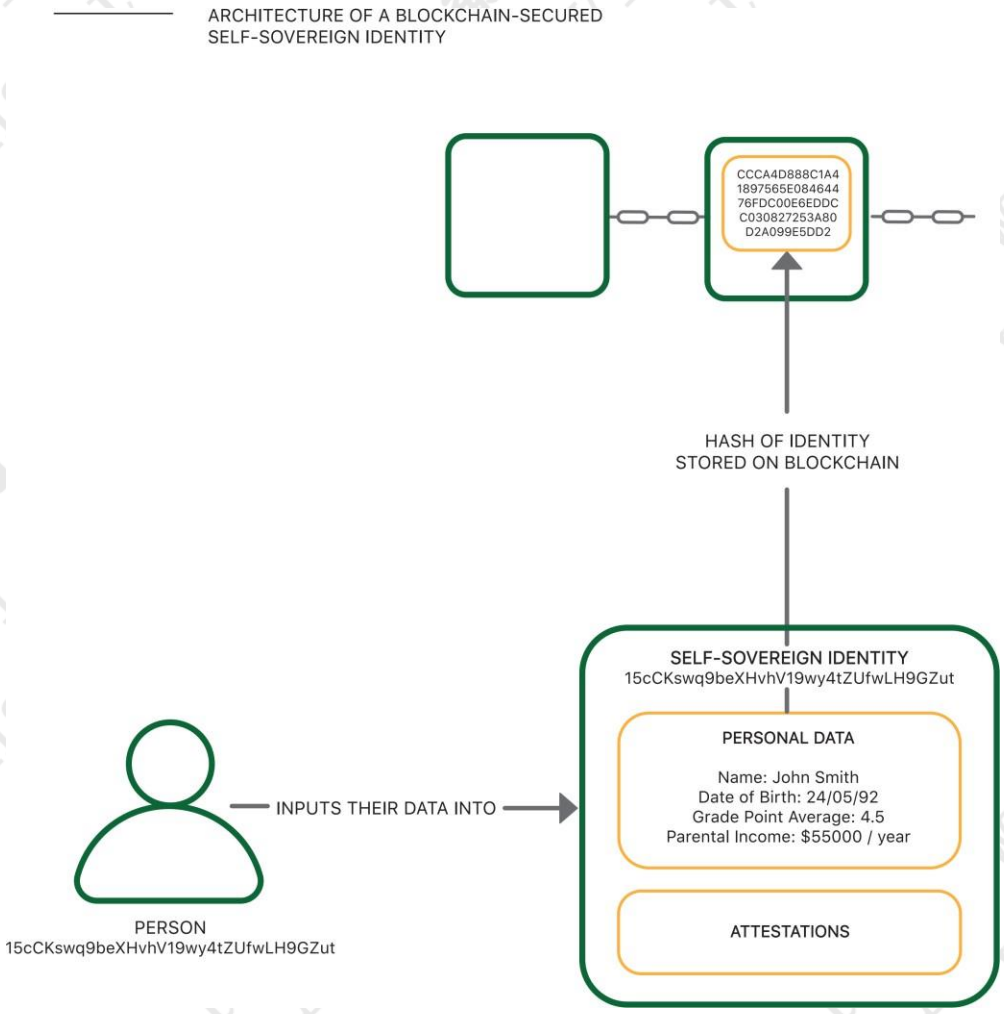
识别的新模式正在出现，尽管目前它们的含义不一定清楚。 一个单一的国家颁发的证书模型演变成一种扩展和网络化的方法，使用国家颁发的证书作为开始。 现在，当前的发展趋向于基于知识的身份属性聚合，通常在用户的控制之下更多。 这包括来自社交媒体的信誉分数，点对点分享和经济平台等。[24]

与数字签名一样，在基于区块链的自主主义身份系统中，一个人通过其公钥来识别。 他们通过输入他们的私人密钥证明他们是公钥的所有者。 在大多数自主主权识别系统中，这个私钥与生物识别信息（如指纹）相关联。

为了创造自我主权的身份，这个人只需要记录他们的个人身份信息并将其与公钥相关联。 这是通过使用自定义软件完成的，通常位于他们的智能手机上，他们可以使用他们的私钥/生物特征数据登录。 该软件在设备上加密其私人数据，并将该信息的散列上传到区块链。

[24]Hanson等人 （2017）

图14：使用区块链技术创建自主标识



来源：安东尼的卡米勒里； Grech，Alex（2017）：自主主义身份的体系结构。 看到：https://doi.org/10.6084/m9.figshare.5371510.v1https://doi.org/10.6084/m9.figshare.5371510.v1

6.3.6.2 证明自我主权的身份

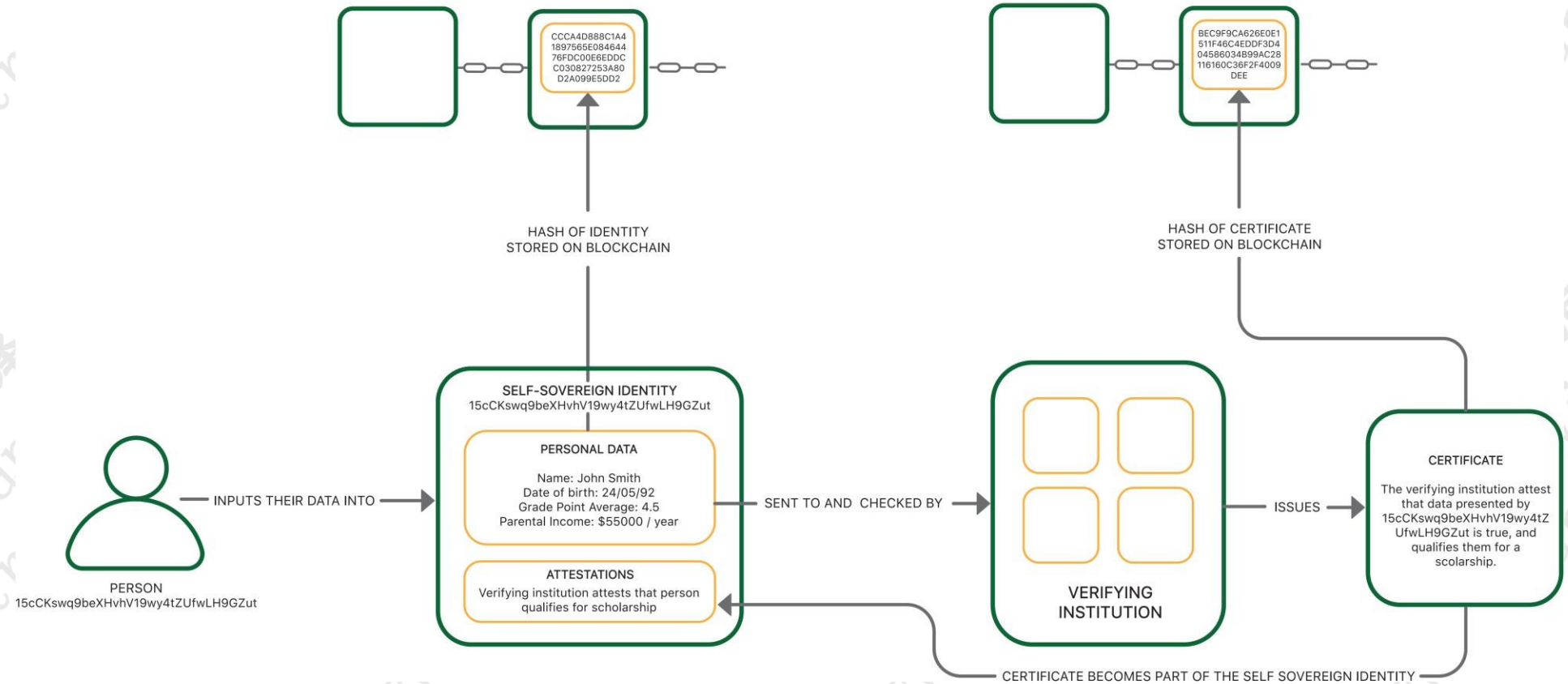
如果第三方需要证明一个人的数据是真实的，他们将需要：

- 该人共享有问题的数据，
- 证据表明这些数据是真实的。

检查完数据后，第三方可以发出证书，证明信息是真实的，例如"我已经证实这个散列信息是真实的"。如果此声明上传至区块链，则会提供公开证明，证明该人员的身份详细信息是真实的，无需披露任何有关此人的任何信息（除了公钥）。

因此，继续我们的例子，如果我们的大学申请人希望获得奖学金，那么招生办公室可能会以护照或出生证明的形式要求他们的身份证明，他们的成绩证明和财务状况。 如果检查了这些信息，招生办公室认为合适，他们可以颁发证书，证明该人有资格获得奖学金。 该证书的散列可以存储在区块链中，而证书本身可以存储在该人员的证书中 自主权 身份。

ARCHITECTURE OF A BLOCKCHAIN-SECURED
SELF-SOVEREIGN IDENTITY



来源：安东尼的卡米勒里； Grech, Alex (2017)："经过验证的区块链安全自主标识体系结构"。 看到：
https://doi.org/10.6084/m9.figshare.5371516.v1https://doi.org/10.6084/m9.figshare.5371516.v1

7 区块链技术在教育中的实现

区块链是一项在个人，机构，团体，国家和国际层面的学习领域显然具有应用性的技术。 它与各种情况有关：学校，学院，大学，MOOC，CPD，企业，学徒和知识库。 技术成为关注的焦点，而不是旧的等级结构，信任向技术移动，而不是机构。 这确实是一个脱媒技术。

唐纳德·克拉克

数字文件可以像纸一样短暂； 通常由供应商以专有格式发给客户，没有正确软件的机构可能无法读取或验证它们。 即使访问正确的软件，在许多情况下，验证过程可能是乏味和不确定的。 数字签名也是如此：即使在立法要求接受的地方，数字签名也有各种不同的安全格式，并不是所有格式都被认为是合法的证据。

数字文件的另一个挑战是人们通过数字方式共享信息的主要方式之一 - 电子邮件 - 通常是不安全的，因此需要构建专有的传输基础设施来发送敏感文档，如健康记录。 这极大地提高了邮件的安全性，但却增加了互操作性的难题。

最后，像纸质文档一样，数字文档也可能被复杂的用户以难以察觉的方式欺骗。

7.1 颁发证书

在证书问题中使用区块链技术时，不仅可以在没有中介的情况下验证证书，而且可以为现有的数字证书生态系统增添价值：BADGR和Mozilla Open Badge已经被用于提供数字在一些着名的学术机构向学生颁发证书。 因此，在区块链上公证证书的目的是将学生通常私下接收的数字证书转换成可自动验证的信息，可以通过不可变的证明系统在公共区块链上由第三方咨询。

在目前的实践中，访问公共平台几乎不可避免地要求学生分享或泄露"明智的"元数据，这往往包括私人信息。 通过使用区块链作为"知识证明"（Aglietti，2017a），在与认证有关的元数据的公开咨询期间，这些私人信息不一定必须被泄露。 在短期内，学生可能会接触学术机构和雇主，同时保持谨慎的保密水平：原则上，只有学生在证明生成过程中标记为公开的信息才能被第三方派对。

Aglietti（2017b）认为，软件组织可以促进和简化访问区块链的过程，为学生和证书颁发者（研究机构，公司，学校等）提供机会。 理想情况下，应用程序将建立在开源架构之上，可以保证终身和全方位学习成果的数据连续性，并且不会锁定一个特定的解决方案。 学术机构和公司不会是唯一利用平台和区块链上可用信息的问责性和一致性的机构。 学生可以利用公共元数据来寻找类似的概况，并在此过程中培养创造社会包容和创业精神的新模式：所有这些都不需要中央当局担保信息的有效性。

7.1.1 Blockcerts：区块链教育证书的开放标准

Blockcerts开放标准的基石是相信人们应该能够拥有和证明其重要数字记录的所有权。 这些记录构成了证明自我方面的基础，符合自主主义身份的原则（参见Allen 2016，Jagers 2017b，Lewis 2017）。 在这种情况下，区块链被认为是一种技术，允许个人拥有其正式记录，并与任何第三方分享即时验证，而一直排除任何企图篡改或编辑记录。

麻省理工学院媒体实验室和学习机器公司（一家企业软件供应商）已经开发了用于在比特币区块链上签发和验证凭证的Blockcerts开放标准（MIT Media Lab 2015；Schmidt 2016）。 Blockcerts目前是在区块链上签发和验证记录的唯一开放标准，Blockcerts社区的目标是推动其被采用为在区块链上发布记录的主要全球标准（在社交领域）。

该标准允许包括教育机构和政府在内的任何用户使用基本代码，并开发自己的软件进行发布和验证。Blockcerts是免费的，供任何人使用，没有信贷或版税给其核心开发者； 从Blockcerts社区论坛的扫描中可以清楚地看到，世界各地的一些组织，初创公司和个人正在使用它开发应用程序。 Blockcerts对于Blockcerts移动应用和钱包的收件人也可免费下载iOS和Android；它的代码也是完全开源的。

制作Blockcerts开源软件的目的是为了避免开发人员认为标准战争和供应商锁定是易于互操作性和广泛采用的两个主要障碍，这是真正的收件人拥有正式记录的先决条件。 被困在孤岛中的数据是现状，被Blockcerts社区视为区块链给我们提供超越的重大挑战。

Jagers（2017）声称，Blockcerts为移动钱包设定了先例，该移动钱包符合数字自主权最重要的统一标准：接受者所有权和供应商独立性。 在这种情况下：

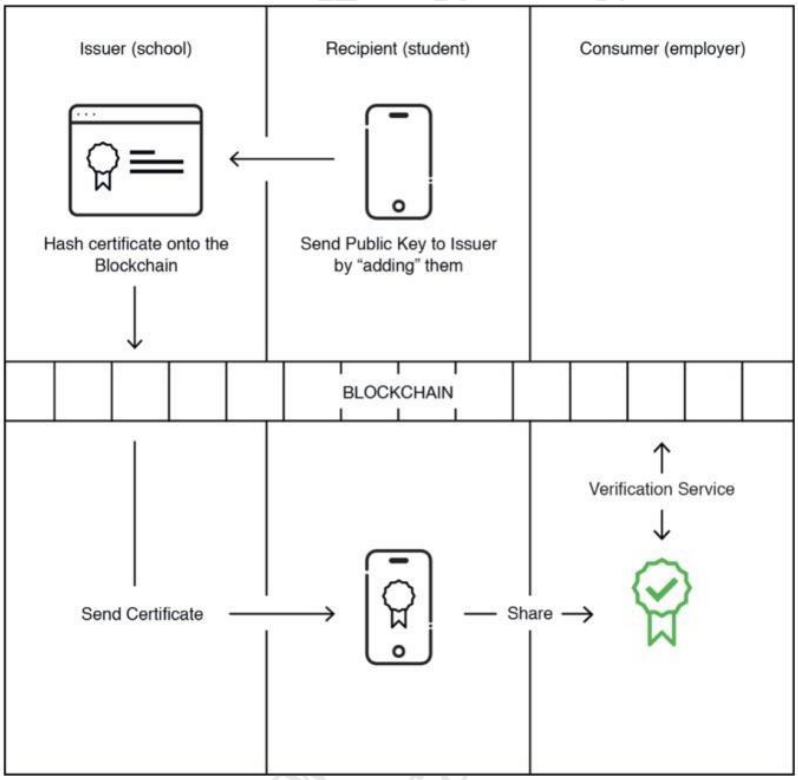
— **接**受者所有权意味着个人控制私钥，使他们能够证明金钱或数字记录的所有权。

— **供**应商独立性意味着访问，显示和验证不依赖于任何特定的供应商。 基于开源标准时，记录可以独立于任何供应商进行迁移，共享和验证。

引用这两个条件的组合是保证个人独立拥有个人数据的唯一方法。

图15下面是这个过程的高级视图：

图15：在区块链上发布和验证证书的简单流程图



来源：Blockcerts（2016）

Blockcerts的建立是为了提供一套通用的模式，以便在任何区块链以及跨不同的市场领域发布和验证证书。 根据参与该项目的主要开发人员[25]，当2015年开始研究时，比特币区块链是支撑终身数字记录的潜在区块链的合理选择。 在2016年，有关于向Ethereum扩展资源的一些讨论，但当时Ethereum的硬分叉使得需要持续一生的凭证看起来并不可靠。 当时做出的决定是尽可能使比特币文件尽可能有用，同时保持对比特币的封锁。 在2017年，Ethereum与开发人员获得了巨大的发展势头，许多人要求Blockcerts将文档（和参考实现）扩展到以太坊。 由于Blockcerts是一个开源社区，因此有几个开发人员正在为扩展而做出贡献[26]。

Blockcerts社区与以下标准化社群保持一致（并为之贡献力量）：IMS Open Badges[27]； W3C可验证声明[28]； W3C关联数据签名[29]和W3C /重新启动信任分散标识符网[30]。

---

(25) 查看社区网站上的讨论，包括http://community.blockcerts.org/t/why-the-bitcoin-http://community.blockcerts.org/t/why-the-bitcoin- blockchain/153

(26) Blockcerts被设计用来写入和验证任何区块链，所以链式分割不会影响这一组库。 根据Blockcerts社区的资料，虽然这项工作的基础已经完成，但更多的链条需要小的扩展和更详细的文档，正如以太坊已经计划的那样。

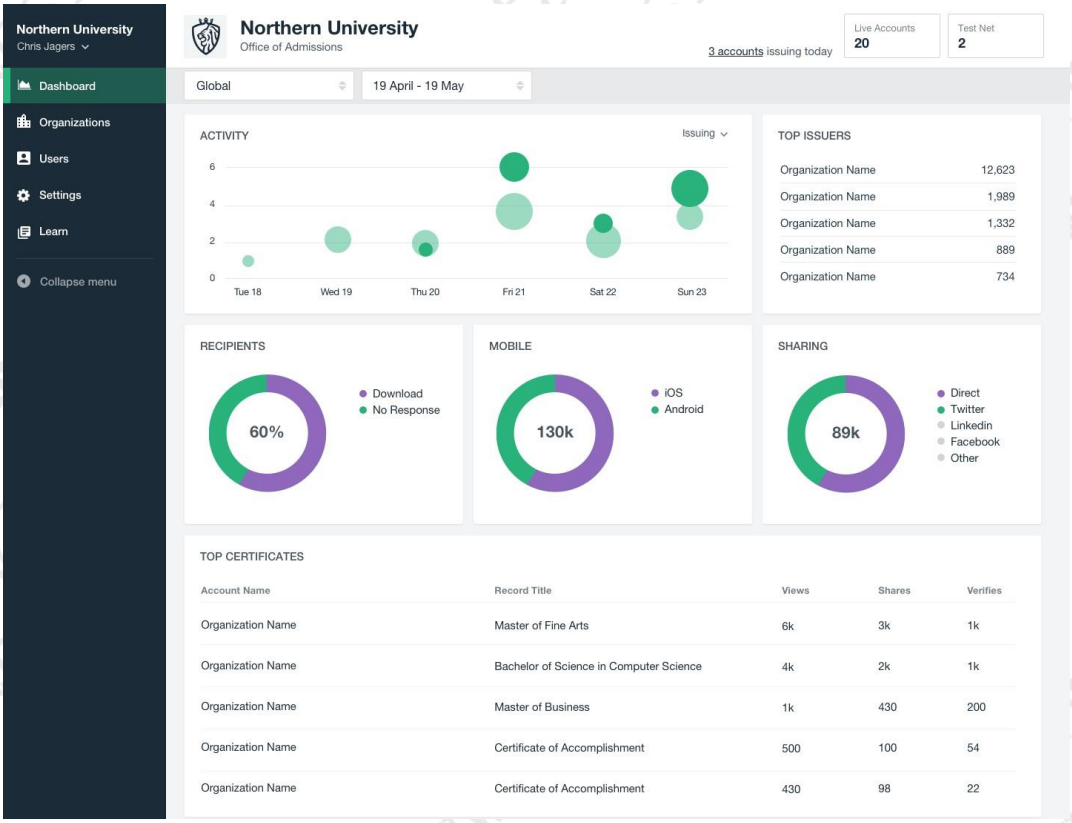
(27) 看到http://www.imsglobal.org/tags/open-badgeshttp://www.imsglobal.org/tags/open-badges

(28) 看到https://w3c.github.io/vc-data-modehttps://w3c.github.io/vc-data-model

(29) 看到https://w3c-dvcg.github.io/ld-signatureshttps://w3c-dvcg.github.io/ld-signatures

尼科西亚大学麻省理工学院和伯明翰大学[31]的研究人员正在使用Blockcerts开放式规范开发自己的系统。

图16：学习机分析仪表板示例



来源：学习机

7.2 证书和身份工作区中供应商的快照

在证书工作区中提供区块链相关产品的供应商正在呈指数增长。 在撰写本文时，有20多家公司在区块链（Mesropyan 2017）上建立客户平台。 它们通常具有相似的一组特征。

Jagers（2017）提出了一个模型，以四个不同的标准为基础来区分这些产品。 在这里转载这些内容作为区分供应商样本的出发点：

(30) 看到https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft- 文件/DID-SPEC-实施者-草案-01.pdf

(31) 见李（2017）和Blockcerts.ehcoo.com

存在证明解决方案使用区块链作为时间戳公证，以保证特定文档在特定时间点之后没有改变。 这些供应商通常使用标准的开源方法，因此区块链被用于验证，而没有任何供应商依赖。 但是，这个象限中的供应商不会将接收方的公钥编码到文档中，也不会将其传输给接收方 - 他们只是提供数据验证。 这意味着文件接收者不能证明未经修改的文件是发给他们的。 这些供应商都不应该与个人的身份要求混淆。

供应商作为公证解决方案还提供数据存在的证据，并将自己定位为颁发身份证件的产品，如学历证书。 但是，它们的格式始终依赖于供应商的访问，托管和验证 - 它们不会为单个收件人提供任何类型的所有权。 实际上，他们正在使用区块链来支持以供应商为中心的方法来验证和管理记录。

了解您的客户解决方案通常会提供一个移动应用程序，允许收件人证明其验证数据的所有权。 虽然这可以提高参与公司的强大网络的效率，但这些公司需要更有效的方式来验证客户数据，但这些数据仅对供应商控制的网络周边的接收者有用。 所以，虽然收件人的所有权已经确定，但对供应商的依赖是绝对的。 KYC解决方案对许多用例都是有希望的，但不应该将其与提供可在任何地方使用的可验证索赔的解决方案混为一谈。

数字自主权解决方案使个人能够接收收件人完全拥有的正式记录，而不依赖供应商查看，共享或验证这些记录。 这种独立性是通过三个组合来实现的：

- 以基于开放标准的格式发布记录

- 发出包含收件人公钥的记录

- 用开放源码容器（即移动应用程序）保存记录，让收件人控制自己的私钥，并继续运行，并超越任何特定的供应商。

图17：供应商独立性与收件人所有权的当前定位

来源：改编自Jagers（2017）

7.2.1 认证解决方案供应商

下列组织目前代表一组供应商[32]，其新出现的一套认证产品和服务可能适用于教育部门。

(32) 认证供应商开始定期出现。 最近的参赛者包括GrowBit（www.growingabit.iowww.growingabit.io）和INTEGRAL +，后者是由Kiron开放式高等教育协调并由德国联邦教育和研究部（BMBF），Kiron和吕贝克应用科学大学资助的一项新举措。 INTEGRAL +正在研究在Kiron和Fülbeck的数字学习环境中向学生提供更多自动化，经过验证和可扩展的发行人托管数字证书的机会。 该项目利用现有的举措，包括联合国联合国大学区块链倡议和区块链证书开放倡议的Blockcerts标准。 计划中的飞行员将测试德国大学和Kiron开放高等教育的几个实施可能性，考察两个主要情景：只有一个在线课程或MOOC达成的成就/学习成果，以及作为多个数字学习机会的组合获得的成就/学习成果。 合作伙伴也在这方面探索将区块链与开放徽章合并的机会。

7.2.1.1 学习机器证书部署在Blockcerts上

Blockcerts可以被供应商用来构建针对特定目标市场需求而配置的商业解决方案。 Learning Machine为组织开发了一套工具，用于发布，跟踪和验证基于区块链的记录 - 本质上是一个商业生态系统，由开源Blockcerts平台上的注册商CRM和一组API组成。 就商业模式而言，发行机构是Learning Machine的付费客户；收件人可以免费访问该服务，包括移动应用程序和钱包，验证者可以通过Web浏览器和移动应用程序安全地访问记录的即时和免费验证。

防篡改格式允许收件人证明所有权，并允许第三方即时验证，而不依赖于中央授权。 发行数字记录的目标客户包括政府，公司，教育机构，认证机构等。 该技术作为一种解决方案进行销售，不需要客户具有任何内部区块链技术技能和能力，无论内容类型如何。 当公司为区块链提供正式的官方记录时，特别是当组织为接收者提供第三方以后可能要验证的记录时，教育机构显然是主要的目标市场[33]。

