



Government
Office for Science

万向区块链实验室 编译



分布式账本技术：超越区块链 Distributed Ledger Technology: beyond block chain

关注微信公众号“区块链铅笔”
Blockchain”，回复关键词“帮助”，
查看下载更多报告和白皮书

英国政府首席科学顾问报告
A report by the UK Government Chief Scientific Adviser





目 录

前言	4
概要及建议	5
定义	17
第一章 视野	21
第二章 技术	31
第三章 治理和监管	38
第四章 安全性和隐私性	44
第五章 颠覆性潜力	50
第六章 政府中的应用	61
第七章 全球视野	70
万向区块链实验室介绍	83
铅笔 ChainB	85

翻译：

暴走恭亲王，Kyle，杜宇，丁磊，高素质蓝领

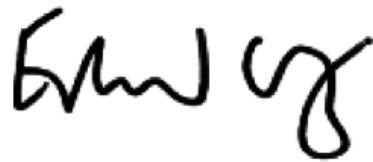
前言

人类的进步是由新技术的诞生及由此释放出来的人类智慧为标志的。

在分布式账本技术中，我们可能正见证着一些可能带来创新潜力爆发的例子，它的催化效应可能会带来不同寻常的创新成果。这个技术有可能为多种服务提供一种新型的信任机制。就如信息公开重塑了公民与国家之间的关系一样，这些技术带来的透明度将有可能改革我们的金融市场、供应链、消费者与 B2B 服务以及上市公司的注册等。

随着分布式账本技术的成熟和改变我们对数据及其储存方式的了解，我们明白这将会带来一些挑战。英国处于一个独特的位置，可以去探索这些挑战并让这种技术给我们的公共服务与经济带来最大的益处。我们已经有了世界级的数字技术处理能力、不断创新的金融服务、一个强大的研究社区以及不断增长的私营部门的经验。当中很关键的是包含阿兰·图灵研究所(Alan Turing Institute)、开放数据学院(Open Data institute)以及数字加速中心(Digital Catapult)在内的机构都是我们的重要资产，它们需要与私营部门以及全球的伙伴一起工作，将这项技术的潜力发挥到极致。（译者注：以上提到的三个机构都是英国著名的数字技术研究机构）

因此，我们两人很高兴成为这个领域里的共同先行者。我们期待与其他部门一起抓住这个机会，同时也试图了解这项技术如何能为英国公民以及经济服务。



MATTHEW HANCOCK 议员阁下
内閣部长及财政部主计长

ED VAIZEY 议员阁下
主管文化及数字经济的国务大臣



概要及建议

引言

使得分布式账本技术产生的算法是一种强大的、具有颠覆性的创新，它有机会变革公共与私营服务的实现方式，并通过广泛的应用场景去提高生产力。

账本从久远的年代开始就是商业活动的核心要素之一，并用于记录很多事情——最常见的是用于记录像金钱和产权这样的资产。这些数据记录的介质从泥板到纸莎草，再到牛皮纸和纸张，一直在进化。不过这么以来，数据的电子计算机化是在这个领域的唯一显著的创新发明，这在一开始是简单地将纸质数据变成电子数据。现在，计算机算法首次让协作维护的数字分布式账本成为可能，这种账本具有超越传统纸质账本的属性和能力。

分布式账本，从实质上说就是一个可以在多个站点、不同地理位置或者多个机构组成的网络里进行分享的资产数据库。在一个网络里的参与者可以获得一个唯一、真实账本的副本。账本里的任何改动都会在所有的副本中被反映出来，反应时间会在几分钟甚至是几秒内。在这个账本里存储的资产可以是金融、法律定义上的、实体的或是电子的资产。在这个账本里存储的资产的安全性和准确性是通过公私钥以及签名的使用去控制账本的访问权，从而实现密码学基础上的维护。根据网络中达成共识的规则，账本中的记录可以由一个、一些或者是所有参与者共同进行更新。

区块链是这种分布式账本的底层技术，它最初是为了在 2008 年实现的点对点数字现金系统比特币而设计的。区块链算法让比特币的交易可以在“区块”里集中起来，并通过密码学签名添加到现有区块组成的“链”里面。比特币账本是用分布式及“无需许可”的方式构建的，任何人都可以通过解决生成新区块所需的密码学难题从而添加一个包含交易的区块。现时，这个系统的鼓励机制是在解决难题并生成每个区块后得到的 25 个比特币的奖励。任何人只要有网络和电脑的算力，都有机会解决这些密码学难题并将交易添加到账本里，这些人被称为“比特币矿工”。挖矿的比喻是很恰当的，因为比特币的挖掘是要消耗大量的电脑运算能力的，因此会带来很高的能源消耗。据估计，比特币网络运行所需的能源超过 1GW（十亿瓦特），可以与爱尔兰的电力消耗相提并论了。

比特币就像是网络上的现金一样。人们是通过物理上的外观及特征去校验现金的真伪的，而在钞票的例子，则是通过序列号以及其他的一些安全设备去实现这个目的。不过在现金的例子，并没有一个用于记录交易的账本，无论是钱

币还是钞票都有被伪造的问题。在比特币的例子上，交易构成的账本保证了它们的真实性。钱币和比特币都需要被安全地存储到相应的钱包（分别对应实物或虚拟钱包），若这个步骤不完善的话，无论是钱币还是比特币都有可能被盗窃。比特币与传统货币的根本差别是，传统货币由中央银行发行，而比特币由一个被称为比特币的全球“协作”机制根据共识决定的数额发行。作为用于交换和商业运行的工具，现金已经被使用了一千多年了。从这个事情上说，玛瑙贝（译者注：古代货币的一种）、锻造的便士以及比特币都是有一定联系的。

不过这个报告并不是关于比特币的。它是关于让比特币成为可能的算法技术，以及关于这种技术具有的潜能——它能在现有的账本系统中进行变革，使其成为记录、协助和维护大范围的各类型交易的工具。所以，区块链的基本架构可以修改成整合各种规则、智能合约、数字签名以及其他新型的工具。

分布式账本技术有潜力帮助政府征税、发放福利、发行护照、登记土地所有权、保证货物供应链的运行，并从整体上确保政府记录和服务的正确性。在英国国民健康保险制度（NHS）里，这项技术通过改善和验证服务的送达以及根据精确的规则去安全地分享记录，有潜力改善医疗保健系统。对这些服务的消费者来说，这项技术根据不同的情况，有潜力让消费者们去控制个人记录的访问权并知悉其他机构对其记录的访问情况。

现行的数据管理方案，特别关于个人数据的管理，通常是在单一的机构内架设的大型传统IT系统。由此还会引入一系列的网络与通讯系统，才能实现与外界的交流，这也增加了额外的成本和复杂性。高度中心化的系统的单点失败的几率很高。这也会带来被黑客攻击的风险，而数据经常会出现没有及时同步的、过期的或者不准确的问题。

与此相反，分布式账本天生的就是很难去攻击的，因为它没有用单一的数据库去存储记录，而是保留了同一个数据库的多个共享副本，因此黑客攻击必须同时针对所有的副本才能生效。这个技术也具备阻止未授权修改或恶意篡改的能力，因为网络中的参与者会立刻发现账本中的某个部分被篡改了。另外，这种技术用于维护信息安全及更新信息的方法意味着参与者可以共享数据，并确保账本的所有副本在任何时候都是与其他副本一致的。

不过，这不代表分布式账本对黑客攻击是免疫的，因为原则上说，任何人只要能够找到“合法地”修改一个副本的方法，则有可能修改账本的所有副本。因此，保证分布式账本的安全性是一项重要的任务，就如确保现代社会运行所依赖的数字技术基础设施的安全性一样。

一些地方的政府开始将分布式账本技术引入业务当中。爱沙尼亚政府使用由Guardtime公司开发的、被称为“无需密码的签名基础设施”（Keyless Signature



Infrastructure, KSI)的分布式账本技术去做相关的试验已经有几年的时间了。

这个基础设施让公民可以验证他们存放在政府数据库的相关记录的正确性。这好像也杜绝了一些有特权的内部人员在政府网络内部进行不法行为的可能性。有了这个保证后，爱沙尼亚相继启动了如电子式商业登记(e-Business Register)以及电子征税(e-Tax)等基于数字技术的服务。这降低了在国家和公民上的行政负担和成本。爱沙尼亚与英国、以色列、新西兰和韩国一起，并列在“数字化五国(D5 group of nations)”里。（译者注：数字化五国是英国政府赞助的一个项目，目的是通过数字化改善公共服务的质量）。英国政府有机会与这些政府以及其他有类似想法的政府一起，去学习和实施区块链及相关技术的应用。

商界很早就看到了这项技术所带来的潜力。分布式账本提供了一种确保商品及知识产权的所有权和起源的新方法。例如，Everledger 提供了一种确保钻石身份的分布式账本，并记录从采掘、切割、销售和承保的相关信息。在这个有相对多的纸质文件被伪造的市场里，这种技术让钻石的归类更加高效，并有潜力降低诈骗的风险，以及防止“血腥钻石”（译者注：即在战乱或冲突地区开采并用于资助战争活动的钻石贸易）进入市场。