Learning Machine声称Blockcerts基于标准的解决方案是防篡改的，因为这些记录是由发行者加密签署并在区块链上注册的数字文件。 每个记录包含一个收件人的公钥，因此可以证明记录的所有权，而不依赖于证书颁发机构。 用Blockcerts，a：

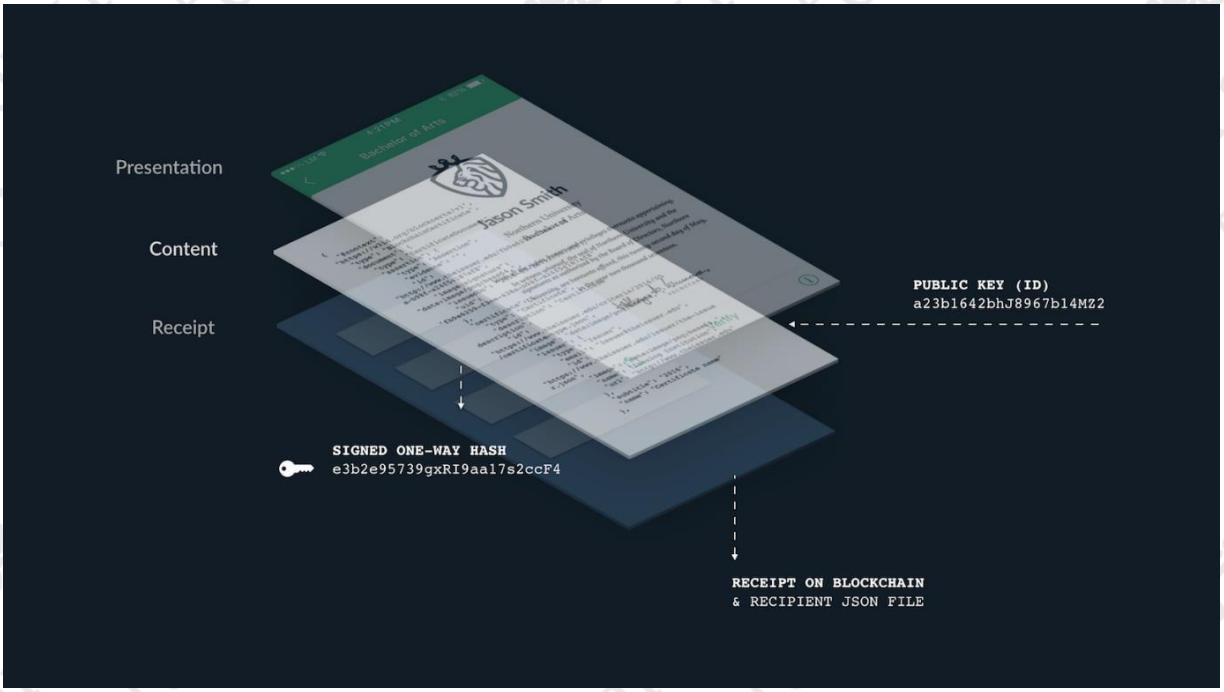
— 表示层可以被设计为模仿传统记录的外观；

— 内容层是包含所有数据和图像的代码；

— 收据层包含交易证明，其中包含内容的签名散列。

(33) 墨尔本大学成为亚太地区第一所使用学习机发行系统在区块链上颁发接受人证书的大学。 看到：https://www.newswire.com/news/university-of-melbourne-first-in-asia-pacific-to-issue-recipient-owned- https://www.newswire.com/news/university-of-melbourne-first-in-asia-pacific-to-issue-recipient-owned-19980513

图18：生成在区块链上公证的证书的多个层次



来源：学习机（2016）

组织使用工作空间来完成设计证书的整个过程，连接收件人并发布这些正式记录。 这些工作区允许用户：

— 导入/管理收件人列表；

— 轻松收集收件人的公钥；

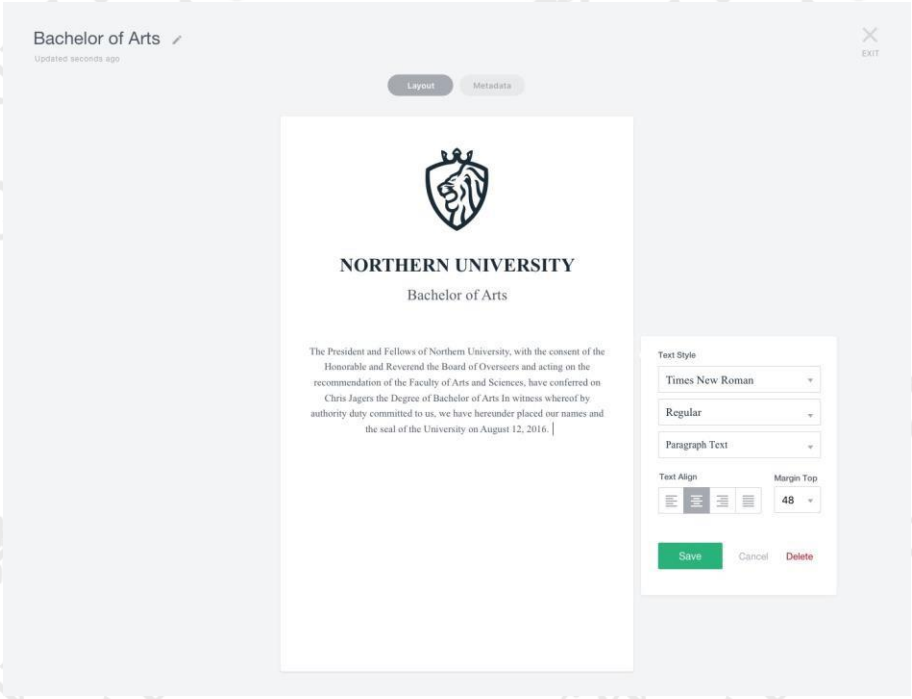
— 数字记录（内容，布局，元数据）的设计模板；

— 向整个队列发布记录；

— 跟踪记录在线使用情况的汇总分析；

— 查看显示发给个人的所有记录的配置文件。

图19：颁发工作空间中的证书编辑器示例



来源：学习机

7.2.1.2 索尼全球教育

自2016年以来，索尼一直在宣布已经开发了使用区块链技术的内部证书发行系统（Sony 2016，Russell 2017）。 2017年8月10日，索尼公司和索尼全球教育公司（SGE）宣布[34]开发专门将区块链技术应用于教育领域的系统。 新闻稿指出，这个可靠的系统通过使用“以公开和安全的方式互相利用教育成果和活动记录的技术”，集中管理多个教育机构的数据，并能够记录和参考教育数据和数字抄本“，该系统建立在IBM Blockchain基础上，由IBM Cloud提供，由Hyperledger Fabric 1.0提供支持，这是一个区块链框架，也是Linux基金会托管的Hyperledger项目之一，它包括1）一个验证功能并控制教育数据的使用权；2）面向教育机构处理这些权利的应用程序编程接口；2018年，索尼将开始部署自己的服务产品，从全球数学挑战赛开始，全球150,000名参与者世界。

7.2.1.3 Attores解决方案

Attores推出了一个名为Open Certificates[35]的产品，该产品将能够在Ethereum区块链上签发教育证书作为智能合约。 该产品目前正在测试；已经有与新加坡教育机构建立伙伴关系的公告。

(34) https://www.sonyged.com/2017/08/10/news/press-blockchain/https://www.sonyged.com/2017/08/10/news/press-blockchain/

(35) https://www.opencertificates.cohttps://www.opencertificates.co

7.2.1.4 *其他公司*

在区块链上提供证书的公司数量在不久的将来可能会增加。 Gradbase[36]和Stampery[37]正在开发专有解决方案，希望成为发布和即时验证资格的新的全球标准。

7.2.2 身份解决方案供应商

以下组织目前代表一组供应商，其新兴的身份解决方案产品和服务可能适用于教育部门。

7.2.2.1 *思域*

思域[38]将自己描述为存储在区块链中的安全身份平台。 该公司刚刚筹集了3300万美元的资金来开发和推出其产品。 使用Civic解决方案，用户可以将一些个人识别信息上传到手机上的应用程序，其散列存储在区块链中。 当任何组织（如大学招生办公室）需要用户的个人信息时，用户可以选择分享哪些信息。思域平台还支持认证，即组织可以向用户颁发证书（也链接到区块链），证明他们已经验证了所提供的数据。 使用他们的个人可识别数据和证明的散列以及他们电话上的生物识别标识，用户可以向需要信息的其他方识别自己，并信任评估者。 在我们大学的例子中，这意味着他们能够向图书馆，食堂，个别讲师和学生协会证明自己，而不需要这些机构存储甚至查看用户的个人身份信息。 此外，由于数据仅在用户的个人设备上存储和加密，而不在中央数据库中，因此不可能大规模地窃取数千用户的数据。

7.2.2.2 *UPORTUPORT*

Uport[39]是由ConsenSys开发并以Ethereum为基础的安全，易用的自主主权识别系统。 uPort技术由三个主要组件组成：智能合约，开发人员库和移动应用程序/基于Web的钱包。 移动应用程序保存用户的密钥。以太坊智能合约形成了身份的核心，并包含逻辑，使用户在移动设备丢失的情况下恢复其身份。 最后，开发人员库是第三方应用程序开发人员如何将对uPort的支持集成到他们的应用程序中。 uPort身份可以采取多种形式：个人，设备，实体或机构。 Uport的身份是自主的，这意味着他们是由创作者完全拥有和控制的，而不是依靠集中的第三方进行创作或验证。 uPort身份的核心功能是它可以数字签名和验证声明，操作或事务 - 涵盖了广泛的用例。 身份可以通过加密方式链接到脱链数据存储。 每个标识都能够存储归属数据blob的散列，无论是在IPFS，Azure，AWS，Dropbox等等，这是与该标识关联的所有数据安全存储的地方。 身份可以自己更新这个文件，例如添加个人资料照片或朋友，或者他们也可以授予其他人临时读取或写入特定文件的权限。 由于他们可以与区块链交互，因此uPort身份也可以控制数字承载资产，如加密货币或其他标记资产。

---

(36) 见https://gradba.se/en/

(37) 请参阅https://stampery.com

(38) 请参阅：https：//www.civic.com/www.civic.com

(39) 请参阅https：//www.uport.me/www.uport.me和Lundkvist等。 (2017)

7.3 存储经过验证的电子投资组合

以下组织目前代表一组供应商，其新兴的电子投资产品和服务套件可能适用于教育部门。

7.3.1懊恼

Indorse[40]正在使用区块链技术来启动一个经过验证的电子档案袋。 使用该系统，任何人都可以将任何索赔与一个如何验证索赔的链接一起上传。 然后将要求该平台的其他用户验证该声明 - 从而创建可信的数字组合。

从用户角度来看，系统架构最好通过一个例子来说明：

— Alice加入了Indorse网络。 在注册后，她会获得一个最低的Indorse Score（一个SCR令牌），使她能够向她的个人资料发出一个声明。

— 她首先创建她独特的个人资料身份，然后添加索赔。 她声称她毕业于马耳他大学。 她为大学的证书信息提供了一个链接到大学的验证页面。 她提交索赔，她的印记分数被锁定。 Indorse平台随机选择一些可以背书的其他成员，并且该申请进入妊娠期。

— 鲍勃是一个反悔的成员谁是选择背书索赔。 他收到一个通知，并看到Alice已经为她的证书放置了验证页面的链接。 他核实索赔是有效的，并支持索赔，锁定他的分数。

— 妊娠期以背书的一致结束。 爱丽丝的倦怠分数增加1，提出有效的索赔 - 如果她的索赔无法验证，她的分数降低1，索赔将保持未经验证。 她也有奖励的回报。 鲍勃也有自己的躁狂分数增加1，并得到一个沮丧的奖励。

— 根据平台在此期间所做的广告，用户的"差劲奖励"将获得现金价值

7.4 管理知识产权

以下组织目前代表一组供应商，其新兴的产品和服务套件专注于管理区块链上的知识产权，可能适用于教育部门。

7.4.1 绑定

绑定（以前称为BlockAI）[41]是区块链上的图像的版权注册服务。 当一个图像被创建时，它的作者可以将图像上传到服务中，并且该图像的哈希值以及上传的时间戳和作者的身份被注册在区块链中。 这为首次发布的时间创造了不可磨灭的，不可改变的证据，后来可以用来强化版权声明。

未来，Binded还将监控网络版权侵权行为，并通过版权局将服务保护的图像的版权注册。

(40) https://www.indorse.iohttps://www.indorse.io

(41) https://binded.comhttps://binded.com

7.4.2 总帐日记

Ledger[42]是一篇同行评议的学术期刊，发表有关加密货币和区块链技术以及与数学，计算机科学，工程学，法律和经济学相关的全部原创性研究文章。 它由匹兹堡大学的大学图书馆系统在线出版。

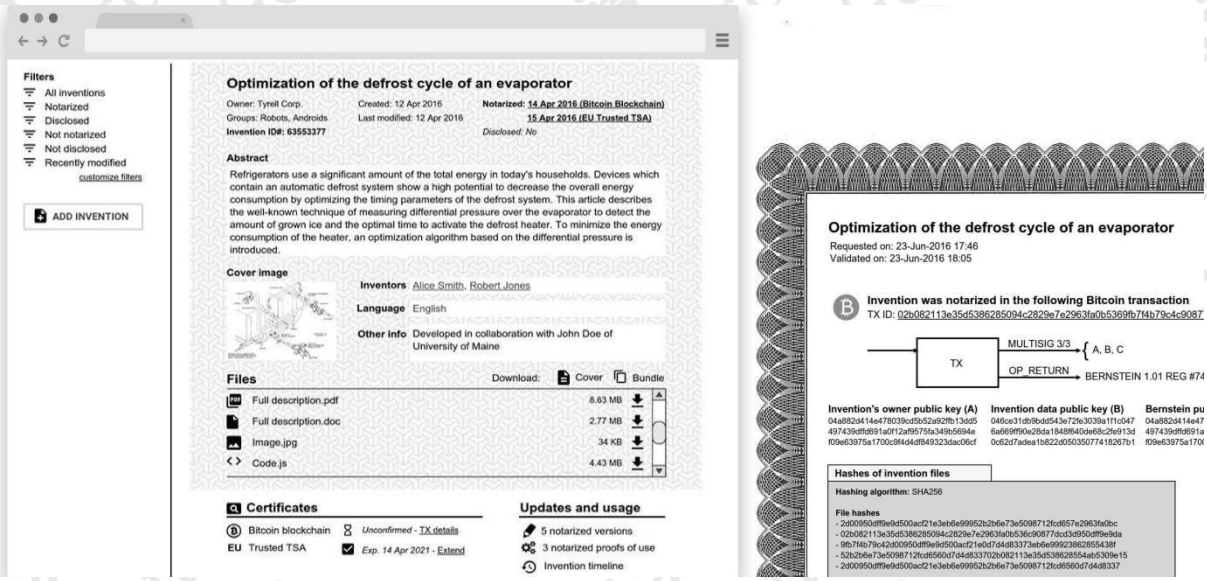
除了发布有关区块链的研究之外，该杂志还要求用户使用比特币私钥对其文档进行数字签名，并在时区印章中发布手稿。 此外，该杂志还为开放式期刊系统[43]创建了开源插件，允许运行该软件的任何人也对区块链上的期刊文章进行签名和时间戳。

7.4.3 伯恩斯坦技术

与已经描述的两种情况类似，伯恩斯坦技术公司在区块链上注册了文件的散列，从而提供存在，完整性和所有权的证据。 然而，伯恩斯坦专门做出知识产权的声明，然后可以用来保护版权或专利。 因此，它提供了一个平台，通过这个平台，专利声明可以上传到他们的平台上，在区块链上公证和加盖时间戳。传统的版权和专利实践为发明提供了保护，但也需要公开这样的发明。 通过将文档的散列存储在区块链中，本发明可以被可验证地发布，而不需要显示其内容。

除版权和专利之外，该系统还可用于保护商业秘密，实验笔记和其他内部知识产权。

图20：用Bernstein管理区块链中的知识产权



来源：伯恩斯坦（2017）

(42) http://ledgerjournal.orghttp://ledgerjournal.org

(43) 开放日志系统（https://pkp.sfu.ca/ojs）是用于管理和发布学术期刊的领先的开源软件包。 全球已有300多万篇学术论文使用该软件发布（资料来源：https：//pkp.sfu.ca/ojs/ojs-usage）。

简单地在区块链上加上时间戳记录或创建一个供应商所有的环境，让收件人可以存储他们的记录不一定会使个人受益：他们必须能够随身携带记录，独立于任何供应商或发行机构进行存储，并证明他们拥有他们。

关于数字自我主权优点的争论，特别是将Blockcerts标准的发展理论 – 或其他尚未确定的标准 – 作为一个开放标准的基础。

在撰写本报告时，要确定教育机构，政府乃至学习者（目标用户）将"开放性"，"厂商独立性"和"学习者授权"这一基本原则的价值，特别是那些与学习者相关的价值观将归于拥有自己的数字证书，而不是永远与（尽管可信的）机构或供应商锁定在一起。 尽管原则上这些论点是有力的论据，但是要确定这些论点是否对目标用户更具吸引力，比如微软，IBM和索尼等全球品牌开发的专有解决方案还是一些尚未公开的混合解决方案还为时过早。

8 区块链技术教育的案例研究

自主权意味着一旦证书在区块链上公证，并且用户的证书在区块链上公证，并且用户具有私钥，它们自动成为他们自己的身份和证书的管理者。 用户现在可以将第三方发布的文档转换成其他有限的认证工具，然后将其转化为更广泛的身份认证。 考虑一下Uport和其他人在构建可驻留在云端的数据存储上所做的工作，但也可以用来作为领先标识符（包括未来的雇主和认证机构）的证据，证明这些证书首先由个人自己控制。 签署的分类账和签字的记录成为更广泛的认同感。

（凯西，MJ 2017，采访）

本节重点介绍了区块链部署在教育背景下的四个用例研究。

8.1 英国开放大学

知识媒体研究所（KMI）董事John Domingue教授访谈

开放大学（OU）的KMI正在区块链上进行多项研究。 这项研究的兴趣主要由对下一代网络，媒体，增强现实，智慧城市和分析的兴趣所推动：OU是英国Learning Analytics的领导者。

在区块链研究和认证的背景下，KMI特别有兴趣通过区块链作为可靠的分类账，来提高网上徽章，认证和声誉的标准。 根据Domingue教授的说法，在区块链项目中嵌入开放式徽章并进行微观认证[44]和电子投资组合研究是一种自然的进展。 KMI正在利用以太坊认证的潜力将徽章变成智能合约，并开发了一个在区块链上组装和发行微型凭证的原型。 拥有超过17万名学生的OU，拥有自己的MOOC平台（FutureLearn）和核心的开放学习平台（每年有超过5M的访问者和8K小时的课程作业），为KMI提供了所有OU课程的证书和公证在区块链上。

KMI的区块链策略是整体性的，研究人员鼓励研究人员探索技术的全部潜力，而不是一个特定的方面（如密码学）。 多明格教授把这与电影的早期等同起来："因为人们只是对拍摄戏剧感兴趣，所以花了很长时间才把电影变成电影。

协作网络

多明格教授将KMI内部在区块链上的活动描述为"数据实验"，而外部活动主要由合作伙伴的利益驱动。KMI正在与教育数字服务机构JISC[45]合作，创建一个区块链，可用于所有英国高等教育和高等教育资格。目标是促进一个可以在高等教育领域开展区块链项目的网络。 例如，KMI，Jisc和南安普敦大学反过来在一个国际版本的区块链中作为一个节点合作，其中包括德克萨斯大学，

(44) 另请参阅Learningisearning2026.org

(45) 见Jisc.co.uk

根特大学和英国电信。 其他目前的KMI计划包括：与初创公司Gradbase[46]和APPII[47]就链接区块链认证和简历的项目进行合作； 与德克萨斯大学奥斯汀分校合作开设微型课程全球认证徽章网络； 并与英国电信合作，为他们新的汤米花研究所提供标识；并与行业合作进行公司内部培训。

Domingue教授解释说："虽然我们继续按照以太坊标准进行开发，但我们在我们的区块链上还有第三方组织的软件，例如英国电信，他们正在防火墙之后部署应用程序.KMI有权探索合作伙伴关系，对于高等教育的现在和未来的影响，在这种情况下，OU是高等教育新途径的实验性试验平台。在区块链研究的背景下，采购是OU的应用研究的一个持续的领域：供应管道和服务通过区块链的智能化，战略性使用，高等教育所需要的渲染可能会大大改善。"

研究和教学

根据Domingue教授的说法，KMI不一定希望生产或开发可为OU创造增量收入的区块链产品：KMI仍然是研究中心，而不是OU的产品供应链[48]。 对于OU进行的研究，外部影响是至关重要的：就KMI管理的区块链项目而言，非学术影响也被测量。

根据Domingue教授的说法，区块链研究并不一定专注于最终用户。 也不能被学生或第三方重新使用。与区块链研究相比，IBM的重点在于大型企业系统，IBM正在开发中间层。 同样，KMI不是使用加密研究人员的团队，而是对应用层更感兴趣。 虽然原则上人们可以控制自己的数据和私钥的钱包，但是在这个时候，应用程序往往过于复杂，普通用户在没有技术中介的情况下采用[49]。

OU正在重新设计学生委员会（以及学生获得学分的方式）以及大学采购。 有权访问具有语义和网络规模数据背景的研究人员，这意味着OU可以在语义上对区块链进行索引； 它也使网站更容易在全球网站上发现。 用户培训与区块链一起成为网络界面的一部分。 在这种情况下，Blockhain可以被认为是Web界面的又一个在线开发 - 类似于移动界面的开发。 用户将获得更多的数据控制 - 比如通过教育钱包。 因此，用户培训将在概念层面，服务器层面，中层管理人员等方面得到发展。OU计划在4月份开设在线教学和区块链的在线和远程学习课程。

没有计划开发一个封闭的专有区块链。 区块链的方法与Web是同义的，具有自己的协议和工具。 有一个根本的，意识形态的原则是关键的：你通过介绍让用户更容易

(46) 看到https://gradba.se/enhttps://gradba.se/en

(47) 看到http://www.appii.iohttp://www.appii.io

(48) OU本身依靠来自各种学术渠道的资助，例如编码研究所和各个欧盟项目的OU大概2000万美元。

(49) 这与Blockcerts场景类似，学习机器作为中介机构来组织发行人和接收人的界面。

中间商（或者说，已经关闭了区块链的版本），你会发现你违反了基本的，分权化的区块链原则。

区块链作为教育模式的破坏者

在他的采访中（Domingue，2017），包括本报告的作者在内，Domingue教授对区块链技术应用于教育的前景充满热情，将技术主要作为学习者赋权的来源，作为重新设计的机会传统的教育机构。 具体而言，区块链将给学习者所有权资格和相关的课程作业和反馈，而不是控制归属于教育机构或雇主。

"我们感兴趣的是任何技术，尤其是在英国的情况下，能够为促进高等教育变得更加物有所值，现在学习的集中模式已经不再可持续 - 实际上，区块链技术可以实现全面的非中介化和分解高等教育的发展今天，在传统教学大学之外的学习越来越多：它发生在网络平台上，思想相同的社区内，或者为现实世界中的项目和计划做出贡献。这个新的分布式学习现实的结果是安全可靠地核对的答案。" 学生可以在一个安全的地方获得对所有教育数据，认证和工作组合的控制权和所有权，任何需要验证他们的人都可以访问，并在他们的整个一生中都可以访问。 在学生，教师和课程作者之间存在直接关系的情况下，新的交易模式将会出现。 例如，当学生观看学习视频时，可以自动向视频作者进行小额支付。

多明格教授认为，从中期来看，区块链将为教育机构的商业模式带来重大挑战和机遇。 区块链的战略应用可能会大大降低管理成本，提高透明度并减少欺诈行为 - 就后者而言，这在交易中的利益相关者相互信任的情况下很有意义。 初看起来，区块链技术的优势更容易被拥有重要品牌资产的高等教育机构所接受。 在英国，大多数大学和技术学院都推出了收费课程，机构也将区块链视为降低招聘流程成本的一种手段 - 例如通过智能搜索简历。

反过来说，OU正在调查"一所大学"[50]，通过部署新工具，智能合约和分布式自治的网络化组织，高等教育教学业务被打乱并重新设想。 研究兴趣侧重于可以改善学生获得高等教育的机会，提高学历的透明度。 在不久的将来，由于各种原因，学生们不会想要开始一个三到四年的大学课程 - 从金融到机会成本。 学位将被解构为"点菜"课程。 学生还希望在欧盟范围内使用即插即用模式 - 在不同地点和不同环境下学习组件，并通过面对面的学费和其他模式通过混合或完全在线的方式进行学习。

在这个新兴的模式中，微观认证将通过区块链进行。 还可以通过MOOC的认证来促进技能的可转移性 - 再次，未来似乎表明通过不同的媒体和不同的地点进行面对面的混合和匹配的教学和学习。 在那些日益成为替代品的领域也有着重大的机遇（或者说，

(50) 在采访中也被称为"Uber大学"

反对）主流的学术方法，如职业教育与培训，企业培训和金融专业机构颁发的资格。

区块链可以促进并允许在公民的终身学习之旅中进行非正式和非正式学习。 这对于高级和高级学徒等资格条件尤其适用，在这些条件下，由许多不同的组织提供方案的组成部分。 例如，在线教育论坛上的内容将存储在区块链中，便于回答问题。 例如，可以存储关于个别学生的信息也可以提供给学生工作的外部考官，从而更好地理解研究。

多明格教授认为，大学内部的行政管理和面向学生的流程已经成熟，可以实现激进的变革，因为目前在校内角色非中介化的基本需求，并为终端用户 - 学生增加了很少的价值。 这些过程的某些组成部分（如认证）需要放在学生的监护之下，而不仅仅是机构。

数据保护

迄今为止，KMI报告说，它没有遇到任何数据保护和区块链问题。 在作为主要合作伙伴的研究项目中，只有公共数据被使用，而这些数据又被放置在以太坊区块链上。 在与初创企业合作时，由于其中一些解决方案是封闭的，所以情况有所不同：在这种情况下，没有任何数据或分析被公开。 KMI通过端到端加密来保护隐私，尽管欧盟关于被遗忘权的立法仍然具有挑战性。 OU目前仅使用学生数据集来尝试为付费学生提高性价比。

Domingue教授目前针对公众对数据保护问题的看法确定了两个有形的风险：a）将不可预见的私人数据发布到公共区块链上；和b）由一些学生因为某种原因或其他目的（尽管是标准的）数据与区块链技术的可供性一起使用以产生新的分析而触发的负面宣传。 在不久的将来，大学将不得不更新和发展道德政策，因为他们开始了解区块链的机会和局限性。

区块链分析和欧盟

多明格教授认为，学习分析将成为教育区块链的重要代表之一，对机构和学生都有积极影响：

"想象一下，每个学习活动都在区块链上注册，包括非正式学习 - 以及非正式的反馈。 所有的考试分数将被映射到整个欧洲的学习环境。 欧洲范围的分析可以从头开始。 欧洲最好的讲师可以很容易地识别出来。 学习将变得更加互动 - 并以更实际的矩阵为基础的声誉"。

多明格教授建议，欧盟应该考虑支持欧盟在教育实验领域的发展。 为同一区块链上更具创新性的项目提供资金 - 从大学联盟和其他研究人员管理的飞行员开始。 它应该为不同的利益相关者组织一个教育计划和一系列的信息会议。 例如，大学应该使用区块链与全国各地的其他大学以及不同的欧盟国家联系 - 促进合作。 与此同时，大学，职业教育与培训机构和高等教育机构也应该关注注册商的职能，以及如何通过战略性使用欧洲区块链来大幅提升这一功能。 欧洲区块链上的飞行员的成功可能会受到阻碍，鼓励欧盟成员国之间的知识转移。

8.2 尼科西亚大学

采访Soulla Louca教授和George Giaglis教授

尼科西亚大学（UNIC）在致力于最大限度发挥区块链教育潜力[51]方面已经取得了多项“世界第一”。 新闻中心称这是第一所大学：

— 接受比特币在大学任何学位课程的学费（2013年10月）；

— 讲授一个关于加密货币的大学课程，作为一个名为"数字货币简介"的MOOC（2014年1月）交付；

— 提供认可的学位课程 – 数字货币科学硕士 – 以英语授课（2014年3月，第一批学生于2016年6月毕业）；

— 使用自己的内部软件平台（2014年9月）发行学术证书到比特币区块链上。

与ASU GSV首脑会议首席执行官Antonis Polemitis进行的讨论，以及随后对区块链倡议协调员Soulla Louca教授和George Giaglis教授的访谈表明，联合国大学认为区块链技术是其战略的基石[52]，与其他高等教育机构的区别。 尽管联合国新闻中心推出的数字货币免费MOOC并不是唯一的[53]，但它被定位为数字货币硕士课程的第一门课程。 MSc的组成部分又被重新包装成区块链专业认证计划，转化为CPD和ECTS。

2017年9月，MOOC第八版将推出。 迄今为止，慕课已吸引了来自80个不同国家的学生，并表现出良好的完成率。 课程内容由新闻中心主办，并由于大学在全球教学界的网络而不断发展。 区块链研究中心定位为新兴技术的世界级中心，将整合，扩大范围，加强在这一演变领域已经开展的跨学科研究。

比特币便于支付学费，招生和访问

当新闻中心以数字货币引入硕士学位时，首先要做的就是让学生用比特币支付。 Louca教授和Giaglis教授都认为这个早期的决定对大学和学生有很大的好处：

— 允许学生加入在线学习的数字货币计划，用数字货币支付学费是完全符合逻辑的。 这立即表明了新闻中心致力于接受新技术及其可供性。

— 它使硕士课程能够吸引真正的多国学员，其中许多来自发展中国家。 外国学生通常与伪汇款案件有关。 中央电视台"按时付费"的学费制度意味着，例如非洲学生正在为此付费

(51) 请参阅DigitalCurrency.unic.ac.cy

(52) 联合国大学在学术界作为区块链创新者的角色也受到区块链行业出版物（如CoinDesk（2016）和Merkle（2017））的认可。 请参阅https：//www.coindesk.com/the-global-/www.coindesk.com/the-global- 高校环抱，cryptocurrency

(53) 请参阅https：//www.coursera.org/learn/cryptocurrency/www.coursera.org/learn/cryptocurrency

按月收费，避免与传统银行结算相关的汇款费用，可能达到学费的20%[54]。

— 重建颁发证书和验证证书系统不一定会解决学生日常问题，如现金流量或管理成本。 能够在没有中间支付提供商的情况下开拓支付系统，可以增加交易双方的价值。 联合国新闻中心鼓励目标学生通过比特币支付自己的支付网关，通过提供比净费用低5%的折扣。

— 帮助某人付费并从注册服务机构的角度出发，也增加了接受高等教育的机会：难民获得了该项目的奖学金，这又导致他获得了居留资格。

使用区块链发布和验证证书

区块链认证是缩小传统大学研究实践与实用解决方案市场需求之间差距的一种方式。 联合国中心委托自己的开发团队使用Blockcerts开源标准，使用Blockchain发行和认证证书 - 与MIT Media Lab的关系可以追溯到2015年。

许多大学所面临的挑战不仅仅是招生办公室对于"国际学生"付款造成的欺诈行为保持警惕，而且还有高校教育机构长期存在的篡改学生人数的问题。 在某些国家，人们准备从一些中央当局贿赂半真实的真实印章。 目前没有注册商SaaS可以随时验证身份。

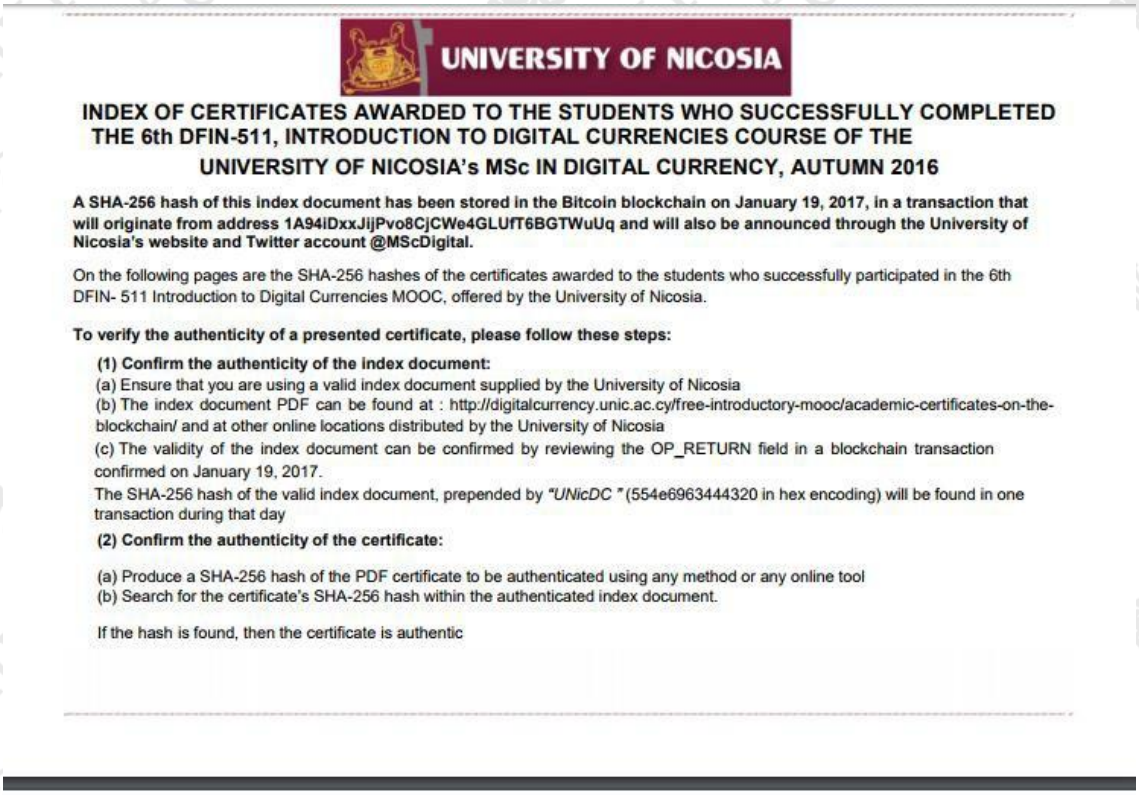
新闻中心描述了使用链接中的区块链发布和验证证书的过程[55]。 所有MOOC证书正在使用公共区块链发布；于二零一七年六月开始测试系统，于二零一七年十月前使用区块链发布所有文凭，并提供软件工具，让人们可透过使用语言及其他应用程式确认证书的真实性。 联合国新闻中心仍然是Blockcerts联盟的一部分，致力于开放标准，但现在正在使用各种工具来改进面向用户的界面层。

下面的图25是证书索引的图示：

(54) 由于付款的模块化，对塞浦路斯的交易支付费用也很高。

(55) 请参阅https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/

图21：尼科西亚大学在区块链上公证的证书索引（摘录）



UNIVERSITY OF NICOSIA

INDEX OF CERTIFICATES AWARDED TO THE STUDENTS WHO SUCCESSFULLY COMPLETED THE 6th DFIN-511, INTRODUCTION TO DIGITAL CURRENCIES COURSE OF THE UNIVERSITY OF NICOSIA's MSc IN DIGITAL CURRENCY, AUTUMN 2016

A SHA-256 hash of this index document has been stored in the Bitcoin blockchain on January 19, 2017, in a transaction that will originate from address 1A94iDxxJijPvo8CjCWe4GLUfT6BGTWuUq and will also be announced through the University of Nicosia's website and Twitter account @MScDigital.

On the following pages are the SHA-256 hashes of the certificates awarded to the students who successfully participated in the 6th DFIN- 511 Introduction to Digital Currencies MOOC, offered by the University of Nicosia.

To verify the authenticity of a presented certificate, please follow these steps:

(1) Confirm the authenticity of the index document:

(a) Ensure that you are using a valid index document supplied by the University of Nicosia

(b) The index document PDF can be found at : http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/ and at other online locations distributed by the University of Nicosia

(c) The validity of the index document can be confirmed by reviewing the OP_RETURN field in a blockchain transaction confirmed on January 19, 2017.

The SHA-256 hash of the valid index document, prepended by *"UNicDC "* (554e6963444320 in hex encoding) will be found in one transaction during that day

(2) Confirm the authenticity of the certificate:

(a) Produce a SHA-256 hash of the PDF certificate to be authenticated using any method or any online tool

(b) Search for the certificate's SHA-256 hash within the authenticated index document.

If the hash is found, then the certificate is authentic

CERTIFICATES OF ACCOMPLISHMENT

Certificates of Accomplishment were awarded to the students who attempted and completed at least 75% of all quizzes and achieved a grade of 60% or above on the final exam of the DFIN-511 Introduction to Digital Currencies MOOC

SHA 256 hashes of certificates awarded:

43392791dd7c5247733f9be8f91e419a3d8bed21c445e353e49d64925b027699
296dd861832844e44b36e7b163e0a2c67a648f031454d418109f05fcae803ebf
df8ed817a150e14ad70b6f200c55e9bbd1bae5199a2af9b82a7bdb1363bb2ed9
9b9d8ca500d8d0fe64f58dca9ba7fe936921c26587e638ce583d7e04264f2b66
f88d748dab2a9e87c26b213867e80d747b0c128ac25e7b6ee155346a37db9513
955c113a44a9c4cb35d6412dac8f249038c49384e6e605027d9a3d00155ffcf9
dbc6fc13ff568e9445a7a5682d5e033472b57e1773595a1fbce50ffa970f4edf
bfb19bef770a05c9706106103d8bf492df1f862b18ef75421e524ec63fcf2539
3be215f0bd5682e6f53e301b6620bb8708184c5484e19533d71f535d85b300fd
2fac30937af41fefc066981ddf68937c359c2f83900df9de638d6994eddebd3a
bc996119794f652347ea35bb287600ef1932bf30654354b2bd81fe9d63d6ec29
15da1de9b16c39280649130356e4b1e452957590e8d131d96565c8ae51046bc7

对认证标准的需求：可扩展性和可移植性

使用区块链颁发证书所面临的挑战并不是技术 – 这可能是方程中最易处理的部分。 如果我们想看看技术的广泛应用，例如将证书验证集成到人力资源软件中，或者使用这种技术来促进大学间信用的无缝识别和转移，那么这个问题还有待于解决，元数据。

Giaglis教授指出："如果你想优化你在区块链上做的事情，并且按比例进行，就会遇到困难。 开发出版PDF证书的技术是一回事； 确实有技术支持完整的成绩单和文凭补充是很复杂的。 不过，这是可行的，现在可以做到。 真正的挑战是如何在高等教育机构中扩展这种技术

它与内部系统整合 – 现在不依赖于技术，而是依靠大学交换信息的倾向；以及雇主和其他有关方面证明证书的真实性，而不必首先与大学联系。 孟加拉国大学的学生应该能够证明证书是真实可验证的，而不必首先联系颁发证书的国家。"

Polemitis先生指出："如果世界各地的高中有一些共同的认证标准，这将是非常有价值的。 区块链上不能有40个标准。 这对高等教育有什么用处？这是由中等教育提供的？ 我们怎样才能让每个人都订阅相同的标准呢？ 如果像我们这样的一个机构这样做 – 这是有限的；如果一个民族国家或一个国家的所有高等教育机构和学校加入 – 这将是非常有用的"。

Giaglis教授认为，Blockcerts目前没有足够的吸引力，使其成为区块链教育事实上的"标准" – 虽然联合国新闻中心继续支持它，并在开放标准上开发应用程序。 "在这个时候，麻省理工学院可能会有不同的优先考虑，因为社区网站的早期动力似乎已经放缓。 独立于Blockcerts的开放精神，开发封闭式应用程序并不符合新闻中心的利益。 但是我们确实需要按照步调。 我们的道路迟早有希望汇合，将有共享的经验，使新闻中心能够重新进入Blockcerts，成为区块链教育事实上的开放标准"。

将首席执行官视为区块链的支持者，意味着联合国新闻中心不可避免地会成为技术提供者的倡导者。 新闻中心认为，其对于区块链战略性使用的承诺很快就会反映在其他机构和教育界以外的网络效应中，影响到工业 –"真正的市场"：有人怀疑高等教育本身可以领导电子商务在短期内使区块链技术持续发展。

其结果是，如果互补行业的人能够互相配合，教育将会带来不可避免的好处。 新闻中心指出，需要一个标准，例如，可以验证区块链上的评论。 这样的协议将导致网络动态。 希望是一个事实上的开放标准将出现 – 尽管企业主要去封闭，专有的解决方案的努力。 当人们看到实际技术的实际效益时，一套共同认可的元数据将不可避免地被交换。

8.3 MITMIT

访问注册服务商办公室注册服务处高级副院长Mary Callahan和麻省理工学院高级助理注册处处长Brian Canavan

2015年，麻省理工学院媒体实验室开始使用Blockcerts向其更广泛的社区中的人员颁发数字证书，例如Director的研究员（Schmidt，2015；MIT Media Lab，2016）。 在这个过程中，麻省理工学院已经成为一个倡导者，他们可以更多地控制他们所获得的证书，而不必依赖大学和雇主等第三方中介机构来存储，验证和验证证书
– 往往需要额外的费用。 区块链技术和强大的加密技术一起被用来开发Blockcerts数字证书和信誉开放平台。 2017年6月，麻省理工学院使用了Blockcerts开发的商业解决方案学习机（LM）证书，为MIT媒体实验室（媒体艺术与科学）和斯隆商学院的两名学生颁发文凭。 这是这种证书的第一次发行，使用LM技术和第一个接收者拥有的文凭的例子。

Callahan女士和Canavan先生确定了两名飞行员的下列目标：

— 为官方的麻省理工学院成绩单提供替代方案，其中已经包括电子转录本[56]；

— 从学生的经历中直接学习，作为在公开区块链上公证的数字证书的接受者；

— 收集可能优化管理控制台开发的信息；

— 安全的信息，可以确定在公开区块链上时间戳，耐用，透明和公证的未来证书格式；

— 在夏季之前从收件人那里收集信息，然后在校园内扩展实施；

— 在2017年第四季度培养更大的领导者的信心和知识，并在2018年在麻省理工学院进行更广泛的部署。

注册服务机构授权学生

两名飞行员的选拔与这样一个事实有很大关系，即大多数学生队列是国际性的，高度机动的，因此对认证和成绩单感兴趣作为在不同地理环境下赋权的手段。 麻省理工学院对这些学生的需求特别敏感，以及在发放纸质证书，文凭和成绩单时收到的反馈。 麻省理工学院致力于授权学生拥有自己的学历，但并不认为区块链技术的实验是规范性的：在可预见的未来，学生将继续获得纸质文凭。

在观察学生如何与新技术互动的过程中，飞行员是非常宝贵的 – 学生是飞行员的关键路线。 一旦他们下载和使用应用程序，学生被引导到一个控制台，鼓励他们提供关于他们的用户体验的反馈。 麻省理工正在使用LM数据分析来达到此目的，监控学生如何与技术接口进行互动，并根据飞行员的预先确定的参数来衡量成功。 注册服务机构认为，现在和未来学习者将从数字空间中获得什么，将学到很多东西。数据和定性数据都将被收集，包括学生在下载完毕后用证书做什么的数据。

麻省理工学院纯粹从服务角度来看这些飞行员。 目标是让学生掌握自己的一些记录，让他们成为自己的管理者，提高全球范围内和学术界以外对证书所有权重要性的认识。

卡拉汉女士注意到：“从他们自己的文凭开始，学生会意识到他们可以在没有大学作为中介的情况下运作。 没有中介的意思，作为注册商，我不参与交易。 需要相信该文凭是真正的，由MIT发行，但现在也在区块链上。 现在，这使我很有信心，证书是受保护的，不会有欺骗的风险。 学生可以控制自己的记录 – 这对于制作纸质版本来说当然是一种不同的动态。 我们有这样一个全球性的学生群体，这个文凭将永远交付给高等教育。 这是一个综合的东西在这个试点汇集在一起，它可以成为一个真正的变革的方式为高等教育。 无论发生什么，我们都会学到很多 – 我们将决定我们的贡献是否真的满足了高等教育的需求。”

Canavan先生重申，试金石是学习者。 “作为注册商，我们正在弄脏我们的手。 我们将获得将循环改进管理的数据。 它是

(56) http://web.mit.edu/registrar/records/transcripts/official.htmlhttp://web.mit.edu/registrar/records/transcripts/official.html

当然不是为MIT节约成本的一种方法。 我们的目标是增强学习者的能力，为学生的利益转化我们的努力。
"

对现在和未来的其他考虑

麻省理工学院决定使用学习机器证书来颁发数字文凭，而不是根据Blockcerts建立内部应用程序，这是基于LM技术为飞行员准备的状态和上市速度。 由于他们与Blockcerts的合作，LM也被认为是MIT值得信赖的合作伙伴。 作为开源的倡导者，使用LM证书颁发毕业证书保留了麻省理工学院接管未来发展的能力，因为证书建立在Blockcerts上，这意味着代码是完全可访问的。 每个文凭都有一个徽章链接到blockcerts.org，所以任何人都可以检查发生了什么，它是如何工作的，区块链上是什么 - 没有"黑匣子"。

卡拉汉女士说，在这个时候，关于证书标准或机构信用转移等更为复杂的问题没有太多的思考， 飞行员是否会导致研究和学术出版物; 区块链记录如何与HR系统连接; 或者与其他大学的合作网络如何演变 - 成为信誉良好的大学之间的私人区块链。

"我们不想co，，但我们还不知道（关于这些问题）。 麻省理工学院的教师有很大的兴趣来证明一定程度的知识，特别是看看还没有获得学位或证书的学术课程和研究。 也许区块链技术可以帮助我们找到一种认证这种学习的方法。 我们也可以考虑将我们对区块链的贡献标准化。 但我们还没有呢"。

飞行员已经被开发出来，可以迅速扩大到麻省理工学院的其他学院，并且可以处理更多的交易。 从注册服务机构获得的经验教训可能会为高等教育的同事服务，包括那些已经表示有兴趣开发自己的应用程序的人。 人们已经意识到，像麻省理工学院这样一个高调的环境中的飞行员将不可避免地产生超出麻省理工学院原生系统和程序的影响。 下一次颁发的文凭计划将于2017年9月完成，届时将制定更大，更强大的飞行员计划。 在这个阶段，注册服务机构也将从学习的角度考虑那些希望采取更加联合的方法的教师的意见。 到目前为止，注册商是由MIT内部技术专家指导的，他们已经将区块链确定为符合具有显着品牌价值的品牌的顶级大学的要求的最高安全性技术：挖掘风险最小。

Canavan先生证实，麻省理工学院注册处的办公室一直在与Learning Machine合作，以改进产品的粗糙边缘，因为麻省理工学院是第一个使用它。 已经交换了许多好的想法以用于未来的改进。 "目前，当我们在比特币区块链上颁发文凭证书时，可能需要长达30分钟才能处理数据 - 但考虑到麻省理工学院和将来需要成绩单的学习者节省时间，这是合理的。 Learning Machine也吸取了教训，所以我们预计在不久的将来用户界面会有所改进。 一个小例子是当我们有一个收件人列表，我们曾经主持这些列表。 我们的期望是，这些数据最终将以数字方式进行交换，而且几乎没有人为的信息 - 现在仍然需要人为干预。 如果我们要开始解决学生的全部问题，这一点尤其重要。

麻省理工学院使用第三方抄本供应商发表抄本。 这样的供应商很可能也会监控与区块链相关的发展：未来在行业中看到垂直合作关系并不令人感到意外。 麻省理工学院注册处的

办公室愿意与其他人分享未来的区块链体验，考虑做可能有益于最终用户的飞行员[57]。

8.4 马耳他教育机构

虽然许多政府表示有兴趣在区块链技术作为其电子政务工作的一部分，很少有人承诺实际的技术推出[58]。

马耳他共和国自2016年以来一直在考虑在区块链上开展一个民族国家的试点项目。马耳他在区块链领域积极主动的愿望并不局限于教育，而是成为"区块链岛"，与其他国家相似小岛屿国家，如毛里求斯（参见斯坦利，2017年）：马耳他拥有先进技术的记录，包括电信和网络游戏，在欧盟赢得"岛屿实验室"（ASU GSV峰会，2017年）的声誉用于测试和快速部署新技术。 没有一个独特的因素可以区分马耳他与寻求类似定位的其他司法管辖区，而不是由多个因素组成：战略位置，规模，地形，社会多样化，语言以及在欧盟内部的主动作用 – 也许最重要的是，决策者和政治阶层。

2017年1月，教育与就业部（MEDE）与Learning Machine Group（LM）签署谅解备忘录。 谅解备忘录正值马耳他欧盟理事会主席[59]2017年1月19日（TF325）至20日之间举行的会议结束。 谅解备忘录标志着双方有意开发和实施马耳他LM民族国家技术平台的试点，该平台基于LMG和MIT媒体实验室开发的Blockcerts开放标准。

MEDE认为区块链技术的战略部署标志着政府的承诺，即为学习者和工作人员提供最大的自主学习成绩的归属和便携性。 这个试点的目标是自我主权 – 根据区块链的可供性，授权马耳他公民拥有自己的证书，充分发挥21世纪移动，国际和自我发展的劳动力的技术成员的作用（作为终身学习者）。 第二个目标是继续采取持续的举措，将从马耳他机构获得的证书与欧盟框架国际化和交叉参考[60]。

---

57 麻省理工学院描述他们与区块链飞行员的经验：见http://news.mit.edu/2017/mit-debuts- http://news.mit.edu/2017/mit-debuts- 安全数字文凭 – 使用 – 比特币 – blockchain技术-1017