这类技术面临的一个重大挑战，就是如何向政策制定者以及公众解释这种技术的重要性——这也是本报告的一个重要目的。

在交流这项技术的过程中，面临的第一个困难就是区块链技术与比特币看似紧密的联系。比特币是加密货币的一种，因为它用密码学的方式确保和跟踪货币的供应量。比特币与丝绸之路（已经被关闭）此类不法交易及“暗网”交易网站的联系使得公众与政府政策制定者对此产生疑虑。不过，各国的中央银行和政府金融部门对数字货币都有一定的兴趣，正大力展开研究。这是因为与实体的现金不一样的是，数字现金的电子化分发方式能够提高效率，能够创造一个没有实体现金的交易账本。

交流这项技术面临的第二个困难是一系列令人困惑的术语。Simon Taylor（译者注：财富500强之一的巴克莱银行的区块链研发事业副总裁）在这部分的内容结束时会提供一系列的定义并将这些术语解释清楚。特别需要提到的一个术语是“分布式”，这个词容易带来误解，有人认为分布式意味着这个系统肯定是没有机构能监管的、也没有持有人的。这并不完全错误，也不一定正确——这要看账本的具体设计规则。在实践中，分布式账本的模式有很多，拥有不同程度的集中化特性，有不同类型的访问控制机制，以符合不同业务的要求。在这个领域里，有“无需许可”的账本，对任何人都是公开的，他们可以为账本贡献数据，而且账本不能被某个人或机构所占有；还有一些“基于许可”的账本，它们可能是所有者的，而且只有所有者才能记录和验证账本的内容。

这其中关键的信息是，通过完全了解这项技术，政府和私营机构可以选择最符合自身业务需求的特定设计，在安全性、中心控制权之间达到平衡，从而又能得到在不同机构和个人之间共享数据的便利性和机会。

就如大多数新技术一样，这些技术将来的用途及可能产生的问题仍然不明晰。就如我们关注所有新技术的时候重视的问题一样，关键不在于这项技术自身是好的还是坏的，而是这项技术有什么应用场景？为什么而设？如何应用？有什么相应安全措施去避免可能带来的问题？

为了帮助解答这些问题，英国政府科技办公室选择出来自商界、政府部门以及学术界的专家们组成了一个高级小组，去评估分布式账本技术用于政府内部以及私营部门的机会，并决定政府和其他部门需要如何在使用分布式账本技术的过程中趋利避害。目标是为政策制定者与关注者解答技术背后的术语，并给他们提供这项技术的愿景和证明，以帮助他们决定什么措施是必须的，以及如何最好地部署这些措施。

总的来说，分布式账本技术提供了一个框架，让政府可以用于减少欺诈、腐败、错误和涉及大量纸质文件业务的耗费。它有潜力重新定义政府与公民在数据分享、透明度和信任意义上的关系。对私营部门来说，类似的潜力也是存在的。

这个主编寄语给出了来自我们研究成果的 8 个建议，涵盖了愿景、技术、治理、隐私和安全性、震撼的潜力、应用及全球视角等内容。这些章节由分布式账本技术领域的专家们书写，但使用了普通人也能看懂的写作风格。我对这些专家提供的指导和体贴的贡献深表感激。

Mark Walport, 英国政府的首席科学顾问, 写于 2015 年 12 月。



愿景

分布式账本技术为政府及其他公共或私营部门提供了广泛的好处。就如名字所暗示的一样，它们可以在精确的控制下进行广泛地分布。这些技术是很高效的，因为有权修改账本的参与者作出的任何改动都能够立刻地反映在账本的其他副本上。这些技术能够可靠地拒绝未经授权的改动，因此篡改账本是非常困难的。不过，分布式账本技术单靠自己是无法发挥全部潜能的，只有与其他应用结合起来——如在这项技术上层架设的智能合约，才能充分地释放分布式账本技术的潜力。

政府支持分布式账本技术开发的首要角色是明确政府部门如何可以使用这些技术去改善自身业务流程及提高为公民服务的质量。要实现这个目的，政府需要作为这项技术的顾客之一去在适用的范围内实施这项技术。通过这个方法，政府可以支持和影响此领域内经济活动的发展，包括新兴和成长中的企业，以及大型的主导企业。

这给政府带来的机会是，让政府服务的供应更加个性化、快捷高效。只要适用的话，公民应该有机会在智能合约里告知他们的个人偏好及需求。内置智能合约的分布式账本应用会在合规、降低成本及可追责性上带来显著的改善。

英国政府的数字服务部门正在架设一个数字平台，用于让政府提供服务。分布式账本可以成为这个工作的核心。

建议 1：我们建议政府应该：

- 建立部长级的机制，去确保政府能够提供实施分布式账本技术的愿景、领导力及平台。具体来说，政府数据服务部门 (*Government Data Service*) 应该作为分布式账本的用户去在政府内负责相关工作，而 DCMS 数字经济基地 (*DCMS Digital Economy Unit*) 应该作为分布式账本技术的实施者去在政府内部负责相关工作。（与英国商业创新和技能部、英国技术战略委员会的“创新英国”组织一起协作）。
- 政府数据服务部门和 DCMS 数字经济基地应该根据这份报告及各部门已展开的一些早期活动，去开发一个有预见性的路线图及相应的支持纲要计划，力求尽快实现；需要持续审查这份报告给出来的其他建议，以实现快速反应。在这项工作的实施过程中，它们应该与其他政府部门、产业、学术界紧密合作，并在有限的时间内建立一个专家顾问组以提供支持。

技术

分布式账本技术仍处于早期的发展阶段。区块链技术的发展是账本技术作出重大变革的第一步、也是重要的一步，有潜力改革公共和私营部门运行的方式。这项技术可以实现“无需许可”的，即任何人都有机会对账本作出“合法的”更改，还可以做成“基于许可”的，及只有限定范围内的团体甚至是个人才能对账本作出“合法的”更改。对政府来说，“基于许可”的账本与比特币的“无需许可”的账本相比更有吸引力，因为前者让所有者/所有者团体能够通过规则去控制系统的访问权。分布式账本能够将系统安全的管理工作放到后台里，从而降低系统的复杂性，让系统更加便捷，并降低成本。

要充分发挥这个技术及相关技术的潜力，还需要解决很多问题，包括隐私保护、安全性、性能及可扩展性的问题。另外，为了在账本上支持更多复杂的功能，如智能合约、签名和其他应用，会有一系列研发这些算法的机会。这会增强和多样化账本使用的价值和范围。这个领域正在飞速发展，这类问题已经有展开各种研究了，一些甚至已经解决了。如果政府要等待“完美”的方案，那么就会失去塑造和取得这项会给公共部门带来最大效益技术的机会，英国也可能会失去由此可能带来的有助于经济发展的机会。

除了确保这项技术的健壮性和可扩展性外，我们也要了解不同潜在的用途所带来的道德及社会影响，以及相关的开支及采用这项技术的好处。就研究和开发来说，英国处于一个很好的位置，我们并不认为这个位置这是理所当然的，毕竟在世界范围内关于分布式账本技术的开发还是有很多的兴趣和竞争的。

由英国工程和物理科学委员会、英国经济与社会研究委员会带领的研究委员会正在扮演一个重要的角色，它在各大学及新成立的阿兰·图灵研究所里支持相关的研究。这里也有给商业机构去投资到相关研究及开发的机会，以及让公共和私营机构联手去攻克安全性、隐私保护和标准制定的共同问题的机会。——用合作取代竞争会给这些领域带来产业上的优势。

由政府和私营部门投资的一些数字技术机构，现在有数字加速中心、未来城市加速中心及开放数据学院。除此之外，怀特查佩尔智库(Whitechapel Think Tank)可以为讨论提供话题和分享想法。这意味着英国处于一个很有利的位置，能够建造一个可靠的分布式账本的研究和测试的潜力。不过这样分散化的活动并不一定能给我们带来最好的效果，而有的人也说得很有道理，就是公共和私营机构的研发社区应该用一种能够带来良性竞争的方式去自我组织和运作，这样才能刺激最大程度的创新。

我们接下来的两个建议的目标是，鼓励更深入的研究并建立英国去试用和试



验不同分布式账本解决方案的能力。

建议 2：为了确保分布式账本具有可扩展性、安全性并能够提供账本内容正确性的证据，英国的研究社区应该投资到相关的研究中。这些技术应该要提供与技术部署场所相对应的高性能的、低延时的特性。这些技术需要节约能源。新成立的阿兰·图灵研究所与类似怀特查佩尔智库的机构一起，可以在对相关技术有兴趣的公共及私营机构的研究和开发部门之间扮演协调和“自我组织”的重要角色。私营部门也应该考虑投资到阿兰·图灵研究所里，在竞争发生前的阶段支持相关的研究，这些研究最终会让商业应用变得更加健壮和安全。这包括密码学和网络安全方面的工作，当然也包含新型算法的开发。

建议 3：政府可以支持地方政府的分布式账本展示项目的创建，这会带来让这项技术及其应用成为可能的各个要素。在城市级别的展示项目是一个尝试和实施分布式账本项目的重要机会。英国技术战略委员会旗下的“创新英国”组织可以在“城市合约”的开发过程中利用这些成果去实施城市展示项目。

治理

有效的治理和监管是分布式账本成功实施的关键。治理由账本的所有者及参与者设定的规则组成。这些规则需要与监管或法规的条文结合起来，这构成了为保护社会广泛利益而设的外部机构的规则框架。政府单独地、或与其他政府一起合作，去订立法规并创建监管所需的框架，通常是创造或者引入一个对政府负责的监管机构去执行相关的工作。

在数字世界的例子里，有两组规则/代码控制着数字技术的运作。第一种是典型的由法规框架、法条及监管提供的一系列规则。第二种是由软件编码的、决定算法运作的一系列规则，这是“技术上的代码”，无论是技术上的代码还是法律上的规则都需要确保其严谨性和精确性。

分布式账本的成功实施将需要治理上的组合，以保护参与者、利益相关者以及监管方面，以确保系统能够抵御系统性的风险或犯罪行为。这里面的挑战是要在保护参与者在系统中的利益和保护社会更广泛利益之间取得平衡，同时要防止过度僵硬的架构影响创新的积极性。

法律与技术代码之间的互动也会带来一些机会。例如，公共监管的影响力可以通过法律与技术代码去混合实现，而不像现在这样只能通过法律规则去实现。在本质上，技术代码可以用于确保遵从法律规则，从而降低合规性方面的成本。这可以作为增强监管所用技术的应用案例（被称为 RegTech，是英国政府科技办公室的一份 FinTech 报告里提到的）。

决定治理与监管、法律规则与技术代码之间的平衡，需要不同寻常的力量一起配合，包括律师、数学家和计算机专家一起去解决第三章里提到的一些重要的问题。

建议 4：政府需要考虑如何为分布式账本技术设立一个监管框架。监管需要根据技术实施和应用的新情况与时俱进。作为监管方面的考量因素，政府应该考虑如何使用技术代码和法律条文去实现监管的目标。DCMS 数字经济基地可以在这个建议里面处于主导地位。

安全与隐私

罪犯们现在不只是盯着金属保险箱和银行金库了。现在钱都以数字化的形式存在，事实已经证明黑客和破解者对数字世界的代码构成了威胁。数字世界的密码学代码是很难攻破的，不过绕过这些代码的加密则是有可能的。密码的持有人有可能主动或被动地（意外）将密码公开，而软件代码里可能存在的缺陷也会带来“后门”。存储分布式账本的硬件也可能会被黑客攻击，因此硬件的健壮性和安全性也是应该关注的问题。

在比特币的例子中，储存货币的“钱包”被证明是很容易被盗窃的——不过账本本身还是很稳健——除了在 51% 攻击（即个作恶的个人或机构掌握的全网算力超过 51%）的情况下可能会带来一些风险。

不过，账本的完整性并不是唯一重要的因素。隐私和机密同样重要。根据账本的特性，它可能包含从金融、家庭和健康信息在内的个人机密记录。分布式账本技术有机会为这些数据提供比现有的数据库技术更高的安全性，但这不是一蹴而就的。在这个过程中，还需要大量的研究和开发工作。

政府需要在安全和隐私的事项上扮演一个重要的角色。所以我们的下一个建议是：

建议 5：政府需要与学术界和产业界一起，去确保分布式账本及其内容有关于完整性、安全性和隐私保护的标准，这些标准需要在监管规则和软件代码里同时反映出来。

对这项技术的具体使用案例，政府和私营部门的用户需要根据自己的需求进行自己的风险评估，以明确可能存在的风险。英国国家基础设施保护中心(CPNI) 和英国政府通信电子安全小组 (CESG) 应该保持对分布式账本技术的关注，并在政府内外担任提供保证分布式账本技术完整性、安全性和隐私性建议的重心。就如“建议 2”所提到的那样，新成立的阿兰·图灵研究所与怀特查佩尔智库及英国政府通信电子安全小组一起可以在公共及私营机构的研究和开发部门之间扮



演协调和“自我组织”的重要角色。不能忽视的是，软件和硬件系统在一段时间后就会与时代脱节了，可能会有新技术的诞生，也可能会有不怀好意的人学会新的攻击方法。因此，若这些系统要长期维持下去的话，初始的设计需要考虑到硬件和软件部件在生命周期内的升级问题。还有，在进行新技术方案的实施测试过程中，在系统层面和用户层面同时进行防渗透的测试也是很重要的。

信任和互联

就如第七章在“全球视角”里讨论的一样，信任是在两个或以上的个人、组织或国家间的风险衡量问题。在网络世界里，信任依赖于两个关键点：证明你的真实身份（验证）；以及证明你有权访问你在请求的内容（授权）。在这两个关键点符合后，我会将服务和产品安全地、高效地、可靠地送达给你，来证明我是可以信赖的。

验证和身份证明有一定的联系，但并不完全一样。验证并不代表我需要知道你的身份，只要你能够提供一个标记去证明这个身份是属于你的，这样的例子有很多，如信用卡或借记卡上的个人号码，或者是有生物验证技术护照或其他文件上的指纹。同样地，当我向你提供这个与身份有关联的标记时，我需要确保这个信息是送达给一个正确的个人或机构，而不是仿冒者。所以，机构向它的用户（包含个人、其他机构和政府）提供自身的验证也是很重要的。

数字环境带来的一个机会，就是能在保护隐私的同时使用和创造一些更强大的、更健壮的身份管理工具，可以用于提供验证。一个类似的系统就是依赖于密码学标准 X.509 的公钥基础设施（PKI）。使用 PKI 技术，机构可以提供、共享甚至简化服务或产品的安全送达过程。还有一个重要的、用于机构身份管理的国际标准被称为“合法机构注册”（ROLO），这是用于机构身份验证的。

现在，将智能手机作为事实上的可信用户设备，有机会为安全的验证和互动提供可能。最新的智能手机内置了如“可信平台模组”（TPM）这样的安全特性，能够为验证、加密和签名相关的数字证书和密码学钥匙提供安全保障、“可信执行环境”以及“可信用户界面”。这些技术对恶意软件都有一定的抵抗力。

以上关于验证的讨论表明，为了最大程度地发挥分布式账本的作用，可能需要与其他账本进行互联。不过，这不仅仅需要验证机制上的互联——更需要在数据互联、政策互联以及国际标准的有效执行上达成协议。

建议 6：这个建议是与“建议 5”联系在一起的。政府需要与学术界和产业界一起，去确保为个人和机构设立最高效、实用的身份管理和校验协议。这与国际标准的实施也要有紧密的关联。

一个快速变化的未来——政府的潜在用户案例

分布式账本技术有潜力撼动很多方面的业务。这种技术的处理能力可以做到实时、防止篡改和越来越低的成本。这种技术可用于多个产业和服务领域，包括金融服务、地产服务、医疗保健服务和身份管理等。这种技术可以巩固其他基于软件或硬件的创新成果，如智能合约和物联网。还有，这种技术的分布式共识、开源、透明性、社会协作的底层哲学，对很多上述的部门会带来很大的影响力。

就如其他重大的创新成果一样，分布式账本在提供机会的同时，也给那些无力面对这些变化的个人或机构带来了挑战。特别是，它可能会给如银行或政府这样的传统分层机构扮演的可信的中介角色带来挑战。

政府牵涉的人员、服务和角色都是很广泛的，政府的运作是一个大规模的任务。政府的一些工作是分配价值而非创造价值，另一些工作是创造和维持监管的体系。很多这样的活动会被分布式账本带来的创新改进和增强，而分布式账本也可能对另外的一些活动带来挑战。

最终，实践是开发新技术的最佳方法。参与这个报告的专家组给英国政府提出了一些可能、具体的案例，这在第六章里用五个案例去讲述了。

- 保护关键的基础设施，抵御网络攻击。
- 降低福利体系的运作耗费和跟踪受益人是否合格，促进普惠金融。
- 提高救助资金的透明性和可追踪性。
- 创造经济增长的机会，支持中小企业的发展，增加就业率。
- 降低税收欺诈。

这些研究案例提供了分布式账本的主张、潜在好处以及评估与实际应用距离的概况。

这份报告只描绘了一部分可能的应用案例，不过我们相信对政府来说，这些是不错的起点，可以用于在部门内尝试研究这些技术。所以我们建议的最终部分目标是实施分布式账本技术的试验以及提高政府在这技术上的相关影响力。