(58) 格鲁吉亚共和国是这种趋势的例外。 2017年2月，他们与Blockchain公司Bitfury签署了在区块链上登记房地产交易的谅解备忘录。 佐治亚州使用私人和公共区块链的组合作为其数字房地产倡议的一部分。 它记录了私人政府区块链上的交易细节，同时也将这些细节加密成公共存储在比特币区块链中的"哈希"。 这样一来，任何人都可以在没有看到房地产交易本身的细节的情况下验证房地产权证的真实性。 在格鲁吉亚实施的房地产购买用案中，保持私人交易的细节是有道理的。

(59) 请参阅："数字教育的国家：从事互联，融合和开放式学习"的链接 https://education.gov.mt/en/digitaleducation/Documents/conference_magazine.pdfhttps://education.gov.mt/en/digitaleducation/Documents/conference_magazine.pdf以及随后的数字教育宣言：https://education.gov.mt/en/digitaleducation/Documents/Malta%20EU%20Presidency%20Digital%20Educhttps://education.gov.mt/en/digitaleducation/Documents/Malta%20EU%20Presidency%20Digital%20Educ 通货膨胀%20Manifesto.pdf

(60) 马耳他自1999年以来一直是博洛尼亚进程/高等教育领域的正式成员。马耳他资格框架（马耳他资格框架）有助于使马耳他资格认证制度更易于理解和审查，在国家和国际层面更加透明。 MQF也是一个参考工具，帮助描述和比较国家和外国资格，以促进各类教育资质的质量，透明度和流动性：主要参考欧洲资格框架（EQF）以及其他非欧洲资格框架。

MEDE特别选择了LM解决方案，因为它是建立在Blockcerts基础之上的，这是一个符合OBI标准的开源项目，为学习者和工人拥有的正式记录提供了一个共同的途径。 在民族国家试点部署的LM技术为政策制定者提供先进的分析。 该解决方案专为学术认证和专业认证而构建，支持基于区块链的证书的创建，发布，查看和验证。 参与机构的数字证书将在公共区块链上进行注册，并以加密方式签名，因此在申请就业，大学或移民时，这些数字证书是防篡改的，并且立即有用。 马耳他的试点项目将开始建立一个教育记录的公共链，同时要警惕这是一个可扩展性和灵活性的方案，可以选择获得区块链证书的公民在将来从公共和私人区块链中受益。

虽然证书是使用区块链（分布式p2p数据存储，不是由任何一种地理位置设计的）发布的，但是如果国家和接收者希望使用Web来显示和验证证书，则证书本身可以被托管在任何地方。 网站上托管的任何东西（从输入到发行平台的数据到签发后存储的证书）均保存在完全符合所有欧盟数据保护法[61]的加密的专用EU数据环境中。 数据和分析界面只能由马耳他政府授权的授权用户访问。

教育观点：在三个机构的平行飞行员

2017年9月22日[NDND]，MEDE与LM签订合同，在马耳他艺术科技学院（MCAST），旅游研究学院（ITS）和全国高等教育委员会NCFHE），2017年第四季度开始[62]。 马耳他大学还正在与LM进行区块链认证试点和学术研究的战略合作。

MCAST文凭

LM将为MCAST提供发行工作空间，以设计文凭模板，批准收件人名单，并通过选择加入程序向毕业生颁发数字文凭。 选择以这种格式获得文凭的学员可以在线或直接与其他人（学校，雇主等）以可独立验证为真实的格式分享。 MCAST受益于欺诈保护以及分享这些数字文凭带来的营销和分析的新形式。

ITS（培训证书）

与MCAST类似，LM将向旅游研究学院（ITS）提供发放工作空间，以向学生授予完成/成就的数字证书。这些官方数字证书可以由毕业生拥有，并为终身学习记录做出贡献。 ITS利用最新技术升级数字基础设施，确保欺诈保护和公众存在，从而提升ITS的形象。

NCFHE（Equivalency Statements）

LM将为NCFHE提供一个发行工作空间，用于创建模板，并根据请求向学习者发出教育等同性声明，以取代目前使用的基于PDF的过程。 这些基于区块链的记录的好处是为NCFHE提供欺诈保护，并且对希望检查声明真实性的任何实体进行即时验证。 这些等同声明由NCFHE拥有，而不是收件人，因此实施过程相对简单。 等效声明的持续应用是对声明人的证书进行认证

---

(61) 另见Smolenski（2017b）

(62) 见http://connectedlearning.edu.mt/malta-first-nation-state-to-deploy-blockchain-in-education/http://connectedlearning.edu.mt/malta-first-nation-state-to-deploy-blockchain-in-education/

难民身份，以非正规移民的身份抵达马耳他或因某种原因无法轻易获得学历证书。

NCFHE（认证和执照）

LM将为NCHFE提供第二个发行工作空间，向其管理的100多个机构颁发认证证书。 这些记录的好处是为NCFHE提供欺诈保护，并且更方便地验证在马耳他境外运营的提供商的机构认证。 预计推出日期为2017年6月，但可能会根据NCFHE的时间偏好而有所不同。

马耳他飞行员将涉及注册服务机构，技术专家，研究人员和政策制定者。 其目的是在这个过程中，可扩展性和私有与公共区块链的战略决策也将被制定。 将证书数据写入公共链和私人链都有好处。 当证书数据记录在公共链上时，学习者可以完全拥有自己的成绩记录：这意味着他们可以向任何雇主，任何招生委员会或任何其他人出示证书，并且该第三方可以立即看到整个凭证的内容，并验证其合法性。

超越教育：民族国家的视角

MEDE试点项目被定位为马耳他国家区块链战略的现场案例研究（Diacono 2017a，b）。 2017年7月，马耳他在总理办公室（OPM）内任命了一名议会秘书，以推动与数字经济相关的国家举措。 因此，作为实践的第一个例子，教育认证的试点正在被部署在这个更广泛的框架内。 很明显，很多潜在的电子政务项目[63]也将受益，其中涉及区块链上的证书问题。 以下是由OPM确定的持续列表：保健；土地登记；公证行为；生活事件（出生，结婚，死亡证明）；地址点；警察行为；法院案件结果；驾驶执照和电子民主事件。

在计划更具挑战性的领域（例如金融）的飞行员时，还将对教育飞行员进行监测。

(63) 马耳他在提供电子政务服务方面享有卓越的声誉。 在欧盟委员会委托的2016年研究中，马耳他在衡量电子政务服务交付和绩效的所有主要指标方面均领先。 参见欧盟委员会电子政务基准（2016），可在以下网址获取：https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016- https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016- 节目 - 网上公共服务，改进，不均匀

9 政府和区块链技术

世界各国政府和监管机构正在密切关注区块链技术的技术进步。 这对政府的好处可能是深远的 – 提供生产力，安全和提高效率。 区块链可以作为一个共同的参考点，将不同级别的政府（地方，州和联邦）召集到政府的开放数据注册处。 这可能意味着政府服务更可靠的整合，各州政府间流动性和业务一致性的提高，以及区块链在受监管行业记录运营信息时更好的监管力度[64]。

9.1 政策制定者的考虑

4.2节讨论的区块链的社会价值主张对政府至关重要。 对于决策者来说，评估区块链等颠覆性技术的当前和未来影响，以及确定将要制定的政策选择以及作为结果而制定的策略，是一项特别复杂的工作。 这不仅是由于技术的新颖性，以及在近期和中期将如何被各利益相关方采纳的不确定性。 这种复杂性与利益相关者对区块链价值主张的相对重要性有很大关系。 在不同的利益相关者群体中可能存在潜在的利益冲突，在这些利益相关者群体中，这些群体可能数量众多，有时不易识别。 对于一个利益相关者群体来说，一个价值主张可能构成一个需要另一个用户群体减轻的风险。 政府有额外的责任，必须减轻风险，并确定可能为"公共利益"而实施的政策和战略。

如果我们不得不迅速评估构成区块链社会价值主张的五个原则对政府的相对重要性，并将其与教育领域其他三个主要利益相关者的可能评估进行比较，则会显示评估的差异。

表1是关键利益相关方对社会价值主张的评估的快照，表明可能相互冲突的立场和议程：

(64) 由英联邦科学与工业研究组织（CSIRO）的创新部门Data61进行的澳大利亚政府最近发表的两篇出版物就新兴技术及其对私营和公共部门组织的影响提供了有趣的见解。 其中一个侧重于澳大利亚区块链采用的四种可能情景，另一个侧重于包括政府注册管理机构和农业供应链在内的多个应用领域的技术机会和风险。 这些出版物是对政府规划大规模采用区块链技术的机会和风险感兴趣的政策制定者的必读材料。 参见Hanson等人 （2017）和Staples等人 （2017年）对本节讨论的一些想法进行更深入的分析。

表1：区块链技术对关键利益相关者的社会价值主张的相对重要性

		政府	行业 / 利益攸关方机构/自律机构	教育机构	学习者
1	**自主主义与认同**	高	不确定	中	高
2	**相信**	高	高	高	不确定
3	**透明度和出处**	不确定	高	高	高
4	**不变性**	高	中	中	中
5	**非中介**	高	低	高	不确定

新的破坏性技术的变化速度和引入速度增加了评估社会价值主张的复杂性 – 特别是因为必须综合考虑规模，速度和复杂性。 政府越来越难以理解这个网格，并利用传统的非协作组织结构来规划，实施和实现收益。

影响政府社会价值主张的几个"未知因素"，其核心是沟通困境：

— 区块链的社会价值主张的"市场"还有待发展：例如，尽管区块链技术预测会影响很多领域（见附件1），但它目前与金融科技而不是教育等同于本研究的主题。

— 尝试将区块链的价值传递给整个社会目前在专业研究人员，学者和业内人士的领域内。 如果我们要取得快速进展，就需要以清晰明了的方式传达非常复杂的概念，并能够与各利益相关方的目标受众产生共鸣。 这个过程还没有开始。

> *"人们经常认为，如果区块链技术具有显着的优势，那么它将不可避免地被采用。然而，采用区块链存在很多挑战。 首先，区块链的许多风险和局限必须与其可能的收益进行权衡。 其次，采用技术的途径并不总是很清楚，尤其是在由于网络效应而大规模采用许多好处的情况下，以及不清楚受益方是否也承担部署和运营成本的情况下。 第三，由区块链带来的潜在破坏和非中介化可能会威胁那些可能会限制区块链技术接受度的强大现任组织"*
>
> *(Staples等2017)*

因此，在考虑如何参与区块链技术的基本社会价值主张时，政策制定者需要在与公共服务具有重大潜力的技术和公共利益正确相关的兴奋之间取得平衡。 以及技术基本面上的不确定因素，因此要求政策和策略同样要谨慎和深思熟虑，因为它们是由获得比其他国家竞争优势的机会所驱动的。

表2列出了政府决策者在参与区块链[65]的基本社会价值主张时的一些主要考虑因素。 事实上，这些原则是相互联系的，因此所提出的问题很可能跨越一些领域，也反映了政府和公共服务的本质。

(65) 这些考虑是基于对行业专家的采访以及澳大利亚政府委托进行的近期研究。 参见Hanson等人 (2017) 和Staples等人 (2017)

表2：决策者对区块链社会价值主张的思考

社会价值主张	对政策制定者的考虑
自主主义与认同	— 从表面上看，欧盟的民主政府预计会支持赋予公民自主权的新技术。 从教学的角度来看，自主权原则是欧洲项目的核心。 — 政府正在采取不同的方法来确定如何与区块链技术合作。 自主权不可避免地在数据所有权，数据保护，在线身份验证，用户隐私，eID系统，分布式验证环境中的用户身份验证等方面打开了潘多拉的盒子 - 仅举几例。 对于公民和学习者来说，尤其是自主权利，可能会对政府组织专有信息和电子身份系统的传统方式构成威胁。 因此，数字身份管理体现了加强对经济活动的信任和确定性的好处，但在隐私和安全方面继续对政府构成挑战。 — 如果我们要使用技术隐喻，在区块链上公民的数字身份是由匿名公钥/私钥组合来表示的。 从政府的角度来看，需要将数字身份与真实的人联系在一起：这可能意味着将其与社会安全号码或将来的生物特征数据或生物特征数据的散列结合起来。 在不久的将来，我们的指纹可能成为我们的默认私人键6667. — 假设成员国从事电子政务解决方案的组织已经在研究和考虑开发能够在区块链上进行评论的解决方案，这是合理的。 这些组织可能从内部技术团队到小众创业公司。 例如，瑞士技术公司Procivis[68]开发了“围绕个人数据的保护和自主权建立的政府可信电子身份识别解决方案”。 其Procivis eID +产品杠杆的生物识别技术， 密码学和区块链为政府和最终用户提供防篡改数字

(66) 在最近的Ethereum峰会上，Case首席执行官Melanie Shapiro宣布，她的公司正在开发使用生物识别技术通过Case Wallet进行部署的应用程序。 在最近的以太坊峰会上，她表示Case正在使用生物识别技术。 看到www.choosecase.comwww.choosecase.com.

(67) 区块链钱包可以作为硬钱包使用，并用生物识别密钥进行保护，并保留指纹记录，而该指纹记录又被安全地保存，因此没有集中记录。 然后你可以给拇指印一些安全性。 在不久的将来，区块链这方面可能会有行业公告。

(68) 看到www.procivis.chwww.procivis.ch

	身份。 Procivis正在研究与真实人物/政府与区块链身份认证相关的问题，以创建一对一的电子政务应用程序商店。 这种双重认证的挑战很可能会与任何已经在电子身份系统上投入巨资的成员国产生共鸣，而现在需要了解区块链主题核心自主权如何影响现有电子身份系统的功能。 — 作为国家eID系统的运营商，政府有责任在网上识别用户，并将其数字与其"现实生活"的身份联系起来，因为这种身份识别对于建立对交易的信任以及获取基本服务至关重要。 目前，数字识别服务通过评估所提供文件的来源来验证关于身份属性的声明。 在我们这个全球化的世界里，每一种消费的商品都与人和物的流动相对应。 然而，底层供应链对最终消费者来说往往是不透明的。 通过识别和交叉引用与地点和人员的关系，为消费品创造透明度和出处，增强对这些交易的信任和信心。 然而，身份证明是数字化世界中最基本的，往往是具有挑战性和资源密集型的交易之一。 — 政府认识到所有可核实数据的来源不一定是"互相交谈"。 区块链可以让学生获得对他或她的数据的权利，并转而分配这些数据的权利 - 创建一个链。 这等于赋予个人能够允许机构相互交谈，而不是假设机构将代表他们这样做。 通过个人保存的主密钥来推动权力，然后个人决定如何处理他或她的身份变体。 智能合同如果编程合适，可以选择整套授权和认证，然后向学习者（或第三方，如潜在的雇主）提供必要的保证，即一切正常。
相信	— 区块链技术对于在信任难以建立的互联网上产生信任的潜力具有重要意义。 — 尽管声称区块链预示着"不信任的社会[69]"的到来，但使用区块链并不能消除对信任的基本原则的继续应用。 用户在使用区块链技术时，仍然不可避免地冒着风险。 在区块链中，信任（依靠）是 区块链软件，激励或契约机制来驱动处理节点的行为

(69) 区块链技术将网络与数据库集成在一起，从而导致基于对等的分布式数据库跨越多个实体，没有单一所有者或单点故障。 区块链技术消除了对信任的需求，因为跨实体的即时同步（"近实时"）意味着不需要单个可信的第三方来保证交易的发生 - 因此是对"不信任社会"的主张。

	经营区块链系统的可信第三方以及在区块链上记录关于外部世界信息的"神谕"的可信第三方。 虽然区块链不会消除信任，但它可以消除信任单个特定第三方维护分类帐的需要，因此有时称为"分布式信任"机制。 在基于区块链的系统中，信任边界更宽。 例如，如果用户通过中介（如数字货币兑换）访问区块链，则他们信任中介：如果中介系统发生故障，他们的用户可能会失去对区块链上资产的控制权。 — 在这个发展的早期阶段，决策者必须考虑区块链可以被信任做多久。 迄今为止与比特币的经验是，数字货币可以被信任保留其完整性，因为它不能被伪造。 不过，正在进行的讨论是，区块链是否可以用于数字货币之外的用例，例如教育部门。 软件面临的挑战是本质上是一个黑匣子 – 特别是对于具有最小化风险和最大限度地控制企业软件传统的决策者而言。 信任是主观的，有条件的和上下文的 – 并且通常依赖于信任某人或某人来执行特定的行为。 新的分布式账本技术（DLT）已经超越数字货币，需要时间和实验来建立他们可信赖的声誉和意识。 政府将对名声长期存在并与表演紧密结合的事实保持敏感。 糟糕的表现迅速侵蚀了人们的信任，人们对机器的信任比人们要快得多。 — 因此，理解技术能力对监管机构至关重要，因此可以确保他们能够在信息披露，公平的商业惯例，如服务质量，纠纷解决和纠正方面设定适当的制度。 核心优势是分布式账本在特定时间点建立事实的基础能力，从而可以被信任。 分布式账本能够充当预言者 – 在这里，预言者是被认为提供可信和可靠（可信）信息的任何信息来源，而这又可以被用作有助于其他交易完整性的参考。 分布式账本可以是身份，内容和/或交易的预言者。
透明度和出处	— 原则上，区块链技术应该有助于政府越来越有义务以透明的方式运作，并在需要时展示出处。 — 分布式分类帐可以存储可信任的真实世界交易的数字化表示，以证明资产或对象的历史。 通过追踪交易，也可以证明资产或对象（或当前所有者）的身份。 对于容易识别的资产（例如学历证书）来说，这样做可能更容易一些，像谷物或牛奶这样的商品通常需要对每个资产单位（如RFID标签）进行代理 – 增加提供的保证，但不提供绝对的出处。 区块链技术将大大有助于保证出处，对政府相关活动和市场产生重大的积极影响。

	— 区块链也可以有助于更好的治理，因为断言或事务的永久性和持久性存储允许它们被信任用于证据目的。 通过分类账的透明度和不变性，区块链为监管机构提供实时或近实时访问高完整性交易记录的机会。 可编程交易和自动化合约工具将使监管机构能够制定与此监督相一致的细粒度和基于风险的市场控制。 — 区块链软件可以嵌入其他信息 – 使区块链登记比正统的财产转移记录和纸质记录以及可能被贿赂的官员更可靠！ — 这样做的必然结果是开放性并不一定意味着开放软件或供应商独立性：实际上，政府部署的一些更具创新性的区块链应用程序目前依赖与少数值得信赖的外部专家合作伙伴和流程既不透明也不一定不可腐败（例如依赖于私人区块链）。
不变性	— 个人自主权与区块链作为防篡改环境的可供性有很大关系：这意味着永久记录是有保证的，因为没有数据被删除，只能附加到区块链上。 — 从政府角度来看，不变性与安全性相关，与标准和互操作性相关联。 政府面向区块链面临的困境是，其存在的一个根本原因是以长期存在的信任观念为基础，即它们作为公众利益代表的能力，作为值得信赖的中介机构。 因此，不变性与政府开发和管理不变的（因此是安全的）系统的能力有很大关系，而这个系统是由政府或其可靠的中间人完全管理的最先进的技术。 目前，政策制定者将这一责任委托给公共区块链是一个挑战，尽管有人声称在实践中可能更安全和防篡改，任何依赖中央管理的系统政府（引入多重风险和失败等）。 — 标准使复杂的生态系统能够形成和发展。 但是，为了相关并推动创新（关于标准的更多信息，请参见第10.1节），它们需要一个相对稳定和明确的系统。 — 互操作性不仅仅是在技术配置上寻求协议。 市场上需要有信任标准才能被遵守。 互操作性涉及三个关键因素： a) 数据互操作性。 我们需要相互理解才能一起工作，所以我们的数据必须具有相同的句法和语义基础。 b) 政策互操作性。 我们的政策需要协调一致或基于商定的共同政策，以便我们可以确信，您将以我期望的方式处理我的信息（反之亦然） c) 国际标准的有效协作实施和使用。 参与

	但是，目前国际标准制定工作中的许多国家更有可能使全球采用和采用相关标准。 — 互操作性也发生在法律层面。 虽然软件是全球性的，但法律不是。 在多个司法管辖区执行"智能合约"时可能会出现复杂的法律问题。 特别是，"智能合约"在哪个司法管辖区运作的问题是一个根本性的决定。 分布式账本也可能被要求遵守许多法律和监管框架，即使不是所有的司法管辖区，也要遵守许多法律和监管框架。习惯法和贸易惯例通常是支持在多辖区情景下解决纠纷的基准。 分布式账本的破坏性潜力包括潜在的新业务模式和新的价值链参与者，但这意味着公认的行业规范尚未形成和测试。 分布式分类账需要在运营和法律上进行失败测试。 — 凯西（Casey，2017）认为，在这个关键时刻，政策制定者应该谨慎对待公众与私人或混合型区块链上的各种辩论。这种技术的未来状况最好是流畅的，所以互操作性是只有明智的选择支持。
非中介	— 对于政府来说，通过取消第三方控制分类帐（尤其是资产和交易数据管理）的非中介化可能被解释为分散化：由于一些社会文化，经济和政治原因，政府倾向于非中介化的怀疑。 决策者还应该考虑以下事实，这一点至关重要： a) 一个中央集权的权力总是代表一个潜在的单一失败点；和 b) 非政府拥有的区块链可能会提供更强大的基础设施来防止记录丢失[70]。 — 政府会担心可扩展性。 像比特币和以太坊这样的区块链系统目前还不能像传统交易处理系统（如Visa支付网络）那样达到最大吞吐量。 这是一个已知的和目前的限制，但正在通过新机制的发展来解决。 尽管区块链目前不具有高度可扩展性，但这不一定是固有的限制，并且可以在中期将来被克服。

(70) 有关分布式网络的更多信息，另见附件2。

9.2 欧盟成员国正在进行的举措简述

大多数欧盟成员国可能正在尝试区块链技术。 有些正在制定国家战略，还有一些正在进行具体应用的试验。

部分考虑的必然结果9.1 区块链技术可能为那些敏捷程度较高的国家（如小国和/或发展中国家）提供了机会，他们认为区块链是一种可以导致超越边界并提供国际利益的重大进步的手段。 以下数据主要是从案头研究汇编而来，其中包括通过具体的国家视角来阐述上述问题的情况。 部分8.4 还包括马耳他的用例研究。

9.2.1爱沙尼亚

作为一个民族国家，爱沙尼亚长期以来一直与数字社会的概念[71]以及最近的区块链技术联系在一起。 在2007年全国性的网络攻击之后，政府决定通过激进的新技术来保护自己的数字基础设施。 2007年，爱沙尼亚密码学家，网络架构师，软件开发人员和安全专家组成的团队在2007年得到政府和私营部门的支持，开始设计数字签名系统，最终形成一种称为无钥匙签名基础设施（KSI）的技术，以保护所有的公众数据。 今天，爱沙尼亚的几乎所有公共服务都通过提供给每个公民和居民的安全数字身份进行数字化和访问。

区块链技术的实验始于2008年左右。爱沙尼亚政府并没有采用全面的区块链生态系统，而是利用其在数字身份管理方面的重要专业知识，与可靠的合作伙伴共同开发私有区块链。 爱沙尼亚的立场是，加密货币协议对于他们的设计是非常好的，但对于大规模的企业数据供应链则不是。

区块链是爱沙尼亚国家身份认证管理系统的核心：几乎所有的公共服务都通过提供给每个公民和居民的安全数字身份进行数字化和访问。 公民与国家的互动通过大量的电子服务和计划（包括投票，电子税务委员会，电子商务，电子银行，电子学校和最显着的电子居留[72]为来自国外的人提供电子驻留。 自2012年以来，区块链技术一直在爱沙尼亚的注册管理机构（如国家卫生，司法，立法，安全和商业代码系统）运作，并计划将其用于其他领域，如个人医疗，网络安全和数据大使馆。 爱沙尼亚依靠集中的审定机构来确认证书的有效性，使用单向散列系统对加密的身份证件进行加密，他们也在报纸上公布，防止日期欺骗。 自2013年以来，爱沙尼亚政府登记 - 包括托管所有公民和商业相关信息的那些 - 已经使用Guardtime的KSI对其数据库中的数据进行身份验证。

爱沙尼亚的国家公共密钥基础设施（PKI）能够实现安全的数字认证和签名。 基础设施还允许通过使用加密密钥对转发数据：公共加密密钥和私人解密密钥。 该技术与电子身份（身份证，手机ID，数字身份证）有关。 爱沙尼亚使用的公钥基础设施是国家公钥基础设施，这意味着国家承诺保证公钥基础设施的存在和运作。

---

(71) 看到https://e-estonia.comhttps://e-estonia.com和 https://www.eesti.ee/enhttps://www.eesti.ee/en.