建议 7：了解分布式账本技术的真正潜力不仅仅需要研究，还要将它用于真实应用当中。政府应该实施分布式账本技术的测试案例，以在公共部门内部评估这个技术的可用性。

我们建议这些试验应该像临床试验那样协调、报告和评估，以确保其一致性



和准确性。这些测试中得到的成果及经验教训应该添加到“建议 1”里提到的路线图里。

我们认为将来的工作还可以包括涉及到保护国家的基础设施、降低中小企业的市场摩擦、英国就业和退休保障部和其他政府部门的资金发放等。在这份报告行文的过程中，我们发现少数的政府官员已经在认真考虑分布式账本技术对政府的潜在用途。我们建议强力支持和鼓励这些人加入政府部门与英国政府数字服务部门的合作关系中。

建议 8：除了从上到下的管理和协调外，在政府内部也需要建立相应的能力和技能。我们建议成立一个跨政府的同盟，将分析和政策制定的社区都结合起来，用于创建和发展潜在的使用案例，并在行政部门内创建一个相应的技术与知识体系。英国政府数字服务部门以及它跟英国国家统计局、英国内阁以及英国政府科技办公室之间成立的“数据服务合作关系”可以作为这个同盟的召集者。政府在这个事情里有重要的机会，就是通过作为一个“聪明的顾客”，刺激商业部门去探索和掌握分布式账本的应用。

结论——站在全球视角观察

英国并不是唯一重视分布式账本技术的国家。其他国家，无论是大的还是小的，都在快速地探索分布式账本技术——爱沙尼亚政府的学习案例展示出一个小国在对数字科技有高度敏感性的领导层带领下进步是有多快。不过，对英国来说还是有机会成为主导力量的——这也是必须的，毕竟金融和服务部门对英国经济是如此重要。

Patrick Curry, Christopher Sier 和 Mike Halsall 在第七章里提到了快速进化的数字技术国家应该具备的特性，他们认为应该包括以下几个重要的特征：

- 一个知晓数字技术的领导层。
- 一个获得授权并专注于此的政府部门去带来全国的数字化，这个部门需要有国际思维并能与所有的产业部门紧密协作。
- 一个由政府投资的、由产业带领的不断进化的国家级计划，具有活跃性和协作性。
- 在每一个政府机构里，都有相应的有技术意识、资深的和有经验的高级政治官员。
- 除了政治家外，还需要有工程师和数字业务的领导者。

我们仍处于这个由信息科技驱动的后工业革命时代的早期阶段，这个时代是非凡的。之所以将它称为革命，是因为它带来了重要的好处（和潜在的风险）。现在有些事情已经很清晰了，在这场革命中，分布式账本技术的诞生已经开始对现有的很多商业行为方式带来震撼。

人类最早的会计记录可以追溯到古巴比伦、亚述（译者注：亚洲西南部的一个古国）和苏美尔（译者注：古美索不达米亚平原南部地区），这是五千年前的事了。作为早期用于记录书写、计数和金钱交易进步史的记录介质，很多泥板仍被保存下来了。至于数字技术的记录能否像泥板那样长寿，现在还很难说。不过，如果先不考虑这个问题，对英国来说，这里面的机会是很巨大的，它可以开发和使用分布式账本技术去为英国国民和经济的利益服务。为了在这个信息技术的重大突破中趋利避害，还是有一系列的“大挑战”需要解决的。这个报告是在专家给出的证据基础上为政府提出一些关键的建议。其中最重要的是，在英国国内及英国与其他国家中的公共和私营部门建立紧密的合作关系。



定义

这个领域的术语依然在演变，区块链、分布式账本和共享账本等术语经常被互换。正式的定义不太可能满足各方的需求——不过为了这份报告，还是会给出一些关键术语的定义：

- **区块链**是一种数据库，它将一些记录存放到一个区块里（而不是将它们收集到一个单一的表格或者纸张上）。每一个区块是使用密码学签名与下一个区块“链接”起来的，这可以在任何有足够权限的人之间进行共享和协作。

为了协作维护账本的真实性，有很多种具体的方法，而它们被称为“**共识算法**”。（“挖矿”是另一种称呼，是在比特币这种加密货币里的一个类似的机制）——详细信息参考下文。

区块链技术的新颖性在于它不仅仅是一个数据库——它同时也给交易设下了一系列相关的规则（业务逻辑）。这与传统的数据库是不一样的，因为传统的数据库里面规则通常是在全局层面设下的，或者是在应用程序的层面设下的，而不是为交易层面而设。

- **无需许可的账本**，如比特币这种就是没有任何主人的——这个系统不能被任何人“拥有”。无需许可的账本目标是让任何人都可以向账本中贡献数据（译者注：只要符合系统规则），并让任何拥有这个账本的人都有一份完全相同的副本。这是一个抗审查的过程，意味着没有人能够阻止一个（符合系统规则的）交易添加到账本里。通过达成对账本状态的共识，账本的参与者能够共同维护账本的完整性。

无需许可的账本可以作为一个不可编辑的全球记录——如用于设立遗嘱，或登记产权记录。不过这对现有的机构和产业来说会带来挑战，而且可能需要政策方面的配合。

- **基于许可的账本**可能有一个或多个拥有者。当一条新纪录被添加进去后，账本的完整性是由一个有限的共识过程去检查。这是由少数被信任的个人或机构去执行的——如政府部门或银行——相对于无需许可的账本来说，这个共识机制过程变得更简单了。基于许可的区块链提供了高度可校验的数据集，因为共识过程创建了一个可由所有参与者校验的数字签名。若让多个政府部门去校验记录，则会让人们增强对记录安全性的信心，而不是像现在那样——政府部门经常用一张纸去共享数据。基于许可的账本速度通常是要比无需许可的账本更快。

- **分布式账本**是一种跨越多个站点、国家或机构的数据库，而且通常是公开的。

数据是在一个连续的账本里按照先后顺序记录的，但并不是存储到区块里面。只有当参与者达成一定数量的赞成票后，记录才能添加到账本里面。

分布式账本需要信任账本的校验者或者是操作者。例如，全球性的金融交易系统瑞波(Ripple)就使用了一组选定的验证者(被称为独特节点校验者)，最多可以达到200个校验节点，它们是已知的、未知或者是部分信息公开的校验者，系统是基于它们不会合谋作弊的基础上运作的。这个过程提供了一个与比特币相比可能会有审查元素的数字签名，但速度要快很多。

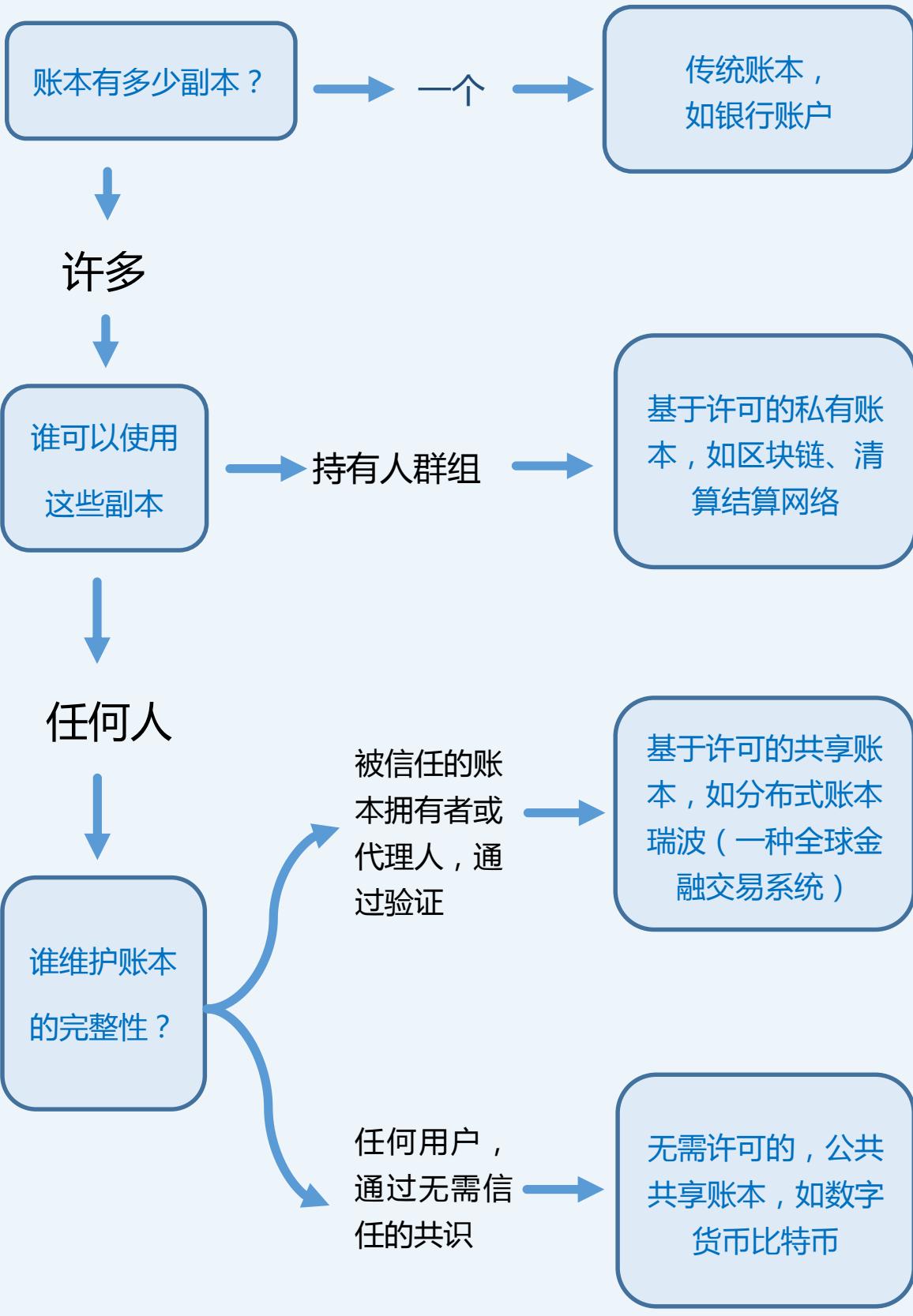
- **共享账本**是分布式账本组织的首席科学官Richard Brown提出的一个概念，他过去在IBM工作过，这个概念通常是指任何由一个产业或者私营联盟共享的任何数据库和应用程序。这是这类技术的一个最通用的、最全面的一种表述。