(72) 看到https://e-resident.gov.eehttps://e-resident.gov.ee

许多与PKI有关的服务是从私人部门购买的，例如认证，查询证书有效性的基础设施，公钥分发的基础设施（LDAP服务），密钥创建环境（例如，身份证芯片）。 数字认证对政府，商业和公共服务至关重要，从起草政策和立法到宣布财务和登记财产和继承权[73]。 公共记录的保管和准确性对于爱沙尼亚来说至关重要：PKI使他们从内部防止篡改，或者通过网络攻击。 最终，KSI区块链意味着虽然爱沙尼亚身份证可能永远不会受到违规（尽管迄今为止还没有）的免疫力，但政府可以保证，对公共数据的无赖更改将被100%检测到。

无钥匙签名基础设施（KSI）

KSI用于独立核查爱沙尼亚的所有政府流程，保护向公众提供的电子政务服务。 KSI将密码"散列函数"与分布式分类账配对，使爱沙尼亚政府能够保证记录网络和数据存储区内任何组件的状态。

使用区块链提供了exabyte规模的实时认证，因为每一个数据段的改变都被记录下来。 通过提供时间，身份和真实性的证明，KSI签名提供了数据完整性，后备保护和数据未被篡改的可验证保证。 它是透明的，也为用户的利益工作：公民可以看到谁审查了他们的数据，为什么，什么时候； 并且必须授权对其个人资料进行任何更改。 而且，通过使用散列函数，与大多数PKI中使用的非对称密码相反，KSI不能被量子算法破坏。 它也是如此的可扩展性，它可以使用可忽略的计算和网络开销每秒钟签署数据的数据。 它消除了对可信任机构的需求，其签名数据可以跨地域进行验证，并且不会因为不提取客户数据而影响隐私。 这个系统显然是PKI的一大进步。

它创建散列值，它将大量数据唯一地表示为更小的数值。 哈希值可以用来标识记录，但不能用来重建文件本身的信息。 散列值存储在区块链中，并分布在政府计算机的专用网络中。 每当底层文件发生变化时，新的哈希值将被添加到链中，并且不能再更改此信息。 每条记录的历史都是完全透明的，可以检测和防止系统内外的非法篡改。 KSI允许政府官员监视各种数据库中的变化 - 谁更改记录，执行哪些更改以及何时更改。 所有爱沙尼亚公民的电子健康记录都是使用KSI技术进行管理的，该国正计划将KSI提供给该国所有政府机构和私营公司。

爱沙尼亚凭借其经验和在线身份验证和电子政务的声誉，为区块链开发了一个明智的政策框架。 这个

(73) 公民可以凭身份证办理处方，投票，在线银行，查阅子女的学籍记录，申请国家福利，申报纳税申报，提交规划申请，上传意愿，申请军队服务，约3000个其他功能。 企业可以使用身份证来申报年度报告，发行股东文件，申请许可证等。 政府官员使用身份证加密文件进行安全通信，审查和批准许可证，合同和申请，并向执法机构提交信息请求。 部长甚至使用身份证准备和举行内阁会议，允许他们审查议程，提交立场和反对意见，并审查会议记录。

框架将最终扩展到教育，并整理高等教育机构颁发的所有学术证书。 目前尚不确定是否：

— 该系统将定位为国家教育数据库，数据是否以及如何与共享的电子身份基础一起使用，并用于教育以外的应用（例如劳动力市场目的）；

— 爱沙尼亚国家资质/证书数据库将与区块链应用程序相互作用；

— 爱沙尼亚的所有大学都将参加这一框架。

9.2.1.1爱沙尼亚电子身份举措的主要参与者

保护时间[74]

这是按收入，人数和实际客户部署计算的全球最大的区块链公司。 它拥有130多名密码学家，开发人员和安全架构师的团队，拥有数十年的防御国家攻击网络的经验。 它支撑着政府的运作，其客户包括全球最大的国防和电信供应商。

Guardtime的使命是验证在线信息并使其通用可靠。 在这种情况下，指出区块链最有价值的应用是组织内部和组织内部的软件，物理和信息供应链。 该公司声称，它可以帮助客户了解这些供应链并制定解决方案来加强它们，消除效率低下并为其完整性提供数学上的确定性 - 在数字和物理项目层面进行追踪。

Guardtime栈是应用于区块链的Unix哲学 - 抽象和封装成层，每个功能都有一个功能。 这种方法提供了可扩展性，互操作性，可靠性，并与遗留系统协同工作。

服务反映了非常广泛的重点领域。 这些被列为：重要的基础设施保护；企业安全；大数据存档；数据泄露管理；内部威胁缓解；对象存储； DevOps的；云无线电区域网络；广告归属；云计算保证；电子政务；物联网（IoT）；连接车辆； GDPR合规性

客户遍布电信，国防和航空航天，金融科技，保险，电子政务和数字广告。

信息系统管理局（RIA）[75]

信息系统管理局（RIA）是2011年成立的一个政府组织，目前正在向经济和通信部报告。 协调国家信息系统的开发和管理，协调有关信息安全的所有活动。 RIA建议公共服务提供者按照要求管理信息系统并对其进行监控。 另外，RIA是欧盟结构援助的实施实体。

SK ID解决方案（SK）[76]

(74) 看到https://guardtime.comhttps://guardtime.com

(75) 看到https://www.ria.ee/enhttps://www.ria.ee/en

SK由瑞典银行，SEB银行和Telia Eesti于2001年创立，专门从事国际电子身份解决方案。

SK是认证和时间戳服务以及处理客户数据的有效性确认服务的官方认证供应商。 作为爱沙尼亚州的合作伙伴，SK负责颁发国家身份证件（身份证，移动身份证，电子证书，居留证和电子身份证号码）的证书。

SK使用ID卡的软件包括DigiDoc软件，该软件支持数字签名，检查签名的有效性并加密数据。 目前，SK使不同国家的公民能够登录到电子服务和数字签名。 它支持600多个组织，其中包括金融，医疗保健以及其他各种私营和公共部门的电子服务。 SK在爱沙尼亚的服务有超过70万的终端用户。

主要举措：

- 认证和时间戳服务；
- 数字签名技术和应用程序的开发
- 验证服务。
- 丹麦电子转速表项目的认证服务。

9.2.2荷兰

荷兰政府正在与行业和知识机构合作，确定一些可在短期到中期启动的国家和国际试点[77]。 荷兰区块链联盟议程是超过20个活跃在物流，能源和金融领域的组织以及政府和研究机构的联合倡议。 联盟认为区块链是公民，社会和公司的信任，福利，福利和安全的潜在来源。 联盟的目标是为可靠和社会可接受的区块链应用创造条件，荷兰的目标是成为区块链技术应用的国际领先者。

几个试点举措正在接近原型阶段，预计将在几年内投入运行[78]。 第一批飞行员于2016年11月完成，行动计划于2017年4月提交[79]。 2017年9月，国际飞行员将启动。 在撰写本研究报告时，联盟正在从研究模式转向实际建立小型飞行员。

尽管荷兰政府赞成由爱沙尼亚，英国和迪拜推动的"区块链式政府"的构想，但其行动计划表明，与爱沙尼亚模式相比，公共区块链和开放标准可能更符合新兴的国家区块链战略促进私人区块链和依赖或密切与私人组织的合作。 具体而言，荷兰联盟确定需要建立由政府资助创建的区块链代码规则和标准，并建议该代码应完全开源。

---

(76) 看到https://sk.eehttps://sk.ee

(77) 看到www.blockchainpilots.nl/home-engwww.blockchainpilots.nl/home-eng 和 www.dutchdigitaldelta.nl/en/Blockchainwww.dutchdigitaldelta.nl/en/Blockchain

(78) 看到 https://docs.wixstatic.com/ugd/df1122_3de6de424d3b4f618af9e768e12d0ca0.pdfhttps://docs.wixstatic.com/ugd/df1122_3de6de424d3b4f618af9e768e12d0ca0.pdf

(79) 看到http://www.the-blockchain.com/2017/04/14/dutch-national-blockchain-coalition-presents-action-http://www.the-blockchain.com/2017/04/14/dutch-national-blockchain-coalition-presents-action- 议程/

有一个明确的方向，即以任何形式避免供应商锁定：这延伸到服务合同和基于开源代码的应用程序。 这也要求公共服务部门与所有供应商做出公开，透明和诚实的安排。 再次，联盟赞成公共部门与"创新型公司"的合作关系，这些公司不一定是"大型IT公司和咨询公司"。 荷兰研究机构TNO是影响国家区块链战略的关键合作伙伴之一[80]。 代尔夫特大学[81]拥有IMS，拥有区块链研究实验室，主要从事与人力资本，金融科技和加密货币相关的区块链研究领域的研究。 联盟计划与ICTU（一个为荷兰政府工作的IT基金会）合作建立一个区块链实验室。 这样的实验室将使区块链团队和政府组织能够在安全和可信赖的环境中快速将用例转化为工作原型。 明显倾向于从小做起：投资于知识和小型实验，作为创建可持续区块链项目的第一个构建块的手段。

政府有义务在下列情况下决定区块链管理的未来：a）概念验证和b）技术证明。 标准化问题需要加以解决，特别是在ISO / TC 307区块链和分布式账本技术[82]的框架内，荷兰是20个参与成员的一部分。

与大多数欧盟成员国一样，荷兰可能欢迎明确的欧盟关于区块链教育开放标准的政策。 荷兰大学目前正在开展独立研究项目，探索公共区块链的标准化过程：撰写本报告时的估计是，在荷兰有大约100个项目，180个来自各个组织的研究项目学位论文：这些可能主要集中在人力资本项目上，但也有一些正在进行中的证书，文凭和监管研究项目。

(80) HTTPS：//www.tno.nl/en/www.tno.nl/en

(81) 看到http://www.blockchain-lab.org/http://www.blockchain-lab.org/

(82) 看到https://www.iso.org/committee/6266604.htmlhttps://www.iso.org/committee/6266604.html

10 区块链在教育领域面临的挑战

除了本研究中已经确定的问题外，区块链在教育领域的应用也面临着一些挑战，并且必然与早期技术相关联。

10.1 标准化

> *在技术生命周期的过程中过早地定义标准可能是有害的，因为创新和商品化的竞争可能会产生反作用的做法和联盟，导致市场分裂。 竞争时，更好的标准可能不会赢。如果组织过早移动，可能会有更好的替代方案被扼杀，如果移动得太晚，现有用户切换到标准的成本将会更高。*
>
> *(Hanson等，2017)*

> *"前方最重要的工作不是技术性的。 与制度和治理有很大关系。 这将需要协调一致的努力，以确保数字证书系统的标准是开放的，并考虑到所有参与者的需求 - 学习者，教育机构，雇主和政府 - 而不是优先考虑某些组织的利益其他。 现在是试验，合作和分享经验的时候，以充分发挥建立数字证书生态系统的全部潜力。"*
>
> *(施密特，2017)*

10.1.1 什么是标准？

一个标准，是同意做某事的方式。

虽然任何人都可能声称要制定一个标准，但并不是所有的标准都是平等的，因为它们需要形成共识和明确的指示。

在标准化社区内，最受尊重的标准是由ISO，CEN和IEEC等组织根据世界贸易组织技术性贸易壁垒（WTO / TBT）（ISO，2010）：

- 透明度；
- 开放性；
- 公正和协商一致；
- 有效性和相关性；
- 连贯性；
- 解决发展中国家的关切。

其他国际标准通常称为国际私人标准，可由非政府组织，网络和/或公司开发。

10.1.2 通过区块链技术分散标准化

如第6.2.1节所述，区块链网络由一组运行相同区块链软件的节点组成。 在这个软件中编码的是网络的规则 - 谁可以写入区块链，共识是如何形成的，数据的结构以及网络认为合适的其他规则。 因此，通过运行软件，网络有效地创建了交易特定区块链所设计的资产的标准 - 确保了网络内部的共识和标准化，因为软件的任何改变都需要被整个网络批准，否则（在技术界被称为"分叉"）。

这种标准化方法非常有效，使得许多人提出了一个分散的自治组织的概念，即企业章程中包含的或法律强加的正式治理规则被编程到区块链网络中，以确保只根据那些规则（Jentzsch，2016）。

10.1.3 当前的区块链标准化举措

尽管区块链技术通过共识机制有效地对特定区块链的用户实施了一套技术标准，但这并不意味着区块链技术是标准化的。

因此，例如，大多数使用blockhchaints颁发证书的供应商仅将证书的散列存储在区块链中。 因此，问题，共享和验证过程都是使用供应商开发的软件在链外进行的，而目前这些软件都没有标准化。 因此，有可能出现几十家公司和组织在相同的区块链上签发证书的情况，但是每个证书需要不同的软件和供应商协议才能够使用。

其次，不同的团体可能会创建不同的区块链来互相交换同一资产，而不保证不同链之间的互操作性。

负责创建大多数支持互联网的（私有）标准的W3C联盟已经成立了一个经过验证的索赔工作组来处理有关教育证书和自主主体身份问题的标准化问题，并且还提供区块链讨论了为区块链创建消息格式的问题。

ISO还启动了技术委员会307来处理区块链和分布式分类帐。 目前已经成立了5个工作组来处理以下问题：

- 参考架构，分类和本体；
- 用例；
- 安全和隐私；
- 身份；
- 聪明的合同。

10.1.4 教育档案的规范化

在欧洲，在教育领域内，学生记录几乎没有标准化。 目前，高等教育所获得的教育已经被标记出来，以ECTS或ECVET两个学分标准之一的学分来表示。 但是，对于任何一种信用标准都不存在元数据标准。

所有在欧洲高等教育地区颁发的学位都附有一个文凭补充标准，用于描述学位的标准条款。 然而，再也没有文凭补充计算机可读数据的标准。 欧盟刚刚发表了关于欧洲文凭补充数字化的可行性研究（Pocius，D.，et al。2017），该文件没有提及区块链提供的机会。

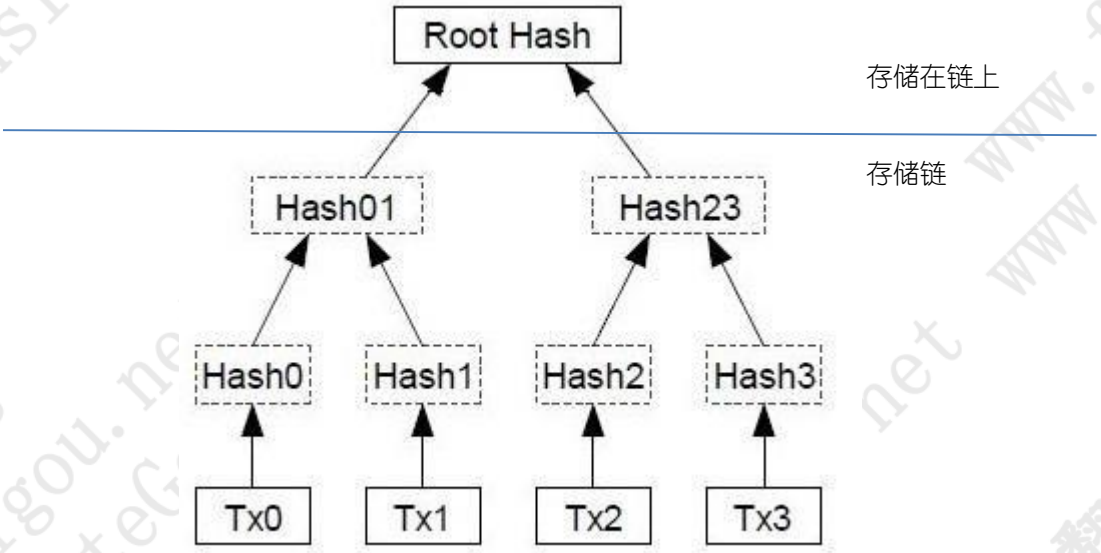
对于没有被ECTS或ECVET涵盖的所有其他级别的教育，没有系统，文档或系统信息的标准化。 尽管区块链整合不同数据源的能力为这一领域的发展提供了巨大的机会，但缺乏标准化将限制任何实施的影响，除非得到解决。

10.2 资源使用和保持复杂性

大多数区块链具有非常高的存储成本，因为整个区块链需要存储在网络中的每个节点上，并且由于处理密码所需的计算能力，所以还具有极高的能量使用。 举例来说，以太坊区块链上1TB的存储成本大约是6000欧元[83]，而相同尺寸的硬盘则大约为60.00欧元。 在能源成本方面，据估计，单个比特币交易目前使用160千瓦时的电力，这足以为美国家庭供电6天。 实际上，比特币网络目前预计将使用全球约0.1%的电力来处理每秒4笔交易。 如果这个比例是线性的，每秒成千上万的交易，这显然会导致全球电力消耗的大幅度增长，并且可能是一场环境灾难。

因此，区块链上资产的任何转移都越来越多地包含在链上和链外的数据。 正如前面的章节所解释的，不是直接将资产或记录存储在区块链中，而只是存储这些记录的散列以节省空间。 但是，即使这样也不足以满足区块链技术的能源和存储限制。 区块链中更多的节点意味着更高的能源和存储成本，而且更高的安全性。 因此，区块链的许多应用程序现在只将整个交易数据的散列存储在区块链中。 进行这种存储的一种常用技术是使用一种称为Merkle树的密码技术，简单地说，它是其他哈希值的散列：

图22：使用Merkle树的区块链存储的典型数据结构



在这样的系统下，哈希所代表的实际数据，无论是证书，签名，个人数据，合同等还是需要存储在某个外链的地方。

[83]假设天然气价格为20克威，而以弗所价格为300欧元。

如何存储这些数据的许多不同的实现正在运行，包括用于存储的系统：

— 用户的个人设备（与自主主体身份相联系）；

— 由第三方操作的集中服务器；

— 其他（更小和更专门的）区块链被称为侧链；

— 分布式对等网络[84]。

10.3 新的第三方依赖关系

尽管区块链技术消除了任何一方控制分类账的能力，并且尽管公共区块链理论上允许任何人加入网络并直接参与创建和验证链上的条目，但实际上存在重大的技术，知识和资源障碍这意味着实际上人们只能通过专门从事区块链技术的公司与区块链互动。

已经建立在顶级区块链技术基础上的数以百计（甚至可能是数千种）的服务类型包括：

— 数字钱包，允许您持有在区块链上发行的资产和/或记录；

— 交易平台，便于在区块链上交换资产；

— 允许在区块链上创建资产和记录的发行平台；

— 全新的区块链；

— 令牌创建者，这些创建者创建了在已经存在的区块链平台之上交易新资产类别的方法；

— 构建与区块链交互的接口的工具提供者；

— 存储解决方案供应商，提供处理脱链数据的方法。

由于解释的限制10.2通常所有这些服务都只是在区块链本身存储一小部分代码和数据，从而有效地将自己作为用户和数据之间的中介，重新引入了依赖于本报告中讨论的中央权威的所有缺点。

如果有关组织采用最好的开放源码和开放式数据的做法，那么它们仍然可能仅仅作为一个促进者而不是一个守门人来访问基于区块链的服务。 然而，架构的复杂性和所涉及的多方性意味着用户能够对哪些运营商真正开放做出明智的决定是不现实的。

对于像银行这样的传统集中分类账，金融监管机构等监管机构和标准化机构制定了技术标准，只有在符合严格标准的情况下才允许组织运作。

目前还没有标准的政府机构或第三方机构可以评估这些服务，以确定他们的要求是否属实，他们是如何处理区块链技术实力的数据。

这种开发应用程序的机会几乎是无限的，再加上法规的滥用和滥用的机会，往往导致区块链生态系统是描述如该*野生西。*

[84]这种网络的一个例子是IPFS（星际文件系统）。 更多信息可以在这里找到：（https://ipfs.io）

11 使用区块链教育的使用场景

11.1 何时使用区块链

考虑到使用区块链技术的成本10.2显然，尽管围绕技术的炒作，从技术的角度来看，它只能应用于特定的用例。 因此，如果一个应用程序符合一套特定的标准（Greenspan，2015），应该只使用区块链技术，即需要：

— 一个数据库被格式化为一个分类账，即一个列有交易时间戳的交易清单，从谁到谁；

— 多个作者，即不同的人（通常在不同的物理位置）需要写入数据库；

— 即在没有信任的情况下进行交易，即每个作者到数据库都不愿意允许其他人编辑他们的条目；

— 也就是说，不同的作者不希望把数据库的控制权交给中央管理机构，以便管理它；

— 交易互动，即交易之间有一定的相互依赖性。 因此，例如，如果人A将1个单位转移给C人，而B人也将1个单位转移给C人，则在确定C的余额时需要检查两个交易；

— 一套明确的规则，即交易只有在满足精确条件的情况下才可以被独立和自动验证；

— 一个有价值的商店，即区块链上的条目应该代表具有真实世界价值的资产或记录。

11.2 什么样的区块链使用

广义而言，可以应用三种不同类型的区块链解决方案，其中每一种在架构和治理方面都存在显着差异：

— 公开的区块链是开放给任何人下载，运行和交易。 使用这种方法构建的解决方案依靠公众共识来达成决策，通常可能运行数百万台计算机。 因此，公共区块链产生最大的不变性，分散性和透明度 - 然而，这是以高储存成本，高用电量以及低交易速度和数量的高效率为代价的。

— 私人区块链只能通过邀请，并根据邀请者制定的一套规则进行操作。 这样的区块链可以被少数几个当事人用来在他们之间独家交易，或者它可以对任何人进行交易，但只允许一组选定的用户改变规则和/或验证交易。 有效的是，私人区块链降低了不变性和链条的透明度，并且是高度集中的（虽然仍然提供比传统数据库更多的优势），然而，减少参与方的数量意味着链本身往往更小专业化 - 导致高效率，高交易量和高速度，从而降低成本和资源使用

— 联盟区块链实际上是两种模式的混合体。 一个联盟区块链是一个私人区块链，也就是说，只有受邀者才可以参与，但所有被邀请的人都拥有公平的投票权，并通过协商一致作出决定。 因此，从治理的角度来看，它保持了公共区块链的分散性。 在不变性，透明度和资源使用方面，它提供了私人和公共连锁的特点。

11.3 区块链教育的使用场景

本部分根据当前的技术发展状况，列出了八种应用区块链的情景。

方案1：使用区块链永久保护证书前景：短期/现在

现状：教育机构目前使用公共密钥基础设施以纸质或电子形式颁发证书。 这些证书花费时间和昂贵的问题，维护和验证。 公钥基础设施要求使用证书颁发机构作为颁发证书的中介，创建可能被滥用的依赖关系。 目前的核查记录在自然灾害或战争中也可能被破坏。

说明：在这种情况下，颁发数字认证的教育机构将使用公共区块链来存储与这些数字认证相关的数字签名。 独特的签名数字认证直接提供给用户。 因此，证书的真实性的验证[85]仅需要与存储在区块链中的数字签名/散列进行比较。

与当前状态相比的优势：证书的证明将完整，安全且永久地存储在区块链中。 因此，即使颁发证书的机构关闭，或整个教育体系崩溃（例如，在叙利亚发生的情况），这些证书仍然可以通过区块链中存储的记录进行核实。 此外，一旦机构颁发证书，他们不需要花费任何进一步的资源来确认该证书对第三方的有效性，因为这些证书可以直接在区块链上验证自己的证书。

先决条件：启用此方案所必需的唯一先决条件是允许签发张贴到区块链的签名的证书以及验证软件来确认这些证书的软件。 Blockcerts是一个已经存在的开源解决方案。

此外，由于证书本身没有存储在区块链中，所以机构和用户都需要一个安全的，故障安全的系统来长期存储这些证书。

情景2：使用区块链验证多步认证展望：短期

现状：目前，欧洲有数百个认证通道。 在公共认证方面，每个国家对于认证机构（以及认证机构）都有不同的制度，而且对于不同类型的组织，往往采用不同的制度。 此外，还有非政府组织和私营部门进行多重重要的认证。

认可证书的雇主和教育机构通常不仅需要验证证书颁发者，还需要验证证书颁发机构的质量。 在这种情况下，政府或私人认证机构颁发的认证对于确定资质的质量具有重要的意义。

要验证证书是否由合法机构颁发，个人需要检查：

[85]请注意，唯一经过验证的是，一个可识别的机构确实已经颁发了具体的，可识别的证书。 这种证书所代表的教育质量没有任何要求。

— 与该机构核实是否真的颁发了证书；

— 该机构声称拥有的认证质量；

— 认证机构是否真正向机构颁发证书的；

— 认证机构由哪个机构颁发认证；

— 如果他们真的授权认可机构进行运作的话。

这是一个非常耗时的技术过程，需要专家进行认证管理。 ENIC / NARIC网络是由所有欧盟成员国的工作人员和办事处组成的完整网络，旨在为获得高等教育资格提供便利。

说明：在这种情况下，教育机构不仅要按照情景1所述的方式使用数字证书，而且授权他们的组织也将自己的数字签名放在区块链上。 这样可以验证不仅X学生确实收到了Y机构的证书，而且Y机构也通过了认证机构Z的认证。

这种制度可以用来确保颁发证书的教育机构获得政府的许可，或者验证教育机构是否具有特定的质量认证，例如，MBA提供者是否真正获得了EQUIS认证。

优势：使用区块链，而不是研究这些连接，需要检查学位"谱系"的机构只需点击一下即可轻松完成。 一个完全自动化的流程将能够对认证链进行可视化，并验证证书确实已经颁发，并且（关键地）证明它们对于链中的每一步仍然有效。

先决条件：有许多不同的方式可以产生这种情况，所有这些方式都假定认证机构在区块链上公布其认证证书（或这些证书的签名），即：

— 认证机构可以在自己的网站上创建和发布"验证人"，这样任何人都可以上传他们的证书，并检查它是否是由认可的组织真正签发的；

— 认可机构可以将已颁发的证书本身发布到公共注册中心。 这将允许任何第三方核实：（a）高等院校颁发给学生的证书； （b）高等院校是否在公共登记处有证书，以及（c）所有这些证书是否真实。 这种实现要求独立的可信任方创建公共注册表；

— 机构可以创建自我主权的身份来存储身份数据 – 在这种情况下，他们已经收到了认可。 因此，第三方验证者将根据区块链检查学生证书的有效性，并根据发布的联合身份元素检查机构的血统。

情景3：使用区块链自动识别和转移信贷前景：中期

现状：目前没有描述ECTS或EQAVET的元数据标准，没有用于存储ECTS的标准数据库，也没有自动存储ECTS或EQAVET的标准化方法。 欧盟委员会已经委托进行可行性研究

数字化文凭补充，而少数由欧盟资助的项目已经考虑了信息通信技术转让学分的可行性[86]。

说明：在这种情况下，使用学分授予学习的教育机构（例如使用ECTS的高等教育机构或使用ECVET的职业机构）将授予专门为这些学分专门构建的自定义区块链的学分并转让学分。

优点：这样做的主要优点是，证书的有效性证明不仅可以存储在区块链中，而且证书本身可以存储在区块链中 – 这意味着证书本身将变成永久的和不可变的。 此外，这意味着不需要第三方来创建"背包"并存储证书 – 学生/毕业生只需要向高等教育机构或雇主提供他们的个人资料，他们在这些学分方面的整个教育历史将是即时可见和可验证。

此外，信贷系统往往用于转移和积累。 转移意味着在一个机构收到的学分被认为是对第二个学校的学历有贡献，而积累意味着在获得一定数量的学分后，学生可以获得学位等资格。

目前，信用转移取决于机构之间的谈判协议承认对方的信用受到一定的条件 – 但学生经常报告，这些协议是不承认。 使用区块链，这些协议可以写成智能合约，即在履行合同条件时，信贷将自动转移。 积累也是如此 – 根据机构的政策，智能合约可以被编程为在实现某些信贷目标时自动颁发学位 – 确保所有案例的转让和积累规则得到公平的应用。

先决条件：该情景需要（a）存在信用标准，具体描述信用由什么组成，以及如何授予信用，（b）创建专门设计的定制区块链，以将这些信息与软件一起存储与区块链互动，（c）参与的大量机构确保区块链交易的不变性。

对于欧洲的高等和职业院校来说，ECTS和ECVET的学分已经分别存在。 这种情况可以用不同的方式进行部署：

1. "信用区块链"可以由具有足够信誉的任何实体（例如政府或领先机构）部署，以确保其作为公开的无许可区块链被采用。 这将允许任何机构在区块链上提供信用。 这可以再与方案2中描述的多重认证系统相结合，以创建更多的信任级别。
2. 已经提供信用的机构可以发起一个信贷区块链作为联盟区块链。 如果其他机构符合某些标准，则只能进入区块链，从而确保区块链上发行的所有信用均来自具有共同质量标准的机构。

最后，如果将智能合约纳入系统设计，则需要建立软件来编制这些智能合约，并将其上传到链中。

---

(86) 伊拉斯姆斯没有纸项目（http://erasmuswithoutpaper.euhttp://erasmuswithoutpaper.eu）试图通过提供基于证据的可行性研究和不同的使用案例情景，以及建立将所有现有系统连接在一个网络中的实际解决方案，来影响高等教育机构通过电子方式充分交流学生的移动计划信息。

情景4：使用区块链作为终身学习护照展望：中期

当前状态：许多不同的社交网络，电子投资公司和"背包"提供商已经为用户提供了一种记录他们成就的方法。 但是，除开放式徽章外，这些系统都不能提供验证这些系统中所描述和包含的经验和凭证的方法 - 因此，这些系统是作为一个装满纸质证书的箱子的数字对应物来运行的 - 几乎没有获得额外的好处或效率从数字化的过程。

说明：在这种情况下，学习者将存储从任何来源（无论是正式的，非正式的还是非正式的）获得的学习证据，并且在共享时，区块链将被用于即时验证这些文档的真实性。

优点：这种情况的好处是，每个学生都可以获得可自动验证的简历，其中包含记录和所有学习和就业的证据 - 大大减少简历欺诈，并根据实施形式大大减少对核实简历感兴趣的组织和个人的工作量。

先决条件：从技术角度来看，最简单的方法是通过创建一个经过验证的数字联邦身份。 可以创建区块链，人们可以上传他们的声明，然后由区块链上的其他节点验证（通过检查声明的事实）。 一旦一定数量的用户确认该声明为真（并且取决于验证该声明的用户的声誉），则该声明接收作为其可验证性的分数的信任分数。 已经有公司测试这种类型的软件和服务，正如部分所述7.3.

如果使用元数据标准来描述不同类型的索赔（例如非政府组织的经验，就业和培训课程），那么这将与招聘软件和系统相关联，以便机构自动验证人员是否具备各种所需的技能位置。

情景5：区块链跟踪知识产权并奖励使用和重新使用该财产

前景：中期

当前状态：目前，跟踪知识产权是由专业组织执行的一项代价高昂的工作，通常在有重大商业案例时才能这样做。 因此，收集机构跟踪音乐和视频的知识产权使用情况，以收取版税，而期刊公司跟踪文章的引用，因为这些数据因其用于学术推广而有价值。 由于追踪知识产权的复杂性，自行出版的人很难跟踪和商品化知识产权的再利用。 因此，例如对开放式教育资源的重复使用通常不会被追踪，或者使用极其简单的指标进行追踪。

说明：在这种情况下，教育工作者会使用区块链宣布公开教育资源的发布，并记录他们使用的引用。 这将允许出于版权原因公布出版日期，并允许跟踪任何特定资源的再利用水平。

在封闭的知识产权情景中，可以使用同一系统来跟踪机构创造的知识产权的使用和再利用。 这也可以与智能合同相结合，根据知识产权的使用数量向作者发放付款。

优点：从结构角度来看，这种情况与用于追踪期刊文章引用的现有系统非常相似。 但是，跟踪期刊文章的引用到目前为止，都要求中介机构对这些文章的使用进行限制，以换取这些服务，通常是以高昂的访问费用，

限制知识产权的共享和使用。 这限制了开放教育资源的使用模式。

使用区块链，我们消除了中介，从而允许任何人公开发布，并准确地跟踪重用，而不会限制源材料。

如果引入这样一个系统，就可以根据实际使用和再利用教学材料来奖励教师，类似于根据引用研究论文奖励教师的方式。 通过作为高质量教材的代理，它还可以让学生和机构根据哪些教材使用的基于指标的决定。

先决条件：在这种情况下，区块链将被用于（a）宣布其资源的发布并链接到这些资源，以及（b）宣布他们在创建材料时使用的其他资源。 根据各自资源的重用程度，教育工作者将获得硬币奖励。

在一个开放的场景中，硬币将不会被消费，而是被用来确定作者的地位。 在一个封闭的情况下，硬币将具有货币价值，并会导致货币补偿。

更高级的实施可能会自动扫描资源，以确定重新使用其他资源的百分比，并相应地自动进行奖励。

情景6：通过区块链接收学生付款前景：短期/现在

现状：目前，学生用指定的货币支付学费。 特别是跨境研究，也是对立法的回应，很多机构只接受电子支付。

说明：在这种情况下，学生将通过基于区块链的加密货币为学习提供支付。

优点：学生并不总是可以使用银行账户或信用卡，这取决于他们来自的国家，年龄，就业状况等。这有时可能成为获得教育的额外障碍。 基于Cryptocurrency的支付将允许解决这个问题。

先决条件：这种情况下唯一的先决条件是学生和学校有办法发送和接收加密货币，即加密货币的钱包。

情景7：通过区块链提供学生资助，以凭证形式展望：长期

现状：许多国家（以及私人赞助商）通过在任何教育机构或预先批准的教育机构名单上给予学生"学券"或"花费"来资助学费。 这样的代金券系统是一种越来越受欢迎的教育资助方式，因为它们为学生提供免费教育，但仍然允许院校相互竞争，为学生提供最好的报价根据资助模式，这些代金券可能受到诸如要求学生毕业。 跟踪这些条件的遵守需要大量的管理。 此外，政策的变化可能意味着承诺的资金并不总是按照最初商定的规则分配给学生。

说明：在这种情况下，政府（或赞助商）的学费资助将作为区块链上的"代金券"授予学生。 可以根据某些绩效标准（如成绩等级），对学券进行编程，以向学生或教育机构分配资金。

优点：通过使用基于区块链的智能合约，资助者可以预先提供全部资金（为学生和机构提供安全保障），但只有在符合某些标准的情况下才能发放资金。 这个过程也可以自动进行，不需要任何中介机构，大大减少了管理这个系统所需的官僚作风。

这样一个系统也可以与学生贷款挂钩，还款的水平和期限与年级绩效，工资或任何其他指标挂钩。

先决条件：从区块链的角度来看，以太坊区块链已经支持这样的能力。 要使用这个系统，只需要（a）软件轻松地"建立"智能合约，并将其上传到区块链，以及（b）数据源（例如学生成绩的数据库）知道合同的条件是否已经达成。

情景8：使用验证的主权身份在教育机构内进行学生识别

前景：中期

现状：在较大的组织中，学生需要定期与组织的不同部门认同。 在这种情况下，组织的每个部门都会为自己收集学生数据，或者组织将使用单点登录，由此组织内所有各方都使用学生数据的一个共享副本。在这两种模式下，数十甚至数百人可能有机会获得学生的个人信息。 要保证数据安全，需要管理所有这些人的访问权限，并确保他们的设备也是安全的，防黑客的
– 一个庞大的事业。

说明：在这里，学生在与教育机构内的招生办公室分享他们的个人资料后，将从同一办公室获得他们的身份证明。 使用智能手机上的生物识别技术，结合本证书，学生将能够向组织内需要识别的其他任何部分（如图书馆，体育馆，食堂，学生宿舍，学生社团等）这些服务将能够识别学生，而无需再次请求或存储任何个人数据。

优点：通过使用经过验证的主权自我身份，只有首先负责验证学生身份的人才需要访问数据。 除此之外，唯一掌握数据的人是学生本人。 这意味着组织不再需要管理复杂的访问权限系统，只需要保证进行验证初始验证的设备或网络。 这将节省大量的资源用于加强数据泄露，员工培训数据保护和管理访问权。

另外，与组织内的学生进行互动的人员不需要承担保密敏感数据的责任，因为他们不需要首先知道这一点。

先决条件：目前有几家公司正在启动可应用于此用例的主权自我认同解决方案。 目前，这些机构需要进行重大的技术工作，将这些系统与现有的学生信息系统联系起来。 当现有的学生信息系统供应商采用主权自我身份进入他们的架构时，可能会广泛采用。

12 结论和建议

本部分根据本研究核心的案头研究，访谈和使用案例研究列出了一系列结论和建议。

12.1 结论

本节列举了本研究过程中所回顾的经验数据的13个重要结论。

结论	
C1. Blockchain 申请教育仍处于起步阶段	- 目前，区块链技术在教育领域的唯一实施正处于试点阶段。 正如本报告所显示的那样，有几个组织正处于使用区块链进行试点颁发证书的初始阶段，而另一些组织正在接受基于区块链的加密货币付款。 - 关于潜在的分布式账本技术应用的索赔与实际推出此类应用之间的差距继续扩大。 有传闻证据表明，越来越多的组织正在利用区块链技术“低头观望望远镜”，而不是将问题带到桌面上，评估区块链技术是否可以提供解决方案，而是将区块链技术引入桌面，寻找技术可能应用的问题。 - 虽然目前大多数关注金融科技而不是教育，但区块链技术的信任将从金融转向教育。 大型球员最终会把注意力转移到教育上。 试图将信任外包给技术的含义和应用不能被准确地预测，并且可能引起我们目前无法想象的复杂和副作用（Collins，2017）。 业内人士正在以三到五年的时间进行交流，但是区块链技术的实施可能是一个长达数十年的实验。 指标是大多数行业及其商业模式都会受到这项技术的影响，就像受到互联网的影响和破坏一样。
C2。区块链技术的全部好处只能通过开放的实现来实现	- 只有“完全开放”的区块链实现才能达到区块链教育的真正目标和承诺。这意味着解决方案的基本组成部分包括：a）接收方的所有权； b）厂商独立性和c）分散式验证。 如果不能全部实现，那么使用区块链可能会浪费所有利益相关者的努力和资源。 - 很大程度上取决于教育机构，政府乃至学习者（目标用户）将归因于“开放性”，“供应商” 独立"和"学习者授权" - 尤其如此

	那些与价值学习者相关的人将归于拥有自己的数字证书，而不是永远与（尽管可信的）机构或供应商锁定在一起。 - 虽然原则上这些都是非常有力的论点，但要确定这些目标用户是否比全球品牌开发的专有解决方案更具吸引力还为时尚早。
C3. Blockchain可能会扰乱学生信息系统的市场	— 区块链技术具有密码货币以外的重要用途，其使用案例已经开始进入主流。 这可能会在未来12个月内发生。 — 基于区块链的分类账有可能破坏当前行业所支撑的关键技术27亿美元[87]，因此可能会扰乱整个市场。 我们很可能会看到几十个到几百个成熟的公司和初创企业，希望确保这个领域的先发优势。 - 由于重要的网络效应将通过规模实现，未来几年内很可能有一些强大的技术供应商将站在整个行业的立足点。
C4. Vested interest有兴趣锁定区块链技术，并根据部分实现创建标准	— 如第4.2节所述，区块链的实施提供了重要的社会价值主张。 这些好处直接导致从单一主管部门的控制中删除重要分类账。 — 已经建立（或正在计划建立）控制这些分类帐的解决方案和业务模型的组织和公司，对抵制实施具有既得利益。 由于他们无法回滚区块链技术的发明，因此他们中的许多人正在创造"部分"和混合实施，使他们能够保留对分类帐的控制，同时还提供技术的其他优势，例如节约成本。 因此，尽管炒作，区块链技术的提及并不意味着一个普遍的信任协议 - 它通常意味着恰恰相反。 要通过区块链处理可令牌化资产以外的任何其他有价值的东西，需要额外的代理层，第三方和审计人员 - 这些与信任架构不一致。 - 在教育领域，首先出现的情况是一系列公司提供发行与区块链相关的证书，但只允许通过专有封闭平台访问这些证书的内容 - 有效地使用公开承诺系统作为创建一个封闭系统的陪衬。

([87]) 据Technavio (2017) 所述，到2021年，学生信息系统市场可能会增长到57亿美元。

C5。公私合作对充分利用区块链是必要的	— 区块链技术在教育中的部署和应用并不总是与市场和公众利益保持一致。 这种情况通常是市场调节的教科书。 — 另一方面，由于区块链技术如此新颖，技术的潜力才刚刚被发现，各国政府不应该在现阶段"挑选优胜者"，或者过度监管地锁定技术。 - 考虑到这一点，我们得出结论，唯一可能的模式是通过一个平衡的，战略性的公私伙伴关系来实现区块链的全部潜力。
C6. Blockchain技术有可能加速证书系统的结束	- 到目前为止，数字证书的采用受到它们可能被伪造的难易的阻碍。 区块链为企业提供了永久有效的永久有效数字证书颁发方式，因为它们的真实性可以通过区块链进行验证。 如果证书作为区块链上的标记传输，即使证书本身可以永久提供。 - 与现有系统相比，这些优势大大增加了数字证书的价值主张，并可能推动数字认证成为主流。
C7.Blockchain 技术 删除 需要 教育性 组织来 验证 证书	
C8. Blockchain有可能围绕学习者的数据发布创新浪潮	- 学习者的数据是许多应用程序的重要组成部分，包括人力资源管理系统，电子档案和专业社交网络。 区块链技术允许所有这些系统以任何（元数据）格式自动验证来自任何发行人的证书。 - 这种存储经过验证的索赔而不仅仅是索赔的能力应该能够显着提高这些系统对各种利益相关者的有用性。 - 我们可以想象应用程序：自动验证简历和候选人具有适当的资格； 以及其他可以自动将员工置于更高收入的应用程序 基于已完成培训的证据和使用经过验证的专业人员的专业网络

[88]如果使用者遗失或撤销证书，机构仍然可以在重新颁发证书方面发挥作用，例如，如果他们迟到被发现通过作弊获得。

	证书作为订阅的要求。 创业公司和在这个领域工作的公司可能会想到无数的其他想法。
C9。自主身份有可能显着降低教育机构的数据管理成本	— 欧洲法对作为个人数据保管人的组织规定了重大义务 – 要求他们控制组织内部有权访问的人员，并确保其在组织内的安全存储。 数据访问的人越多，管理越复杂，成本越高，数据泄露或滥用的风险就越高。 — 自主主义身份有效地创建了一个安全的身份证，可以由学生持有，并可以通过生物统计学与他们联系在一起 – 允许学生识别自己而不需要实际交付任何数据，也不需要与数据库交换数据由该机构持有。 该机构将能够识别学生，而无需实际保留和保留其数据。 – 这显着降低了管理开销，并减少了数据泄露或滥用的潜在"足迹"。
C10. 区块链技术可以使更为复杂的系统可靠地跟踪知识产权的使用情况	— 区块链技术有可能彻底改变知识产权的管理。 根据所作的政策选择，可以用来增加公开性或关闭知识产权。 — 通过将文档散列发布到区块链上，人们可以提供首次发布的证明，而不需要共享正在发布的文档或发明。 这使得传统的版权和专利法概念变成了一种头脑，使得可能有一个更加严格的制度，从而可以保护知识而不被分享。 – 区块链技术还允许详细和增量追踪谁使用过知识产权，在何处以及如何以及如何与信用相关联 – 以付款方式或以学术信贷的形式。 这种知识产权制度可以作为未来期刊的基础，甚至可以作为跟踪开放教育资源生产和再利用的基础。 这样，他们就能够大大激励教育和教育资源的开放。
C11. 教育网络可以通过分散式自治来自动化和标准化其许多功能	— 一个分散的自治组织（DAO）实际上是一个社区，根据事先商定的规则组织资源，并在其代码中列出（Allen&Overy，2016）。 因此，为了创建和转换这些资源而不违反既定规则的社区是被重新设计为DAO的理想候选人。 — 在欧洲的教育领域，这样的社区有几个例子。 美国的质量保证

网络	高等教育由利益相关方共同管理，共同制定认证机构的标准，并为符合标准的机构颁发认证。 ECTS没有集中注册机构，实际上是一个同意根据既定规则授予信用额度，然后允许机构之间转移信用的机构网络。 - DAO的应用可以：（a）自动确保在每个实施中按照相同的一套标准始终发生这种授信或认证； （b）确保这些证书的转让和/或使用始终按照规定进行； （c）创建一个统一的获奖证书数据库； （d）分享网络成员之间的系统控制权，没有一方有集中控制权。
C12. 法规和标准化可能决定进展的程度和速度	— 任何基于记录的系统的广泛采用需要标准，协议和监管框架以及系统的互操作性。 — 虽然多种形式的学生资格数据，尤其是高等教育的学生资格数据，多年来在整个欧洲得到了一些统一和标准化，但还有其他数据仍然没有统一的格式和标准。 在较低的教育水平下，学校离校证书尚未统一或规范。 — 此外，确实存在的工具，如文凭补充，ECTS和Erasmus协议，并没有设计数字记录 - 这些基本工具都没有遵循数字数据格式或数字元数据标准。 — 区块链能够存储不同类型的记录，并且能够在没有中央权威的情况下自动建立双方之间的共识，区块链可以简化这些标准的创建，但是如果没有这些标准，就无法真正在泛欧意义上部署。 — 开放标准和封闭标准之间存在权衡，但数据可移植性的可操作性至关重要。 如果我们希望人们能够通过任何系统在世界任何地方取得和验证他们的数据，那么开放标准是必须的。
C13. 人们不了解区块链技术的社会优势和潜力	— 随着世界各地几乎每天都有重大数据泄露的消息，采用数字技术记录保存意味着一个社会契约：提高效率和成本的代价：较低的安全性，隐私性和永久性。 — 正确实施区块链技术显着改善了这三个标准，使数字记录的副作用少得多。 — 然而，教育机构几乎没有证据证明区块链具有重要的价值 添加， 或 至 他们自己 要么至 其 学生们。 理解 该 潜在 的 blockchain 无

	例子 的 实现 至 点 至 需要重要的知识和专业化。

12.2 建议

本部分根据本研究过程中回顾的经验数据列出了7项重要建议。 这些建议旨在为寻求改善区块链教育过程和成果的政策制定者提供指导，而不是更普遍地推广区块链技术的高层次建议。

建议	
R1。 创建和宣传"公开"教育记录的标签	- 欧盟是否应该支持"开放"区块链实施的发展，并体现以下原则：a）接受者所有权； b）供应商独立性；和c）分散验证，那么这些条款将需要根据教育记录来定义。 - 我们建议欧盟召集一批认证，区块链技术专家和数据保护专家，为"开放记录"标签定义标准。 - 创建之后，为了促进开放记录的观念，欧盟与会员国可以同意只支持和/或采用符合这种开放记录标签的技术。
R2。 政策制定者应考虑调查和支持区块链技术在具体教育用例中的应用	— 我们建议区块链在颁发证书，认证途径，终身学习护照，知识产权管理和数据管理等领域的重大潜力将被进一步调查，并且开发解决这些使用的应用程序案件得到支持和加速。 — 由于这些使用案例中的每一个都有不同的依赖关系，而且由于解决每个使用案例有多种技术途径 - 我们强烈建议欧盟为每个使用案例提供资金和支持竞争性试点，以使最佳技术解决方案易于使用，鉴定。 - 这些试点应该鼓励来自几个国家的私营公司，创业公司，教育机构和公共机构的合作，例如使用"地平线2020"等工具。最好的想法是接受后续的主流化资金，从而完成全面创新管道。 — 这些场景在11.3节中描述
R3。 欧洲应该紧急考虑支持创建数字化元数据标准	— 元数据标准支持数据使用方面的创新（Dawes，2010）。 因此，基于教育记录（包括区块链）的任何创新都需要广泛认可的数字元数据标准。 — 需要开发标准来识别

教育记录	记录学生在不同教育程度的正式和非正式环境中的成绩，记录机构的认证和认证以及教育资源的使用和再利用等等。 - 数字元数据标准应通过多国多利益相关方的方式制定，以确保其处理所有（与标准有关的）贸易技术壁垒。 - 欧盟委员会应与成员国一道，在这一领域开展紧急和重大的标准化工作，可能与CEN或ISO合作。
R4。 支持利益相关者与区块链技术和分权自治组织的合作	- 区块链技术最令人兴奋的潜在实施方案主要围绕其在网络各方之间进行信任证书，信用，认证或其他资产转移的能力。 任何区块链策略的关键基础都不应该是“重新发明轮子”，而应该包括使这些网络能够利用区块链技术来改善利用区块链在网络内传输这些资源的举措。 - 因此，我们建议欧盟建立一个支持欧洲大学联合会（或其他教育组织联合会）的机制，使其能够调查区块链的应用，启动飞行员并将这些活动纳入其网络。 这种支持可能采取针对这种网络的有针对性的业务资金形式。 — 我们建议将这些活动连接到R2中的活动。
R5。 支持决策者了解区块链技术对教育领域各种活动的影响	— 将区块链充分发挥其教育潜力需要政策制定者确保区块链的出现可能对现有的和计划中的活动和战略产生重大影响。 具体来说，政策制定者需要通过获取知识来定义这一方面，从而为区块链优先设计思路提供信息。 — 这样做需要易于访问的跨领域知识。 - 我们建议组建一个咨询小组，负责为欧盟和成员国的决策者提供定期咨询，以获得具体应用的技术潜在回报，帮助成员国平衡风险和管理预期。 - 这将需要来自不同学科的专业人士和学科专家的参与和支持，包括私营部门专业组织和行业内部人士。

	– 此外，我们建议这样一个小组涵盖正规教育，非正规教育和就业的范围。
R6。 将自主权视为关键的数字能力	– 期望数据保护立法集中于仅仅处理数据处理者的责任就足以防止对高度敏感的个人数据的滥用和错误处理，这是不现实的。 – 用户拥有自己的数据并分担管理责任的自主权概念是数据管理的最佳模式。 – 为了让用户利用自主权，他们需要了解可用于数据管理的不同选项，以及每个选项的优点和权衡。 应将这些原则纳入有关终身学习数字能力的教育框架。
R7。 支持可能影响教育部门考虑使用区块链技术的关键领域的进一步研究	— 政策制定者和教育机构将受益于对隐私问题的进一步研究，知识产权管理；和数字身份。 — 作为框架的一部分，指导方针，培训，法规和其他机制可能是必要的，以确保防止分布式账本的误用导致不可接受的隐私侵害。对新出现的用例进行风险评估将分析当前需要填补的空白。 – 研究管理知识产权来源和完整性的有效平台可能会释放重要的经济活动和新的商业模式。 – 数字身份管理提供了增强经济活动信任和确定性的好处，但在隐私和安全方面带来了挑战。 由于区块链技术的新发展，对政策和技术方案的研究将为监管机构和行业提供相关风险和回报的改善方法。 能够实现数字身份管理的重要数字基础设施可被视为欧洲共享资产，对欧洲具有竞争优势。

参考

Abramovich, S., Schunn, C., &Higashi, RM (2013)。 徽章对教育有用吗？ 这取决于徽章的类型和学习者的专业知识。 教育技术研究与发展，61 (2)，217-232。

Aglietti, A. (2017a)。 知识的证明：相同的区块链，不同的故事。 可在：https://tail.aqquadro.it/proof-of-knowledge-efc138f2a17c

Aglietti, A. (2017b)。 GROWBIT @国际公开认可日。 可在：https://tail.aqquadro.it/growbit-international-open-recognition-day-a39281072a6c

艾伦 & 安理 (2016). 分散 自主性 组织。 可得到在：http://www.allenovery.com/SiteCollectionDocuments/Article%20Decentralised%20Autonomous%20Organisations.pdf

阿伦, C. (2016). 该 路径 至 自主权 身份。 可得到在：http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Au, S.不要忘记uPort不要求自己的主权身份系统。 可在：https://decentralize.today/dont-forget-what-self-sovereign-identity-system- UPORT-没有按叔权利要求到DO-1f43ca228575

Batchu, Y. (2017). 什么 没有 #Blockchain 带来 至 该 表？ 可得到在：https://blog.unocoin.com/what-did-Blockchain-bring-to-the-table-ded18ef70432

Byrne, WI (2017)。 什么是区块链？ 可在：https://medium.com/badge- 链/什么 - 是 - Blockchain-5e4498f05c20

Cheng, S., Daub, M., Domeyer, A.和Lundqvist, M. (2016)。 使用区块链改善 数据 管理 in 该 上市 部门。 可得到 在：http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-Blockchain到提高数据管理功能于对公共部门

Christensen, Clayton M. (2003)。 创新者的解决方案：创造并保持成功的增长。 哈佛商业出版社。国际标准书号978-1-57851-852-4.