共享账本可能使用分布式账本或者区块链作为底层的数据库，不过通常会根据不同用户进行权限的分层。“共享账本”是具有一定程度的许可管理的账本或者数据库技术的统称。某个产业的共享账本可能会有一些限定范围的校验者，系统信任它们去维护账本，这能够带来显著的好处。

- **智能合约**是一种用计算机语言取代法律语言去记录条款的合约。智能合约可以由一个计算系统自动执行，如一个适用的分布式账本系统。智能合约的潜在好处包括降低签订合约、执行和监管方面的成本；因此，对很多低价值交易相关的合约来说，这是有明显的经济价值的（译者注：降低人力成本）。智能合约潜在的风险是要依靠计算机系统去执行合约。在这个阶段，风险和好处大多是理论上的，因为智能合约的技术还处于早期阶段，有些时候离大范围的应用还有不少距离。



分布式账本分类





• CHAPTER 1

Vision 视野



诸如比特币这样的数字货币都依托于名为区块链的底层技术。区块链可以将每一笔发生在数字账本上的交易都复制到其他用户那里去。这种“共享账本”的方法能够简化政府机关和经济运行中的很多服务。



Author

Simon Taylor,
VP for Blockchain R+D, Barclays



第一章 视野

引言

诸如比特币这样的数字货币创造性的提供了一项能够追踪每一笔金融交易的技术。这些数字货币的底层技术，即区块链，将每一笔交易的信息都做了拷贝，并存储在每一名使用者的计算机上。

金融机构、监管人员、央行和政府也都在探索这项新技术的未来应用前景，诸如是否能够简化经济活动中大量冗杂的事务。

很多这些潜在的应用前景都还只是中期的展望，而公共和私有部门的发展都是长期的，有关区块链技术将提升效率的说法很早就有传闻，这促使政府官员们必须现在就开始研究这项技术将来会如何使大家受惠。这一章将描绘技术应用的未来前景。

什么是共享账本？

共享账本实际上是一个数据库，其记录了金融、物理、电子资产拥有者的信息：举例来说，一颗钻石、一单位货币、或者是集装箱里的货物。最关键的是每个参与者都可以保留一份区块链上的所有交易记录，并且随着新交易发生，记录也随之更新。账本信息的安全性和准确性都可以通过数学的方法保证，诸如密码学。几乎目前所有记录在纸张上的信息都可以储存在共享账本上。（详情请见第二章关于共享账本技术的讨论）

比特币自从 2008 年出世之后，就一直依托于区块链技术。许多有关比特币的误解，也都随之衍生。比特币和“丝绸之路”这样的网上黑市的联系，使公众觉得比特币就是与洗钱和恐怖分子有关的东西。现在，这种误解又继续影响着大家对与区块链技术的看法。

得益于区块链技术的四个特征，共享账本和数据库有可能会给政府和金融服务带来极大的好处。

1) **通过加密技术对账。**目前，政府和商业机构会把交易的详细信息发送给对方。

一旦收到信息，每个机构就会在自己的账本上更新信息。但现在还没有一种方法可以保证这些信息的准确性。区块链可以通过一系列方法解决这个问题：例如通过“证据点”证实数据。这个方法对于政府的数据组也一样适用。通过不同的共识算法（工作量证明、权益证明、拜占庭将军问题），账本的参与者可以就底层数据的状态达成共识。

- 2) **数据复制。**许多机构都有部分或全部数据的拷贝，这极大降低了错误数据出现的可能性。对于现在的数据库技术来说，数据复制工作会增加 IT 系统的成本，并对 IT 系统的复杂性提出更高的要求。将数据大量复制的一个好处就是，哪怕有一处数据出错了，其他的数据还是准确的。很多机构可以通过对账计算，就可以证实他们的数据是否准确。
- 3) **访问控制。**分布式账本使用钥匙和签名来管理能够进入账本的人和事。这些钥匙在特定情况下具有特定的功能。举例来说，一名监管人员想检查一个机构所有的交易，可能需要一把“观察钥匙”，但这样的钥匙只有被法庭拥有才具有这样的效力。
- 4) **透明性和私密性。**因为许多机构都拥有账本的备份（第一点），同时也可以验证每份记录的真伪（第二点），所以共享账本的透明性是很高的。因此，监管者或是独立第三方(司法)可以确信数据库的内容没有被篡改。鉴于此，他们可以公开原本是私密或不可公开的文件信息。在监管报告和欺诈预防方面，共享账本技术可以帮助银行等商业机构，甚至可以使民众拥有监督政府履行职责的能力（详见第五章）。通过独特的加密签名技术，可以证明正确的人已经按照正确的规则添加了正确的记录。