克拉克·唐纳 (Clark Donald, 2016)。 10种方式区块链可以用于教育。 OEB见解。 可在：https://oeb-insights.com/10-ways-blockchain-could-be-used-in-education/

硬币电报 (2015)。 爱沙尼亚如何使区块链接近公民：GovTech案例研究。 可在：https://cointelegraph.com/news/how-estonia-brought-Blockchain- 近到公民 - govtech-案例研究

Collins, A。 (2017)。 四个质疑区块链炒作的原因。 可在：https://www.weforum.org/agenda/2017/07/four-reasons-to-question-the-hype-around-Blockchain

Consensys (2015). UPORT：该 钱包 is 该 新 浏览器。 可得到在：https://media.consensys.net/uport-the-wallet-is-the-new-browser-b133a83fe73

D'Artis, K., Ciaian, P.和Rajcaniova, M. (2016年)。 虚拟货币的数字议程。 比特币能否成为全球货 币 ？ 可 在 ：http://publications.jrc.ec.europa.eu/repository/bitstream/JRC97043/the%20digital%20ag恩达%20of%20virtual%20currencies_final.pdf

Dawes, Sharon S."管理和有用性：基于信息的透明度的政策原则"。 "政府信息季刊"27.4 (2010)：377-383。

德勤 联合王国 (2016). Blockchain：民主化 相信。 可得到 在：http://www.mondaq.com/uk/x/506472/fin+tech/Blockchain+Democratised+Trust

Diacono, T., (2017a)。 马耳他为"革命"国家区块链策略而设。 可在：

http://www.maltatoday.com.mt/business/technology/76459/malta_set_for_revolutionary_national_Blockchain_strategy_#。WTfGvpB96Uk

Diacono, T., (2017b)。 马耳他奠定了区块链革命的基础。 可在：

http://www.maltatoday.com.mt/business/business_news/79185/malta_lays_the_ground_for_a_blockchain_revolution#.WXiM2oiGOUk

多明格， J., (2016). Blockchains 和 更高 教育。 可得到在：https://www.slideshare.net/johndomingue/the-potential-of-Blockchain-in-higher- 教育

多明格， J. (2017). 教育的 新 孩子 上 该 块。 可得到在： http://www.open.ac.uk/research/main/news/educations-new-kid-block

复仇 基础 (2017). 复仇 主页。 可得到在：https://www.ethereum.org/

欧盟委员会（2016年）。 电子政务基准2016年。欧洲电子政务发展的转折点？ 由凯捷，IDC，Sogeti和米兰理工大学为欧盟委员会进行的研究。

Evans，J。（2017）。 区块链是新的Linux，而不是新的互联网。 可在：https://techcrunch.com/2017/05/28/double-double-cryptocoin-bubble

Feldstein，M.（2017）。 一个灵活的，可互操作的数字学习平台：我们还有吗？ 可在：http://mfeldstein.com/flexible-interoperable-digital-learning-platform- 然而

Findlay，C。（2015）。 分散和不受侵犯：区块链和数字档案。 从...获得https：//开头rkroundtable.org/2015/01/23/decentralised-and-inviolate-the-blockchain-and-its-uses- 换数字档案馆/

福德， B. (2017)， 运用 Blockchain 至 保持 上市 数据 上市， 可得到在：https://hbr.org/2017/03/using-Blockchain-to-keep-public-data-public

Gibson，D.，Ostashewski，N.，Flintoff，K.，Grant，S.，&Knight，E。（2015）。 教育中的数字徽章。 教育和信息技术，20（2），403-410。

Gideon，G。（2015）。 避免无意义的Blockchain项目。 可在：http://www.multichain.com/blog/2015/11/avoiding-pointless-Blockchain-project

全球银行与金融评论（2017）。 爱沙尼亚的区块链技术：政府层面会发生什么？ 可在：https://www.globalbankingandfinance.com/Blockchain-technology-in-estonia-what- 恰好，在政府层面

加拿大政府（2011年）。 加拿大政府的身份管理联盟：背景资料。 可在：https://www.canada.ca/en/treasury-board- 秘书处/服务/ accessinformation隐私/安全身份管理/ federating- 身份管理，政府canadabackgrounder.html

英国政府科学办公室（2016年）。 分布式账本技术：超越区块链。 可得到在：https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/GS-16-1-分布式总账，技术.pdf

格林斯潘 G. (2015). 避免 该 无意义 blockchain 项目。 可得到在：https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

Gupta，M.，（2017）。 Blockchain for Dummies，IBM限量版。 可在：https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN&

Hall，M.（2016）。 区块链革命：大学会使用它还是滥用？ 可在：https://www.timeshighereducation.com/blog/Blockchain-revolution-will-universities- 使用-IT-或滥用，它

Hanson, RT, Staples, M。 (2017)。 分布式总帐，澳大利亚经济未来几十年的情景。 堪培拉。 英联邦科学和工业研究组织。

IBM (2017)。 区块链基础知识：分布式账本介绍。 可在：https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-TRS / index.html的

Inamorato dos Santos, A., Witthaus。 G.＆Punie, Y. (2016) OpenCred：在欧洲通过MOOC讨论非正规学习的认识问题。 可在：http://emoocs2016.eu/wp-content/uploads/2016/02/proceedings-emoocs2016.pdf

国际标准化组织（1999）。 信息技术 - 编程语言 - Ada：语言处理器的符合性评估，1999。ISO / IEC 18009：1999。

国际标准化组织。 （2010年）。 国际标准和"私人"标准。 瑞士日内瓦：国际标准化组织。

介绍至该荷兰人Blockchain联盟(2017)。 可得到在：https://www.dutchdigitaldelta.nl/en/Blockchain/introduction-to-the-dutch-Blockchain-联盟

Jagers, C. (2017a). Blockchain为基础记录和可用性。 可得到在：https://medium.com/learning-machine-blog/Blockchain-based-records-and-usability-179a4eeaeb6e

Jagers, C. (2017b). 数字身分和该Blockchain。 可得到在：https://medium.com/learning-machine-blog/digital-identity-and-the-Blockchain-10de0e7d7734

Jentzsch，C。（2016）。 分散的自治组织自动化治理。 取自https://download.slock.it/public/DAO/WhitePaper.pdf

Kirkland，R.（2017）。 Blockchain的下一步是什么？ 可在：http://www.mckinsey.com/industries/high-tech/our-insights/what-next-for-Blockchain

Lewis，A.（2017）。 温和地介绍自主主义的身份。 可在：https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity

李，R.（2017）。 基于区块链的多签名教育证书。 伯明翰大学。 未发表的论文。

Lilic，J.（2015）。 UPORT：新一代自主主权认同制度的一瞥。 可在：https://www.linkedin.com/pulse/uport-glimpse-next-generation-self-主权身份的约翰 - 利利奇

Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., Sena, M. (2017)。 的UPort。 一个平台自主权身份。 可得到在：https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

Mamoria, M. (2017)。 跆拳道是区块链？ 用简单的英语来理解区块链的最终3500字指南。 可在：https://hackernoon.com/wtf-is-the-Blockchain-1da89ba19348

马文，河（2017）。 2017年区块链：智能合约年。 可在：http://www.pcmag.com/article/350088/Blockchain-in-2017-the-year-of-smart-contracts

麦肯锡(2016)。 怎么样Blockchains可以更改该世界。 可得到在：http://www.mckinsey.com/industries/high-tech/our-insights/how-Blockchains-could-改变世界

MIT媒体实验室（2016年）。 我们从设计区块链上的学术证书系统中学到了什么。 可在：https://medium.com/mit-media-lab/what-we-learned-从-设计-的学术-证书系统上最Blockchain-34ba5874f196

马耳他教育和就业部（2017年）。新闻稿可在：https://www.gov.mt/en/Government/Press%20Releases/Pages/2017/January/24/PR170153.aspx

Morabito，V.（2017）。通过区块链实现业务创新。B3视角。斯普林格。

Nakomoto，S。（2013）。比特币：一个对等的电子现金系统。可在：https://bitcoin.org/bitcoin.pdf

纽曼，P.（2017）。物联网报告中的区块链。分布式账本如何通过更好的可见性和创建信任来增强物联网。商业智能报告。

Peters，GW，Panayi，E。和Chapelle，E.，（2015），加密货币和区块链技术的趋势：货币理论和监管观点。金融观点杂志：金融科技。2015年冬季，第3卷 - 第3期。

Peters，GW，&Panayi，E。（2016）。通过区块链技术了解现代银行账户：货币互联网上的交易处理和智能合约的未来。在P. Tasca，T. Aste，L. Pelizzon和N. Perony（Eds。），"超越银行和金钱的银行业：二十一世纪银行业务指南"（第239-278页）。湛：斯普林格国际出版社。https://doi.org/10.1007/978-3-319-42448-4_13

Piscini，E.，Guastella，J.，Rozman，A。和Nassim，T。（2016）。区块链：民主化的信任。分布式账本和价值的未来。德勤大学出版社。可在：https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology/deloitte-uk-科技的发展趋势，2016 blockchain.pdf

Ryan，P。（2017）。我们需要弄清楚如何正确使用区块链。这就是为什么。可在：https://www.weforum.org/agenda/2017/06/Blockchain-is-stalling-but- 什么保持，它向上

Rzepecki，L。（2017）。区块链，电子签名和PKI / EIDAS有什么区别？可在：https://www.quora.com/What-is-the-difference-between-block- 链电子签名和PKI-EIDAS

Pocius，D.，Vaikutyte-Paskauske，J.，Ravaioli，S.，Dumcius，R.，Saduikis，K.，Buinauskas，D.（2017）。研究审查文凭补充的修订和分析可行性的它的数字化在欧洲的水平。可得到在：https://publications.europa.eu/en/publication-detail/-/publication/1ae19aac-6a9a-11e7-b2f2-01aa75ed71a1 /语言EN /格式PDF /源32160429

Russell，J。（2017）。索尼希望使用区块链数字化教育记录。可在：https://techcrunch.com/2017/08/09/sony-education-blockchain

Schmidt，JP（2015）。证书，声望和区块链。可在：https://medium.com/mit-media-lab/certificates-reputation-and-the-blockchain- aee03622426f

Schmidt，JP（2017）。证书，声誉和区块链。可在：http://er.educause.edu/articles/2017/4/credentials-reputation-and-the-Blockchain

Shrier，D.，Wu，W.，Pentland，A。（2016）。麻省理工学院。区块链和基础设施（身份，数据安全）。可在：https://cdn.www.getsmarter.com/career-advice/wp- 内容/上传/ 2016/12 / mit_Blockchain_and_infrastructure_report.pdf

Siebold，S.和Samman，G.共识。价值互联网不可动摇的协议（2016）。毕马威会计师事务所。可得到在：https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-Blockchain-consensus-mechanism.pdf

Smolenski，N。（2016a）。数字分权时代的学术证书。学习机研究。

Smolenski，N。（2016b）。 身份与数字自主权。 一个新的公海主权范式。 可在：https://medium.com/learning-machine- 博客/身份和数字自主权，1f3faab7d9e3

斯摩棱斯基，N. (2017a). Blockchain 记录 对于 难民。 可得到在：https://medium.com/learning-machine-blog/Blockchain-records-for-refugees- bd27ad6e6da1

Smolenski，N.（2017b）。 欧盟一般数据保护条例和区块链。 可在：https://medium.com/learning-machine-blog/the-eu-general-data- 保护监管和最blockchain-1f1d20d24951

索尼（2016）。 全球教育使用区块链技术开发学术能力和进步记录公开分享。 可在：https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html

斯坦利，答（2017年）。 Consensys，毛里求斯国家在谈判创造"以太坊岛"可在：http://www.coindesk.com/consensys-nation-mauritius-talks-create- 复仇岛

Staples，M.，Chen，S.Falamanski，S.，Ponomarev，A.，Rimba，P.，Tran，AP，Weber，I.，Xu，X.，Zhu，J。（2017）。 使用区块链和智能合约的系统的风险和机遇。 堪培拉。 英联邦科学和工业研究组织。

Stockton，N.（2017）。 用区块链拯救环境的奇妙计划。 可在：https://www.wired.com/2017/05/curious-plan-save-environment- Blockchain

Tapscott，D。和Tapscott，A.（2017a）。 区块链革命与高等教育。 可在：http://er.educause.edu/articles/2017/3/the-Blockchain-revolution-and- 高等教育

Tapscott，D。和Tapscott，A.（2017b）。 实现区块链的潜力。 管理区块链和加密货币的多利益相关方方法。 可在：http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

Torverkar，G。和Moskowtiz D.（2017）Indorse White Paper。 V 1.0。 可在：https://indorse.io/static/media/Indorse-Whitepaper-v1.0.869d6b72.pdf

"经济学人"（2017）。 政府可能是区块链的大支持者。 可在：http://www.economist.com/news/business/21722869-anti-establishment-technology- 脸讽刺点亮是算命的政府，可待大支持者

经济学家Babbage科学播客：数字自主权。 可在：https://soundcloud.com/theeconomist/babbage-send-in-the- microbots？utm_source =的SoundCloud

Technavio（2017）。 全球学生信息系统市场2017-2021。

汤普森，斯蒂芬。 "保护区块链上的数字签名"另见：UBC iSchool学生日记。 3（2017）。 可在：http://ojs.library.ubc.ca/index.php/seealso/article/view/188841/186526

尼科西亚大学（2017年）。 比特币区块链上的自我验证证书 https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on- 在-比特币，Blockchain

Vian，K.（2016）。 自己的成就：区块链技术的三种方式正在破坏教育。 可在：https://Blockchainfutureslab.wordpress.com/2016/03/16/own- 您-成就，三方面-Blockchain高科技-IS-破坏教育

Vigna，J.和Casey，MJ（2016）。 Cryptocurrency时代：比特币和区块链如何挑战全球经济秩序。 皮卡多尔。

Watterson，A.（2016）。 教育区块链：简介。 可在：http://hackeducation.com/2016/04/07/Blockchain-education-guide

维基共享资源（2017，“File：Hash function.svg”，维基共享资源，免费的媒体资源库。 https://commons.wikimedia.org/w/index.php?title=File:Hash_function.svg&oldid=172142077

威尔逊 S.（2016）. Blockchain 真 只要 不 一 事情 好。 可得到在：https://theconversation.com/Blockchain-really-only-does-one-thing-well-62668

Winjum，JO（1971）。 “会计与资本主义的兴起：会计的观点”会计研究会刊：333-350。

Witthaus，G.，Inamorato dos Santos，A.，Childs，M.，Tannhäuser，A.，Conole，G.，Nkuyubwatsi，B.，Punie，Y.（2016）。 验证非正式的基于MOOC的学习。 欧洲评估与认可实践分析（OpenCred）。 JRC科学政策报告。

Wong，JI（2017）。 微软认为区块链技术可以解决互联网最棘手的问题之一：数字身份。 可在：https://qz.com/989761/microsoft- MSFT-认为，Blockchain高科技，可以求解的一-的最互联网络，最棘手的-问题 - 数字 - 身份

世界经济论坛（2015）。 深移技术临界点和社会影响。 可在：http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.PDF#页= 24

Yamey，BS（1949）。 科学记账与资本主义崛起。 经济史评论，1（2-3），99-113。 https://doi.org/10.1111/j.1468-0289.1949.tb00108.x

12.3 网站Blockcerts.org

Blockcerts.ehcoo.com

Blockchain.open.ac.uk

Blockchain.mit.edu

Blockchain-lab.org

Blockchainpilots.nl/home-eng

Certificates.media.mit.edu

Community.blockcerts.org

网站导航

Hyperledger.org

ibm.com/Blockchain

openbadges.org

Tierion.com

Wiki.P2Pfoundation.net/Blockchain

12.4 影片

ASU GSV峰会，（2017）。 信任但验证：块链 - 作为货币的知识。 可在：
https://www.youtube.com/watch?v=x6TDCTiUO9M

Brownworth，A.（2016）。 区块链如何工作 可在：
https://www.youtube.com/watch?v= 160oMzblY8

Clark，D。（2016）。 OEB2016区块链教育。 可在：
https://www.youtube.com/watch?v=0ZYnPDirJmA

CNBC。 什么是区块链？ 可在：
https://www.youtube.com/watch?v=8o9QxMxhTp8

De Filippi，P.（2017）。 区块链革命。 Meetup达索系统。 可在：
https://www.youtube.com/watch?v=3ukEXQ66_ss

英国政府科学办公室（2016年）。 块链技术。 可在：
https://www.youtube.com/watch?v=4sm5LNqL5j0&feature=youtu.be

未来思想家（2017）。 区块链将会扰乱的19个行业 可在：
https://www.youtube.com/watch?v=G3psxs3qyf8

古普塔 V.（2017）. 欧洲的 议会 Blockchain 介绍。 可得到在：https://www.youtube.com/watch?v=fCYT9KWoldI

IBM开发人员视频（2017年）。 可在：
https://www.youtube.com/channel/UCpEJ53BOa9YWTTXerZtKNhg/videos

IBM Think Academy (2017)。 区块链，它是如何工作的。 可在：
https://www.youtube.com/watch?v=lD9KAnkZUjU

Inamorato dos Santos, A. (2017) Blockchain in Education - 欧盟委员会的JRC报告预览，格罗宁根教育会议区块链。 可在http://bit.ly/2lsyvDb

Mesropyan, E. (2017)。 21家公司利用区块链进行身份管理和身份验证。 可在：
https://letstalkpayments.com/22-companies- 利用-blockchain换身份管理和认证

Perry, RE (2017)。 区块链技术：从炒作到现实。 可在：
https://www.youtube.com/watch?v=v--lqndp0V4

Rosic, A. (2017)。 什么是以太坊？ 一个简单的解释任何人都可以理解。 可在：
https://www.youtube.com/watch?v=ptLfwp6JYgk

Rosic, A. (2017)。 什么是智能合约？ 初学者指南。 可在：
https://www.youtube.com/watch?v=qdoUpGg_DpQ

Stagars, M. (2017) 区块链和我们。 可在：
https://www.youtube.com/watch?v=2iF73cybTBs

Tapscott, 答 (2016) 区块链革命。 在谷歌会谈。 可在：
https://www.youtube.com/watch?v=3PdO7zVqOwc

缩略语列表

AWS 亚马逊网络服务

CEN 欧洲标准化委员会CPD 持续专业发展DAO

分布式自治组织DLT 分布式账本技术

IPFS InterPlanetary文件系统

ISO 国际标准化组织FINTECH 金融与科技的融合

KMI 英国开放大学知识媒体研究所 学习机

MCAST 马耳他艺术科学与技术学院 麻省理工学院

MOOC 大规模开放在线课程非政府组织 非

政府组织P2P 点对点

PKI 公钥基础设施

TSA 信任的权威SaaS 软件即

服务中心 尼科西亚大学

定义列表

为了本研究的目的，我们使用以下定义：

认证是指通过私钥/公钥来证明对方身份和资产的存在的过程。

徽章是指成就，能力，技能或品质的象征或指标。 这与学校毕业后参加活动或圆满完成课程的证书类似。 数字徽章是一个图像文件，可以轻松共享。 此外，数字徽章在其代码中包含隐藏的加密数据，其中包含所有者的信息，来源，获得该数据所需的条件以及确认成功获取的文档链接。 因此，教育工作者，雇主和其他可能想了解更多关于学生，候选雇员或志愿者的人员都可以获得表演任务，标准和证据。

BADGR是一个免费的开源成果识别和跟踪系统，用于发布，组织和分享开放式徽章。

比特币是指一个名叫Satoshi Nakamoto的未知程序员或一群程序员发明的加密货币和数字支付系统。 它在2009年作为开源软件发布。系统是点对点的，并且交易直接发生在用户之间，没有中间人。 这些交易由网络节点验证，并记录在称为区块链的公共分布式账本中。 由于该系统没有中央存储库或单个管理员，比特币被称为第一个分散数字货币。 比特币除了被创造为挖矿的奖励外，还可以在合法或黑市交换其他货币，产品和服务。 比特币区块链的发明使其成为解决双重支出问题的第一个数字货币，而不使用可信任的权力机构或中央服务器。

区块链意味着一个分布式账本或数据库，保持不断增长的交易记录列表，并提供各种防篡改和修改保护。它是由使用它的每一方共同建立和维护的。 它由许多被称为块的条目组成，这些条目由被存储的数据组成。 这些数据块被传送给分布式账本中的合伙人，这样他们就可以由无关方面进行验证。 每个块都包含一个哈希代码，用于标识紧接在其之前的块，使这些块连续并链接在一起 - 因此称为"区块链"。 就规模而言，比特币是最大的区块链，在流行的白话方面自动关联为"区块链"。 在实践中，还有其他的区块链，比如以太坊区块链，以及公共和私人区块链。 所有区块链都有与之相关的某种数字货币。

共识机制意味着在区块链或分布式账本上验证和验证价值或交易的方法，而不需要信任或依赖中央机构。共识机制是区块链或分布式账本运作的核心。

加密货币是一种交换媒介，在区块链中以电子方式创建和存储，使用加密技术来控制货币单位的创建并验证资金的转移。 比特币和以太是最着名的例子。

密码术是指通过仲裁结构强制执行交易完整性的验证和密码验证以及通过代码进行确认的过程，而无需信任或依赖中央授权机构。

密码签名是指如果用户保持私钥签名交易安全，则毫无疑问地数学验证一个数据的所有者的方法。

分散的自治组织（DAO）是一个计算机程序，运行在一个对等网络上，包含治理和决策规则。 DAO可以编程为自主操作，无需人工干预，代码可以直接实时控制DAO及其控制的资金。 最早的DAO。

委托证明是指选择"证人"负责订购和提交交易的利益相关方，负责协调软件更新和参数变更的"代表"。

数字签名是指二进制代码，与手写签名一样，认证和执行文档并标识签名人。 数字签名实际上是不可能伪造的，不能单独发送，而只能作为电子文档或消息的一部分。 它与电子"指纹"相似，以编码信息的形式，数字签名将签名人与记录的交易中的文件安全地关联起来，数字签名采用被称为公钥基础设施（PKI）的标准接受格式，提供最高级别的安全性和普遍接受度，是电子签名（eSignature）的特定签名技术实现。

分布式账本意味着所有权的数字记录不同于传统的数据库技术，因为没有中央管理员或中央数据存储；相反，分类账在对等网络虚拟专用网中的许多不同节点之间复制，并且每个交易用私钥唯一地签名。

以太坊意味着一个运行智能合同的分散平台。 作为具有共享全球基础架构的定制区块链开发，可以移动价值并代表财产的所有权。 网络中的每个节点（计算机）都运行称为以太坊虚拟机（EVM）的操作系统。EVM理解和执行用以太坊特定编程语言编写的软件。 以太坊虚拟机执行的软件/应用程序被称为"智能合同"。