这几大特点结合后，可以帮助解决之前成本高、难度大的问题。

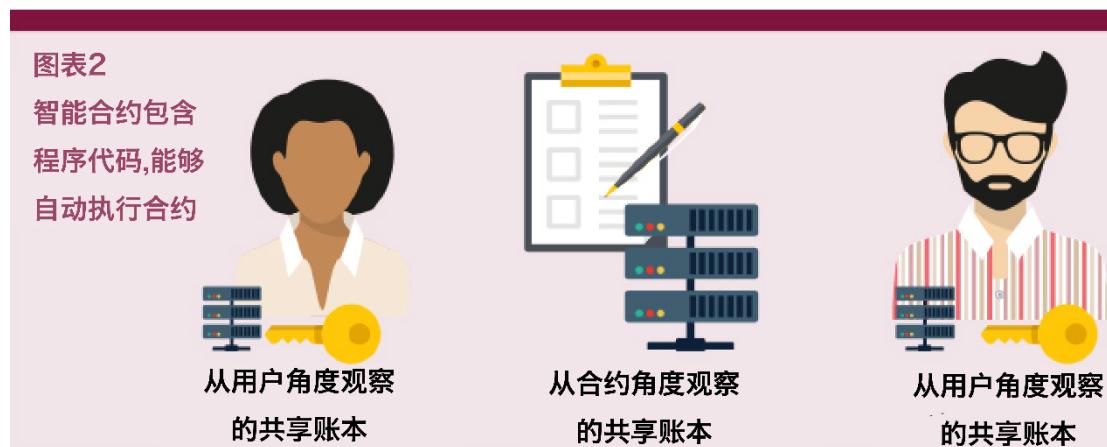
什么是智能合约？

如果区块链是一个数据库，智能合约就是能够使区块链技术应用到现实当中的应用层。传统意义上的合同一般与执行合同内容的计算机代码没有直接联系。



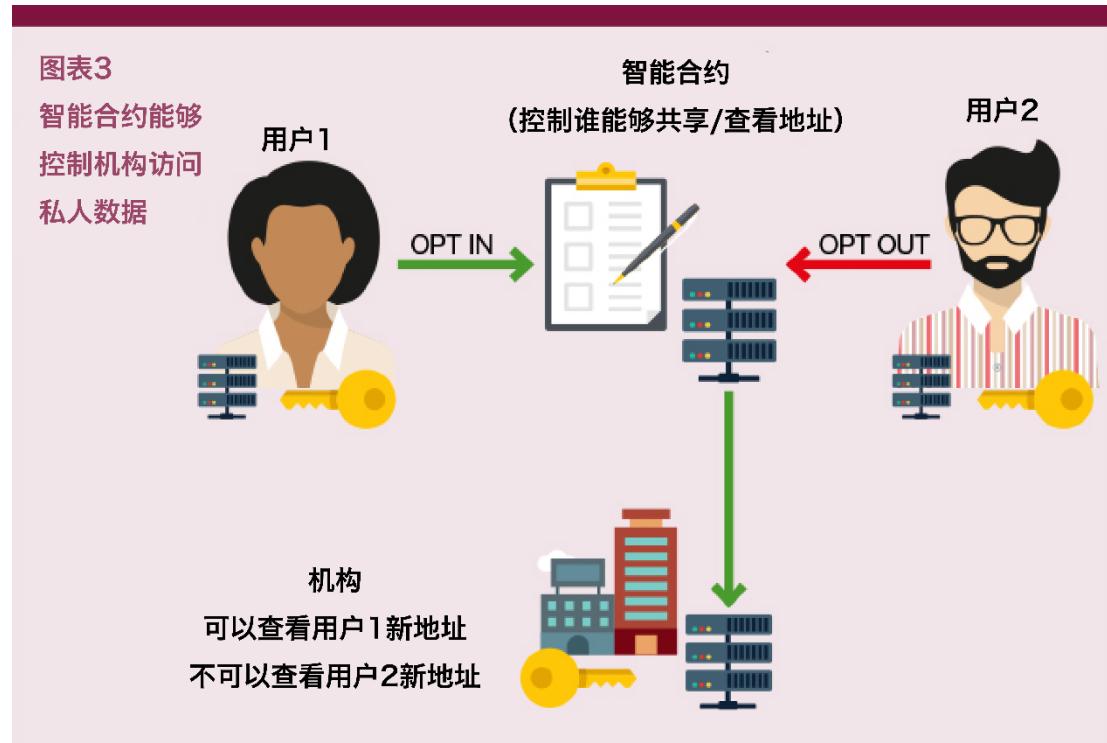


纸质合同在大多数情况下是被存档的，而软件会执行用计算机代码形式编写的合同条款（不一定能100%遵守纸质合同的原意，只能做到近似的效果）。这可以参考图1所展示的内容。



当签订一项服务时，这个方式是很有效的（如视频点播），但如果向用户提供复杂服务的时候，就变得极具挑战了（如更新多个政府部门数据库的一个地址）。这需要更复杂的数据保护和数据隐私立法工作，以保证个人的隐私。此外，目前诸如信息分享和合同签订等活动还停留在纸质阶段。

共享账本的关键特点（加密对账技术、信息复制、访问控制、透明性和隐私性）同智能合约结合之后，在允许数据复制和分享的前提下，可能会为这些问题的解决提供出路。如果两个用户签订了一份智能合约，就可以在智能合约的数据之上按照规则运行。这会提高效率并减少公共和私营部门的人力流程，提高生产力和增速。应注意，仍有诸如遗留数据库管理的其他挑战需要我们处理，但多系



统的“准入允许”才是智能合约真正得以运行的基础。

在另一个场景下，用户 1 选择在一个共享账本上使用智能合约，向一家持有“蓝色钥匙”的机构共享他的地址（还有很多别的机构，持有别的钥匙）。但用户 2 选择不共享他们的地址，因此机构只获得了用户 1 的最新地址。当用户通过市政厅登记地址信息的时候，地址信息的改变会反映在护照、驾驶证和其他重要部门的数据库中。Onename. io 借助社交网络提供类似的服务，信息的改变会反应在所有机构的数据库中。

智能合约正被人们考虑用于更广阔的应用，尤其针对监管合规、产品可追溯、服务管理，以及针对下列领域中假货和欺诈问题：

食品、金融服务、能源、制药、健康、航空、飞机、电讯、IT、交通、公共事业、农业、石油天然气。

上述领域会在本章和第六、七章讨论。

从总体上说，当机器、公司、人都想建立一份数字化协议并有密码学上的确定性去确保合约相关的账本、数据库或账号都会遵守这个协议的时候，智能合约就可以发挥作用了。

未来视野

民主政府的一个关键角色，是将资源合理的分配给公民（个人和企业）。分配的内容不仅包含货币，还有无形的社会资产，例如安全、民主、法律、自由市场、低通胀、私有财产不可侵犯、契约精神。然而，这样的分配也是基于公民与政府之间的建立的协议之上的（通过投票和宣言）。

随着民主模式不断发展，国家机器变得越来越大、越集权化、越远离民众。

政府主要通过各式各样的税收获取资源，成本高昂、系统复杂，资源的分配则通过福利金、救济金和养老金分发。这样复杂的方式部分也是由于政府的中央化特质。

私营部门已经开始认识到这个中心化的模式提供的是低质量的服务，不再具备经济性，同时也不能将电子商务和数字化发展的福祉发扬。政府也开始认识到应该满足公众的需求，提供个人化、数字化的政府服务。共享账本和智能合约的应用就为政府提供了一个领导潮流的机会，确保有需要的人受惠于技术的福祉。

这一潮流在“共享经济”的发展中十分明显，尤其体现在阿拉伯之春和占领中环等社交媒体引领的运动中。这些现象显示出社会自我调节的变化。但到目前为止，还没有一个方法能够保证你一边拥抱新技术，一边还在推动自由市场。有



一种观点认为我们之所以还不能把民主制度搬到线上，是因为我们需要一个成本昂贵、集中化的身份验证系统才能够有所保证。假如这样一个系统是不可期的，那么区块链技术其实就能在这一领域发挥作用。

此外，政府参与到区块链早期的技术发展和统筹中，可以帮助削减政府的成本，也有可能带来一个更加个人化、高效、合规、有民主潜质的政府。

拥抱区块链技术的步骤

共享账本技术正被积极的推动并被世界上几大经济体开发，如美国、中国、新加坡、拉美。英国如果理解支持这个新兴领域发展，还有机会在未来与其他国家竞争。

政府在分布式账本技术中的角色可以从三个视角来看：

- 公共服务提供者
- 立法者
- 经济的守护人

政府：公共服务提供者

账本技术可以影响公共服务的许多关键领域，例如隐私、数据转移、移动技术的感应能力等（详见第六章）。

政府：立法者

分布式账本技术还处于早期，以后还有很长的发展周期。照此，政府可以瞄准技术发展的三个领域。

领域一：支持新兴生态系统

在比特币和其他共享账本系统中，已经有很多提供类似交易所、“钱包”等服务的提供商。应该认识到这一技术和商业还有待成熟，领域一内的活动包含：

- 要求交易所验证用户的身份（KYC）
- 向银行提供手册，说明公司的区别：那些通过区块链转移价值的公司；向区块链公司提供软件服务的公司；提供区块链软件解决传统商业问题的公司。

- 针对钱包服务提供商设立安全标准。
- 向学术界和初创公司提出难题：建立合适的技术架构；如何使技术用来验证身份，解决洗钱，阻止犯罪；如何通过多重签名钱包建立新型的政府-公众的用户体验，使大众可以审计处理自己的数据。
- 利用合作伙伴来跟政府保持协调。

领域二：早期试验和试点

政府在自己能够大展拳脚的领域会先进行试点，政府尤其会考虑以下几个问题：

- 哪些公共领域会受惠于共享账本/数据库技术？
- 哪个的试点会支持现有政策（养老金改革，福利改革）？
- 哪个试点能提供最大的学习机会？

领域三：英国在竞争中的角色

分布式账本技术领域接收到的风投资金大部分都投入到了比特币和美国西海岸。但这项技术的未来机遇在其他地方：

- 英国应该认识到这个不同，并通过自己的监管机构发挥作用。（关于监管和管理，详见第三章）
- 英国可以建立一个技术中心，并作为全球 FinTech 和英国贸易投资计划中的重要一项。

政府：经济的看护人

如果想进一步了解政府是如何推动技术发展并将技术福祉发扬的，最好去观察两个领域的案例：金融服务；保险和其他行业。

金融服务

账本技术在金融服务业中的应用案例：

- 资本市场效率提升
- 贸易金融的欺诈减少、效率提升



1. 资本市场效率提升

资本市场仍旧依赖纸质记录跟对手方进行对账。中央化的交易平台已经在过去建立了，清算交易和确认对手方已经同意的能力是十分重要的，这要求信赖的原则。银行业的很多罚款和固定成本都是基于信赖原则。一家银行必须依赖另一家银行而且没有其他方法验证银行的行为。区块链可以以监管者看得见的方式，显示交易过程和有关方。大型银行现在正在寻找合适的技术工具进一步激发效率。

2. 减少交易金融中的欺诈和提高效率

交易金融仍然沿袭着几千年来相同的方式运行。每一次交易至少需要 5-6 个参与方才能完成（买家、买家的银行、货运公司、中间人、卖家、卖家的银行）。已经有不少人尝试将交易金融标准化，创建中央交易平台。共享账本提供了一些独特的优势。

- 一个“部分许可”的系统可以保证纸质文件的安全性（如，关于集装箱中货物信息的提货单）。这可以之后由每一方签署（可验证地或数字化的）。（主要特点：透明、加密对账）
- 相对于今天要简单存储的文件，共享账本只需记录这些文件的状态即可。如果应用的更广泛，文件可以通过共享账本就可以传递，不必打印和签署。（特点：高扩展性、复制性）

行业和机构

1. 资产跟踪和产地保障

诸如工艺品和电子产品等商品，他们本身就携带着很多数字化标识。然而，还没有一个全球化的平台可以追踪这些产品。很多机构依赖纸质文件来证明产品的来源地。但是，如果纸质文件也是伪造的，那么就没有办法验证了。如果供应链中的一部分使用了共享账本，同时也“签署”了数字账本，那么产品是否真伪就一目了然了。

举例来说，provenance.org 是一家希望借助区块链技术向零售商提供验证衣服真伪方式的公司。现在，零售商们都是使用纸质文件来验证衣服真伪，但这不能保证这些文件是真的。如果使用区块链技术，负责人就会用自己的私钥签署电子化文件，零售商可以知道这份文件是什么时间签署的。区块链技术的本质要求签署文件可以显示给被授权的零售商。

2. 通过用户控制，保证数据安全

数据准确性和机密性要求，对机构来说是最大的问题。如果拥有被多个来源

验证的数据（如政府和银行），保险公司就能做出更精确的产品、制定更准确的价格和保费。问题在于让公众掌控自身数据的同时，还能保证数据的安全。

通过一个名为 guardtime 的方案，区块链可以提供有关每一份数据来源的信息。如 ARM 的 trustzone 芯片，使用手机中的 TEEs，任何索要信息的行为都会被记录在区块链中。除非公众授权保险公司，否则有关数据就不会被移动。如果任何改变数据的行为发生了，那么有官方就会立刻被告知。

当共享账本技术与移动手机相连后，解决了有关安全型管理的很多难题。准备在未来采用这一技术的机构，需要赢得大众的信任，而且最好在早期有所试点。

3. 工业装备（连接的物联网）

如何做到实时精确地收集到关于众多行业部门设备的数据，是一件很困难的事情。随着物联网的到来，很多难题都将会被低廉的硬件（感应器）解决，但这些硬件很容易受到攻击。根据最近一份 IBM 研究院的报告：

“结果就是：随着数以百万计的感应器成本下降，它们能够成为更加复杂系统的一部分。”

“在物联网网络中，设备信任很难建立，成本很高。随着物联网进一步扩展，用户拥有掌控隐私的权利，同时也将隐私和匿名都整合到产品设计中。现在的安全模式是基于闭源方式的（即“模糊中的安全”），这一方法已经落后了，需要用新的方法替换（即透明中的安全）。”

“我们看来，在去中心化的物联网中，区块链帮助交易处理和设备间的联动。每个设备都有自己的角色和行为，最终形成一个‘去中心化、匿名化的物联网’，也可以看成是数字世界的民主化。”

如果每个设备即作为自主主体，又作为整体的一部分，那么就不会有故障点。在这个情况下，机构通过使用物联网设备，获得实时数据和联通的好处。共享账本和区块链技术为物联网的应用提供了新的商业和技术模式。

案例一：一辆拖拉机以自主主体的方式运行，这一地区的农民都拥有拖拉机的使用权，拖拉机则按次收费。它能获知并支付天气信息，与厂商保持通讯，获得定期维修保养。

案例二：在零件是真品，设备被授权的前提下，工业设备能被授权去订购零件。这可能会带来有关工业设备新的融资方式，新的市场也将建立在设备表现和效率的参考上。



结论

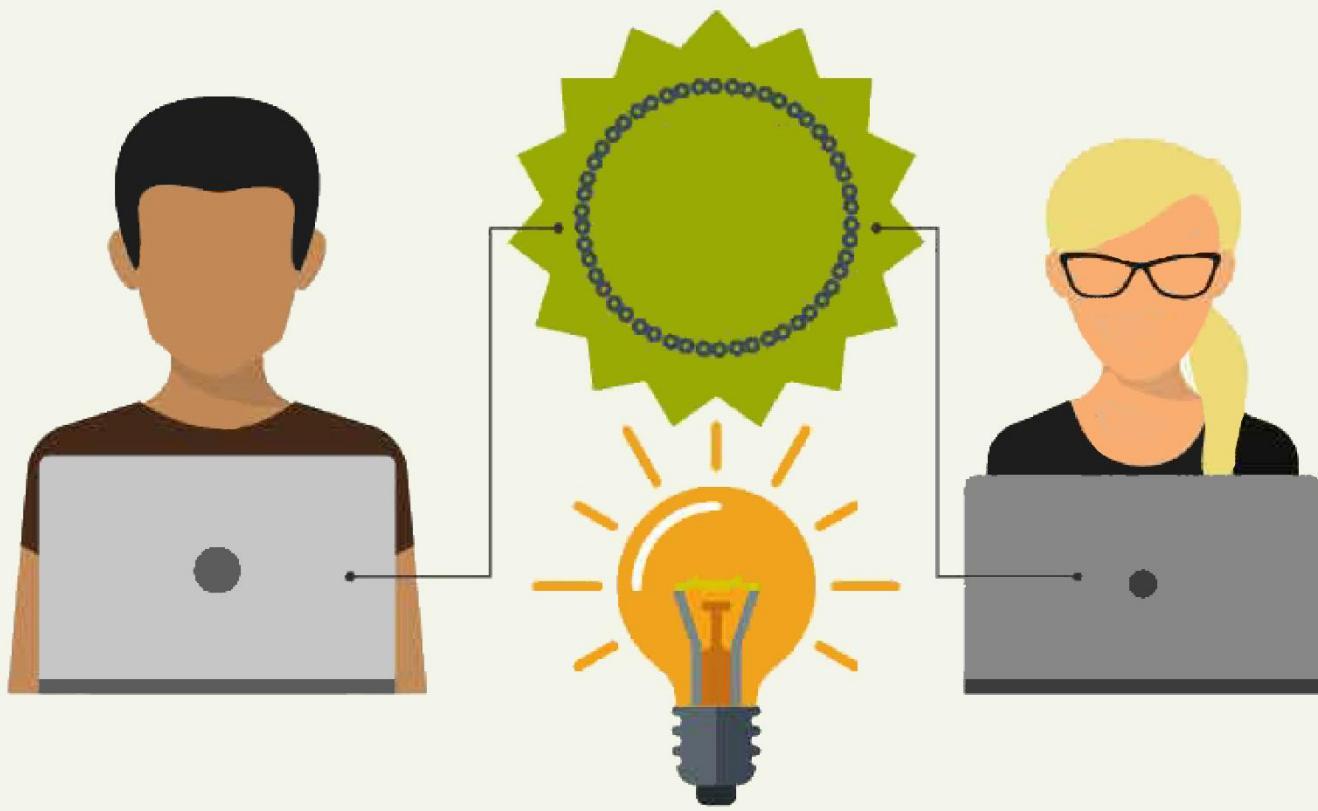
我们可以预见一个这样的未来，区块链技术将创造一个更值得民众信任的“玻璃政府”。现在已经有一些应用的案例，而且随着技术的进步，越来越多的案例将会出现。这也会帮助施政目标的实现。政府官员应该认识到：

还处于自身早期阶段的区块链技术现在已经展现出了很大的前景。想要实现区块链技术的前景，一定要理解基于密码学的对账方法、大规模的数据安全性复制技术以及可验证的透明性的组合是如何为支持新兴的生态、早期试点和定位英国为一个全球领导者的角色而服务的。



第2章

技术 Technology



实物现金不同于其他形式的货币。两个人之间的现金转移是不需要银行与政府这样的第三方机构的参与或许可。比特币及其区块链已经向我们展示了如何通过电子化来实现与实物现金一样的转移方式。但区块链这项数字技术所蕴含的影响与机遇远不止这些。



Author

Richard G Brown,
Chief Technology Officer, R3



第二章 技术

引言

比特币是一种新型**电子现金**。与其它由央行发行的货币不同，比特币的发行是由**去中心化**网络中的计算机控制。这个网络采用密码学与其他技术来管理比特币的供应并追踪谁拥有这些比特币。因为比特币也被称为**加密货币**。

银行通过账本来记录用户的账户金额。比特币也使用**账本**，但是这个账本是由去中心化的网络中的计算机共同维护。这个账本也被称为**分布式账本**。

当账本中加入新一批条目时，也加入了上一个批次的索引值，让所有参与者都可以验证账本上所有条目的出处。这些批次就被称为“区块”，而所有区块在一起则被称为“**区块链**”。

这个章节将会更多的解释这些概念，为什么这些概念很重要，以及他们如何可能称为更广泛的应用的基础。

什么是钱？

一张 20 欧元的钞票是一个很特别的东西。只要将这张钞票递给其他人，就完成了 20 欧元价值的转移，而且不需要任何的第三方来验证这笔交易的真伪。如果是这两个人单独在一起，整个世界内没有其他人需要这笔交易的发生，也没有人能够阻止这笔交易的发生。

但是这种点对点的价值转移只有在双方非常近的情况下才可行。如果要转移 20 欧元的价值给另一个的城市或者国家的人，就需要相信其他人并赋予他们一定的控制权。例如：一个处理包含着 20 欧元钞票的信件的邮递员，或者执行电子资金转账的银行。事实上，如果银行认为这些资金与非法交易相关，银行可以阻止这笔电子交易或者冻结电子账号。