以太坊钱包意味着在以太坊区块链上分散应用的门户。 它使用户能够容纳和保护建立在以太坊上的以太网和其他加密资产，以及编写，部署和使用智能合约。

"欧洲通"意味着欧盟的一项举措，旨在帮助人们在欧洲清楚和容易地理解他们的技能和资格，从而促进学习者和工作者的流动。 Europass文件的设计方式是帮助人们以一致的方式记录他们的技能和能力，无论他们计划参加教育或培训计划，寻找工作还是获得海外经验。 Europass包含以下五个文件的组合：个人可以独立完成的两个文件 - Europass履历（CV）和Europass语言护照；由主管机构代表个人完成的三份文件 - Europass流动性，Europass证书补充和Europass文凭补充。

容错是指即使某些组件发生故障，系统也能继续正常运行的属性。

联合共识意味着实现拜占庭协议（达成共识）的一种方式，其中节点可以共享另一个节点并达成共识，而不需要直接了解所有其他节点。

创世纪区块意味着区块链中的第一个区块。

治理意味着建立一个分散的控制：没有中央主管部门的命令需要获得批准才能达成共识。 一些类型的共识机制使用一个领导验证的选举出来的领导，并维护在节点之间共享的数据。 治理方面还包括允许的网络中的节点的入职和离职。

减半意味着比特币的供应有限，这使得它们成为稀缺的数字商品。 将要发行的比特币总量为2100万。 每块产生的比特数每四年下降50%。 这就是所谓的"减半"，最后的减半将在2140年进行。

哈希函数意味着应用程序编程接口通过称为散列的过程为每个文件创建唯一的密钥或数字指纹。 密码哈希（如SHA256计算算法）确保对事务输入的任何更改（即使是最微小的更改）都会导致计算出不同的哈希值，这表示可能会损害事务输入。

哈希率意味着比特币矿工在给定的时间内（通常是一秒钟）可以执行的哈希数。

分层确定性密钥意味着从称为种子的单个起始点推导密钥的系统。 种子允许用户在不需要任何其他信息的情况下容易地备份和恢复钱包，并且在某些情况下允许在不知道私钥的情况下创建公共地址。

不变性意味着不可改变。 一个不可变的对象（不可改变的对象）是一个对象，它的状态在创建后不能被修改。 区块链数据实际上不能轻易改变，因为它在不同的地点和组织中不断被复制。 区块链显而易见试图在一个地方改变它将被解释为欺诈，并被其他参与者的完整性攻击，并将被拒绝。

Interledger协议意味着将过去的传统分类账与未来的分布式分类账连接起来的协议。

星际文件系统是一个协议旨在创建一个永久和分散的存储和共享文件的方法。 IPFS利用了比特币blockchain 协议以及网络基础设施，以便存储不可改变的数据，在网络上移除重复的文件，并获得访问存储节点的地址信息以搜索网络中的文件。

以领导为基础的共识意味着一种共识，在这种共识中，选举领导人并保持控制，直到表决决定新的领导人为止。 在这个模型中，它是验证事务并将数据发送到其他节点的领导者。

分类帐是指只有追加记录的商店，记录是不可变的，可能比财务记录拥有更多的一般信息。

生存意味着传输现在正在发生的数据，而不是以前发送的数据记录的重放。 通过混合不能再次复制的数字，生存被引入到安全传输中。 如果一个节点能够在没有任何失败的节点的参与的情况下将新的值外化，则它享有活力。 有些节点可能会出现故障，只要大部分节点可用，网络仍然能够运行，总体上可以达到一致的响应时间），并且还要考虑对分布越来越大的分类帐的网络带宽的影响。

Merkle树意味着多重签名；一个认证功能，允许一组用户用一个以上的私钥签名单个文档。

采矿意味着记录保存服务。 矿工通过反复验证和收集新的广播交易到一组称为一个街区的交易中来保持区块链的一致性，完整性和不变性。 每个块都包含前一个块的加密哈希，使用SHA-256哈希算法，将其链接到前一个块，从而为其提供了区块链的名称。 为了被其他网络所接受，一个新的区块必须包含一个所谓的工作证明。 工作证明要求矿工找到一个叫做随机数的数字，这样当块内容随着随机数散列时，结果在数值上比网络的难度目标要小。 这个证明对于网络中的任何节点来说都是很容易验证的，但是对于一个安全的加密哈希来说，生成是非常耗时的，矿工必须

尝试许多不同的nonce值（通常测试值的顺序为0,1,2,3，...），每遇到2016年的阻塞（大约14天），根据网络的最近性能调整难度目标，目的是在十分钟之间保持新区间的平均时间，从而使系统自动适应网络上的总采矿量，证明工作系统和区块链一起， Blockchain非常困难，因为攻击者必须修改所有后续块，以便接受一个块的修改。随着新的块一直被挖掘，修改块的难度随着时间的推移而增加，随后的块的数量（也称为给定块的确认）增加。

网络协议意味着正式的标准和政策，包括定义两个或更多设备之间通过网络进行通信的规则，程序和格式。 网络协议管理及时，安全和管理的数据或网络通信的端到端流程。

节点是指共识网络的成员或系统； 一个持有分类账副本的服务器； 可以具有不同的角色：发布，验证，接收，通知等。对于所有意图和目的，节点可以是VM实例。

节点到节点（N2N）是指一个机制，其中只有两个节点参与交易；实际上它避开了传统的共识机制。

开放标准是指由所有愿意加入的组织管理的非专有协议或规范，如ISO标准。

参与者是指可以访问分类帐的演员：读取记录或向其中添加记录。

同侪是指为维护分类账的身份和完整性而共同承担责任的行为者。

点对点（P2）网络是指在对等点之间共享任务，工作或文件的计算机或网络的体系结构。 同行在网络中是环境中的平等特权和权力的合作伙伴。 在P2P网络中，每个计算机或用户被称为"节点"，并且它们共同构成节点的P2P网络。 区块链中的P2P网络由一系列计算机和服务器组成，每个计算机和服务器都充当网络中的一个节点。 区块链网络可以是权限许可的，也可以是无权限的。

许可是指用户设置有关访问，共识机制，治理，参与等规则的专用网络。许可网络仅限于给定业务网络内的参与者。 在经过许可的区块链上，参与者只能查看与其相关的交易。

Permissionless意味着一个对任何参与者都开放的网络，在这种网络中，事务是根据网络中已有的规则进行验证的。 任何参与者都可以查看分类帐上的交易，即使参与者是匿名的。 比特币是无权限网络最熟悉的例子。

许可账本是指参与者必须有权访问账本的分类帐。 允许的分类帐可能有一个或多个所有者。 当添加新记录时，分类账的完整性将通过有限的共识流程进行检查。 这是由信任的行为者（例如政府部门或银行）执行的，这使得维持一个共享记录要简单得多，以至于未被许可的分类账使用的共识过程。 允许的区块链提供了高度可验证的数据集，因为共识流程创建了数字签名，各方都可以看到。 许可分类账通常比无权限分类账更快。

隐私意味着确保只有预期的接收者可以阅读该消息。 计算密码学领域通过在任何应用到应用通信的上下文中使用针对特定安全通信要求的数学公式来解决分布式共识的许多安全和隐私问题。

私密区块链意味着一个区块链与一个共识算法，只允许预先选定的一群人贡献和维护区块链的完整性的限制读/写访问。 私人区块链也可以指由私有实体或联盟运营的区块链，没有或仅限于其他方的访问，并且通常具有少量（数十个或数百个）处理节点来操作区块链。 在这种情况下，与公共区块链相比，技术优化可以用来改善区块链的延迟和吞吐量，BFT共识机制可以用来为交易完成提供更强的保证。

私人货币是指由私人或公司发行的货币，通常以无保险资产作抵押。

私钥意味着私钥是一串数据，表明您可以访问特定钱包中的比特币。 私钥可以被认为是一个密码；私人钥匙绝不能透露给任何人，除了你，因为他们允许你通过加密签名从你的比特币钱包里支付比特币。

私钥是指唯一链接到所有者的加密密钥，只有交易双方才知道。 它是秘密地在一个数字钱包里。

专有共识机制是指本质上独特的共识模式，可能或不可能基于任何现有的共识算法。 网络中节点用来交换消息断言的风格和阶段（在技术上可以通过（节点）领导者选举，领导者类型，验证事务的方法，容错级别，令牌的使用，严格性算法，活性保证和权限管理）

公共区块链是指任何人都可以通过阅读数据，提交交易和参与验证过程来参与的网络。 公共区块链作为公共对等系统运行。 各方通常使用假名公钥/私钥进行识别，Nakamoto共识的形式通常用于允许大量（数千个）处理节点操作区块链。

公钥是指其他钱包发送交易价值的公共地址。

公钥基础设施（PKI）是指使用公钥加密（PKC）的安全数据传输和身份验证系统。

远程程序调用是指一个程序可以用来从位于网络中另一台计算机上的程序请求服务的协议，而不必了解网络细节，有时也称为函数调用或子例程调用

循环意味着节点轮流成为领导者的共识机制。

可扩展性意味着能够应对和执行不断增加的吞吐量，并在通过更大的操作需求进行测试时保持甚至提高其性能或效率水平。 延迟是交易处理的延迟

安全或分布式账本安全是指保护和保护商业和个人数据以及交易信息的过程。 在非拜占庭式的失败下，结果的确认应该是正确的。 还包括完整性（向接收节点保证接收到的消息没有以任何方式改变）和不可否认（一种证明发送节点确实发送该消息的机制）。 安全性可以包括数字签名作为一项功能

侧链是指资产从一个机制转移到一个单独的"挂钩"机制；专用账本。

智能合同意味着在定制区块链上运行的应用程序，完全按照程序设计，不存在宕机，审查，欺诈或第三方干扰的可能性。

吞吐量意味着衡量一定时间内可以处理多少交易

标志化是指用唯一的标识符号替换敏感数据的过程，这些标识符保留了有关数据的所有重要信息，而不会影响其安全性

电子钱包是指商店提供交易比特币所需的信息。 虽然钱包通常被描述为持有或存储比特币的地方，但由于系统的性质，比特币与区块链交易分类账是分不开的。 描述一个钱包的更好的方法是"存储你的比特币资产的数字证书"，并允许你访问（并花费）它们。 比特币使用公钥密码学，其中生成两个密钥，一个公钥和一个私钥。 从最基本的角度来说，钱包就是这些钥匙的集合。 有几种类型的钱包。 软件钱包连接到网络，并允许消费比特币，除了持有证明所有权的证书。 软件钱包可以进一步分为两类：完整客户端和轻量级客户端。 以太坊区块链使用不同的工作证明散列函数（Ethhash），并支持图灵完整的脚本执行。 任何愿意付钱执行的脚本都可以运行在以太坊之上。 这与比特币相反，比特币使用SHA-256哈希函数进行工作证明，并支持非常有限的一组脚本指令

附件1：教育之后的潜在区块链应用

区块链技术代表了一种全新的业务交易方式。 他们迎来了一个强大而又聪明的下一代应用程序，用于注册和交换物理，虚拟，有形和无形资产。 由于密码安全，分散共识和共享公共账本（拥有适当的控制权和可视性）的关键概念，区块链技术可以深刻地改变我们组织经济，社会，政治和科学活动的方式。

表3重点介绍了一些可以从区块链技术中受益的用例：

表3：超越教育和电子政府的特定领域的潜在区块链应用

受Blockchain影响的域名	潜在的区块链应用程序
物联网	设备管理（付款，目录，操作等）；电网监测；智能家居办公室管理；跨公司维护市场。
卫生保健	电子病历；病毒库；种子库备份；医生 – 供应商RFP服务和保证合同；区块链健康研究公用事业；区块链健康公证
金融服务	信用证；公司债务和债券；交易平台；交易发起；证券采购 股票；固定收入；衍生品交易；退货交换；抵押品管理；付款汇款；回购协议；外汇；价值转移；了解你的客户；反洗钱；客户和产品参考数据；集资；点对点贷款；合规报告；贸易金融；风险可视化；博彩；预测市场；资本资产管理。
支付	小额支付；企业对企业的国际汇款；税务申报和征收；钱包和个人银行业务。
保险	索赔处理； P2P保险；所有权标题；销售和承销；财产支付；欺诈预测和预防。
政府	电子政务 （各种） 包含 政府 招标程序；表决；税收等
产业	制造过程
零售	忠诚点
媒体	数字版权管理；游戏货币化；购买和使用监控；购票；追踪风扇 广告点击欺诈预防；实时拍卖 广告展示位置
身份管理	个人；对象；对象家族；数字资产；多因素认证；难民跟踪；购买和审查跟踪；雇主和员工的评论
计算机科学	工作现代化；支付工作；直接付款；付款API；公证和认证；点对点存储和计算共享；域名服务。

资产标题	各个
消费者	数字奖励；分享经济；对等销售；跨公司品牌和忠诚度跟踪。
供应链	贸易金融；商品定价；供货实时拍卖；药物跟踪和纯度；农业食物来源追踪；航运和物流管理；航运和物流管理；预防诈骗。
资源	能源，废物和水管理；资源提取和组帧；环境监测；工业运营。

来源：改编自IBM（2017）和专有资源

附件2：权力下放网络

从技术的角度来看，区块链是一个面向网络的软件实现。 它将代码执行和数据存储的风险和责任从集中式机器转移到分散式网络。 Batchu（2017）改编的下表总结了区块链技术的三个组成部分，这三个组成部分实现了分散式网络。

对权力下放的贡献	区块链如何有助于分权
参与节点的无可比拟的共识 *分布式计算的基本问题是在出现故障的玩家的情况下，实现系统的可靠性和完整性*	区块链为使用加密散列函数的分散网络共识提供了解决方案。 它开发了适用于不同控制级别，延迟，安全性和透明度的不同集合的一致性算法的不同风格： — 工作证明，强大处理能力的可靠性主要偏好于高度安全的网络。 — 网络忠诚的利益相关者的可靠性和可靠性，这有助于避免能源浪费。 — 指定签署者，被认为是具有严格访问控制的高性能网络。 — 许可，适用于企业解决方案和行业会计标准化。 — 许可，强大的公共项目协助互动和交易模式。
保持共同的事实 *真相是企业或公共组织的基本要素，包括政府*	区块链引入了一种创新的机制来保存数字共享真相的来源，这个机制通过一个按时间顺序链接的块来保存交易信息，这个信息总是指前一个块。 区块链引入了一种保留"数字共享真相"出处的创新机制。 实现安全共享真相的三大创新实现是： a）以交易为基础的分类帐 – 使用单一来源（同意创始块）验证分类帐数据变得容易，并提供了交叉验证标记所有权的突变记录的额外功能。

	b) 块级激励 – 使模块化，开放和竞争参与，保持系统的安全和运行。 c) 不变性和块确认 – 反向引用前面的块不断增加安全层，每个块都由网络确认，并且使得在这些块内部进行反向工程或更改元数据实际上是不可能的。 通过这些技术的结合，区块链实现了一个安全，透明，不可变的真相存储库，旨在高度抵抗中断，操作和不必要的复杂性。
分散执行程序 *代码执行的分散编排是应用程序效率和性能的关键*	除了分类账，区块链还引入了一种新的方式来协调计算机程序的开放和分散执行。 这背后的关键技术可能是： — 脚本功能 – 标准化的汇编代码语言，在逻辑范围内协调一致的节点，有助于设计复杂的可接受事务。 — 智能合同 – 自主软件代码，可以帮助建立独立运行的大型商业逻辑。 软件执行的独立性使数据和决策过程具有完全的自主性。 在oracle网络（自主硬件采集激励模型数据点）的帮助下，我们即将目睹完全自主的工业规模系统。

附件3：关键区块链技术概述

不同的区块链可能被用来存储不同类型的记录。 区块链在用户访问它们的权限，使用的数据结构和用于达成一致的机制中也可能有所不同。 本节概述了当前正在使用的主要区块链。

比特币

比特币是基于密码证明而不是信任的电子支付系统，允许任何两个自愿的双方直接相互处理，而不需要可信的第三方（Nakamoto，2013）。 发明人是本名志聪（Satoshi Nakomoto）发明的，它是区块链技术的首次实现，而今天比特币网络仍然是目前最大的公共区块链。

比特币是在线等值的现金。 现金通过其外观和特征进行鉴定，在通过序列号和其他安全装置进行纸币的情况下。 然而，在现金的情况下，没有记录交易的分类账，并且伪币既有硬币也有钞票。 在比特币的情况下，交易账本确保其真实性。 硬币和比特币都需要分别安全地存储在实际或虚拟钱包中 - 如果这些钱币没有得到适当的照顾，硬币和比特币可能会被盗用（英国政府，2016年）。

由于一项功能允许它在每笔交易中存储多达80个字符的字符串，比特币区块链也被用作公共注册来存储文件的散列。 这反过来又能启用防篡改的数字签名，如6.3节所述。

比特币是一个完全开源的项目，因此受比特币用户社区的管理。 比特币软件，协议和区块链的更新在网络中超过一半的计算机选择切换到新版本的软件时被接受。

比特币区块链有一些局限性：

- 它只能存储发送者，接收者，现金转移金额和散列。
- 它每秒只能处理少于10个交易（与典型信用卡网络的数万个交易相比），这是一个已经达到的限制。
- 它的规模正在成倍增长，导致只有具有大量计算能力的用户才能保留整个区块链的副本，减少网络中的计算机数量，并且整体上降低安全性。

复仇

以太坊是一个分散的平台，运行智能合约 - 应用程序完全按照程序运行，没有任何停机，审查，欺诈或第三方干扰的可能性。 这些应用程序存储并在定制的区块链上运行。

以太坊使开发者能够创造市场，存储债务或承诺的注册，按照过去很长时间的指示（如遗嘱或期货合同）以及许多其他尚未发明的东西来转移资金 - 所有这些都没有一个中间人或交易对手风险（以太坊基金会，2017）[89]。

以太坊允许用户启动他们自己的加密货币，加密货币中的每个"标记"可以表示任何东西，包括资产，学习单元，股票，

(89) 有关快速概览，请参阅https://hackernoon.com/wtf-is-ethereum-c65e0d67ac09

证书，成员资格，引用等。因此，以太坊大大增加了区块链可以使用的应用程序的数量。

而且，以太坊可以每秒处理更多的事务，并且可以存储在其上的数据的数量和种类更加灵活。

Ethereum也是一个开源项目，它由Ethereum企业联盟支持，Ethereum企业联盟将埃森哲，微软，三星，德勤等40多家大公司以及全球几家最大的银行聚集在一起。 该联盟不断更新以太坊路线图，并为项目贡献代码。

其他区块链

虽然比特币和以太坊区块链是两个主要的区块链，Smith&Crown是一家专门的区块链研究咨询公司，在撰写本文时，还有大约30个其他公共区块链可用，另有100多个区块链正在启动。 这些区块链中的许多包含适合特定用途的数据结构或验证机制，包括注册知识产权，交易特定种类的资产，游戏，存储身份等等。

这些区块链中的大部分都是通过"初始硬币发行"（Initial Coin Offerings）获得资金支持的，因此将通过区块链进行交易的代币销售给公众，作为筹集启动资金的一种方式。

此外，许多公司或集团公司可能会选择运行私人区块链来交易特定类别的资产。

技术提供者

技术巨头IBM和微软目前正在大力投资区块链解决方案[90]。 两家公司都部署了类似的三叉战略：

- 为客户提供使用IBM或Microsoft云计算产品推出自己的私人区块链的能力；
- 在公共区块链之上构建应用程序，尤其是向智能合约提供存储或数据服务，以确定是否满足其条件；
- 推动公共区块链（特别是以太坊区块链）的代码，以帮助推动技术向前发展。

微软

2017年3月，微软宣布扩大其在Azure上的区块链支持，成为第一个允许多成员联盟区块链网络解决需要部署专用网络的公共云的公共云。 在一篇文章[91]中，微软表示，它将场景分为三种“常见拓扑”：

1. 单一组织，多个订阅：当组织中的部门之间不相互信任时，例如当一个部门正在审计另一个部门时，这是一种常见的拓扑。

2. 多个组织，私人的：这是真正的联盟情景，每个组织都有自己的足迹，但部署的服务不能在互联网上公开访问，即使通信将发生在组织之间。

---

(90) 看到https://www.coindesk.com/ibm-vs-microsoft-two-tech-giants-two-blockchain-visions/

(91) 看到https://azure.microsoft.com/en-us/blog/multi-member-consortium-blockchain-networks-on-azure/

3. 面向公众的多个组织：类似于上述拓扑，但在IT要求允许或要求部署的服务可通过互联网公众访问的行业，企业或方案中。

微软的Bletchley项目[92]概述了该组织对Azure支持的开放式模块化区块链结构的展望，并强调了我们认为是企业区块链体系结构中关键的新元素。 2017年8月13日，微软推出了一款新的基于区块链的框架，名为Coco，旨在帮助企业构建和扩展基于区块链的企业网络[93]。

IBM

IBM还开发了自己的称为Hyperledger[94]的区块链技术。 Hyperledger是为推动跨行业区块链技术而开发的开源协作工作。 这是由Linux基金会主办的全球协作，包括金融，银行，物联网，供应链，制造和技术领域的领导者。 这些130多个成员和8个正在进行的项目，包括Hyperledger Fabric和Hyperledger Composer，共同创建了一个开放的，标准化的企业级分布式账本框架和代码库。

> *如果我们认为区块链只是一种分布式技术，它是否可以处理撤销，所有权变更以及当前被视为"真相"的变化？ 事实的真正解决可能存在于一个堆栈中。 堆栈是您需要证明的核心内容 - 证书，股票 - 数字签名。 然后你进入另一个级别的认证 - 你通过一个信任链。 您以不同的方式验证堆栈的每个级别。 如果你有一个自我主权的认证水平证明我的身份 - 如果我可以让我的银行证明我的身份 - 我们有一些有趣的东西。 载体是个人，他们的身份和交易。 (Gray，2017)*

> *"也许比特币区块链受到缺乏灵活性和性能的阻碍，以太坊还有其他弱点 - 比如多面语言的稳固性。*

---

(92) *看到*https://github.com/Azure/azure-blockchain-projects/tree/master/bletchley

(93) 据微软称，Coco的建立是为了加速交易速度，简化公司区块链网络的治理，并将与多个开源的区块链和分布式账本相集成，其中包括以太坊，R3的Corda，Hyperledger Sawtooth和摩根大通专有的以太坊法定区块链。 微软声称，Coco可以启用区块链在以太坊区块链的私有版本上每秒处理多达1,700个交易，相比之下，在没有整合的情况下，每秒钟可处理约13个交易。 Coco还包括一个内置的治理工具，使区块链参与者能够对其网络的所有条款和条件进行投票，例如可以添加或删除成员。 微软表示，这简化了治理程序，从而加快了交易速度。 摩根大通（JP Morgan）发言人证实，该行将于明年启动时将可可纳入法定人数，以加强区块链的速度和安全性。

请参阅公告：https://www.coindesk.com/coco-revealed-microsoft-jpmorgan-demo-new- blockchain 助力高科技/

请参阅白皮书：https://github.com/Azure/coco- 框架/斑点/ 46596b4cb83ad759cd6dd8fd1cd5bce1629f3d3b /文档/可可%20Framework%20whitepape r.pdf

(94) 看到https://www.hyperledger.org/wp- 内容/上传/ 2017年/ 08 / Hyperledger_Arch_WG_Paper_1_Consensus.pdf

建立替代这些。 香港有B2 Chain，RChange，可扩展的区块链 - 有趣的想法试图成为概念的证明，但将其他共识机制提升到更高层次。 有混合区块链出现。 IBM的Hyperledger可以构建上面的私有区块链。 微软正在试图建立一个免费提供的链条，他们的身份项目正在与以太坊联盟以及比特币上的Blockcstack合作。 以太坊有能力建立私人连锁。 现在实验足够好了。 如果你不能在比特币区块链上扩大规模，那就建立一个私人链条，但是要准备在某个阶段转移到一个没有权限的链条上。

我们可以做的是在我们的解决方案中建立互操作性。 解决方案不是区块链或以太网能否成为赢家，而是我们能否实现一个不受信任，许可的未来的承诺" (Casey, 2017)

欧洲直通是一项服务，可以帮助您找到有关欧盟的问题的答案。

免费电话号码（*）：

00 800 6 7 8 9 10 11

(*) 所提供的信息是免费的，大多数电话都是免费的（尽管有些运营商，电话亭或酒店可能会收取费用）。

有关欧盟的更多信息可在互联网上找到（http://europa.eu）.

如何获得欧盟出版物

免费出版物：

- 一个副本：
  通过欧盟书店（http://bookshop.europa.eu）；
- 多个副本或海报/地图：
  来自欧盟的交涉http://ec.europa.eu/represent_en.htm）；来自非欧盟国家的代表团 http://eeas.europa.eu/delegations/index_en.htm）；通过联系欧洲直接服务（http://europa.eu/europedirect/index_en.htm）或拨打00 800 6 7 8 9 10 11（欧盟任何地方的免费电话号码）（*）。

  (*) 所提供的信息是免费的，大多数电话都是免费的（尽管有些运营商，电话亭或酒店可能会收取费用）。

定价出版物：

- 通过欧盟书店（http://bookshop.europa.eu）.

KJ-NA-28778-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

DOI: 10.2760 / 60649

ISBN 978-92-79-73497-7