正因为实物现金与其他形式的货币有着本质的区别，所以导致了世界金融通道的产生。这种金融通道包括了支付系统、银行间的合作关系，以及 SWIFT (the Society for Worldwide Interbank Financial Telecommunication) 这样的电子通信网络。只有实物现金才是不记名的有价凭证。也只有实物现金需要其他人的许可就进行价值转移，这就是所谓的“抗审查性”。

直到 2008 年底比特币的出现改变了这种情况。比特币的创造者宣称比特币是一个真正意义上的点对点的电子现金。所有者拥有完全的控制权，不需要得到银行的许可就可以发送比特币给任何一个人，而且没有遭受账户被冻结的风险。

在比特币系统中，每一个全节点都存储着从比特币运行第一天起至今所有的交易记录，这些记录被储存在一个一个的区块内。每一个区块都通过密码学的方法链接到前一个区块，形成了一个拥有着全部历史信息的区块链。这也是为什么被称为分布式账本。用户可以使用各种不同的应用来访问账本，账本的每一个副本都会根据算法来同步以保证账本状态的一致性。

FAQ

什么是“区块链”？

一个区块简单来说就是一系列支付的列表。区块链就是一系列区块链的列表，每一个区块链都可以追溯到前一个区块。然而，当人们在讨论区块链的时候，区块链一般指的是支撑比特币系统的一系列技术。其他的一些项目将区块链技术作为他们的灵感以用来解决金融与其他行业存在的一些问题。

比特币并不是在 2008 年凭空产生的。对于数字货币的研究几十年前就开始了，比特币系统的每一个组成部分也是已经存在的。比特币的突破之处在于：1、将已有的技术通过创新的方式结合起来；2、选择了一个合适的时机，当时互联网上开源软件模式已经成熟，并且人们也已经愿意接受一种新的货币体系的理念。

这个系统的设计使得篡改已生成的区块变得越来越难（实际上难度大到不可能）。一旦交易有足够的确认，就永远不能被修改，也就是具有了抗审查性。总之，比特币是真正意义上的数字现金。

那么也难怪世界各地的政府与监管者们非常谨慎的审视这项发明。一个抗审查、数字化不记名资产似乎是一个用于犯罪网络的理想货币。比特币也成为了丝绸之路（一个已经被取缔的在线黑市）网站上的主要货币单位。

然而包括很多英国政府部门在内的世界上大部分监管者并没有选择禁止比特币，很多合法的公司也正在大规模的投资这项技术。这是什么原因呢？

机会还是威胁？

首先，这些系统并不是像有人预料的那样是不可控的。与大众的认知相反的是，底层架构使得追踪交易与追查系统滥用者变得相当容易。**监管者开始学习如何控制这个系统的价值流入与流出环节。**

比特币这样的平台一开始听起来有点让人觉得担忧，但是比特币并不能保证用户的匿名性。如果用户想将他们的比特币换成英镑、美元或者欧元，那么交易所就可以执行监管规定的身份识别、反洗钱、反恐怖份子融资等。此外，很多非常有意思的应用近期将会讨论实行用户审核制度，以决定是否接纳特定用户接入该系统。

第二个新兴的理念是支撑比特币的技术有很多非常有价值且正面的应用案例，并可以促进未来很多方面的重要创新。从法律与监管的角度来说，比特币的抗审查性是一个问题。所



以，从短期与中期来看，主要的公司与银行不大可能会与比特币及其相关的技术走的太近。

但是加密货币背后的分布式账本技术却是非常开放并且相当有价值。一个不被任何人控制的，且拥有着非常繁荣的开发者社区的开放平台，一次又一次的成为了创新的推动力量。他们可以让圈外者以及新进入者向之前被忽视的用户提供新的产品与服务。（第五章将会进一步介绍区块链技术所带来的潜在的颠覆性。）

尽管分布式账本技术的发明是为了实现电子现金这个目标，企业与其他机构正在积极的探索如果使用区块链技术来解决其他各种紧迫的问题。例如，企业经常发现带有权限管理的区块链远远比没有权限管理的区块链更加吸引人，因为特定的组织需要可以授权去验证交易。这使得企业能够创建一个涵盖互信的企业与个人的安全的、私有的网络。（第三章将会进一步讨论需要许可与不需要许可的区块链网络）。

总而言之，这个技术在中心化程度是连续性的，可以根据中心化的程度进行划分（比如根据无需许可的程度来划分，见图一）。然而中心化并不是这个领域内分析不同类型技术的唯一维度，其他还包括对于一个资金使用目的的定义程度（如只有父母签名后，孩子才可以使用某笔资金）以及代表除了金钱以外的其他资产的可能性（比如证券乃至所有权证明）。

FAQ

比特币与其他货币根本的区别在哪儿？

比特币可以被任何个人所持有，而不需要得到银行或者政府的许可。比特币可以被发送给任何一个拥有比特币“钱包”的人。这就是立法者与监管者所担心的比特币的本质突破：**抗审查性**。

图一：不同账本技术的不同的中心化程度

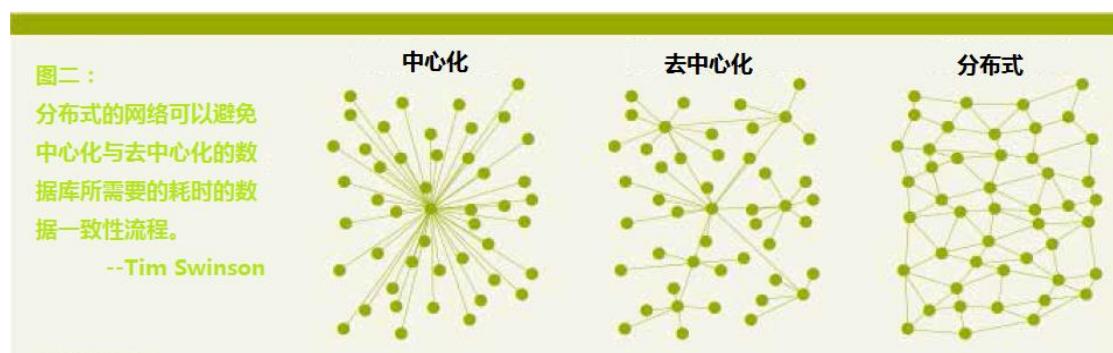


潜在的应用

分布式账本技术可以解决的问题归纳为三点：成本、备份、对账。

以银行业务为例，每个银行都会建议或者购买至少一套（一般是好几套）用于追踪与管理金融交易的系统。每一套系统都需要资金去建造以及更多的资金去维护。这些系统之间必须彼此相连并通过一系列对账的机制来保持一致性。每个银行相关的小组的成员需要与其他银行相应的人员进行确认，确保交易信息能够匹配，并能够在交易信息不匹配的情况下解决问题。

最常见的方式是建立一个单一的、中心化的、被所有参与者共享的账本。英国这个方面已经有很多成功的应用，特别是快速支付服务（Faster Payments Service）。但是中心化的系统的成本通常很高。同时，由于数据的存储及处理是中心化的，所以这个系统必须有所有参与者的系统进行整合。而相反的是，许多去中心化的数据库并不需要经过中心就可以完成信息的传递。（见图 2）



图二： 分布式网络可以避免中心化与去中心化的数据库采用的耗时的对账过程。

相反，比特币通过互联网来同步分布式网络中的几千台计算机。如果我的计算机认为我拥有一个比特币，那么比特币网络中的每一个计算机都会认可。如果银行系统可以用同样的技术，那么在不需要大量的人员来保持数据一致并维护系统的情况下，银行的系统之间也可以保持数据的一致性。关键的是，我们并不需要比特币来达到这样的目标，因为是其底层的分布式账本技术提供了可能的解决方案。

这可以帮助解决金融服务中最大的问题：使用纸质文件的成本。在近些年，有很多举措来试图在经济活动中不再使用纸质文件。然而，在很多场景下，新的技术只是用一种新的方式在实现原有的流程，或者是在其他的步骤上继续使用纸质文件。例如，向出口商提供金融服务非常依赖纸质文件。通常出口商的银行根据进口商的银行发行信用证明来事先向出口商付款。虽然这个过程是电子化的，但是随后的验证过程却要依赖于全球范围内大量的纸质文档。与此相反，分布式账本技术可以利用一些更加快速与无纸化的处理流程来取代一些基于纸质文件的银行业务。工程与物理科学委员会(Engineering and Physical Sciences Research Council)已经开始支持对于这项金融应用的研究。（详见研究与水平扫描的案例）

但是这个机遇不仅仅限于银行业。医疗行业（病历保存）、政府管理（土地登记与福利发放，详见第六章）、电子工业（包括物联网，详见第一章），甚至是艺术与珠宝行业（追踪钻石的原产地）都可以使用分布式账本技术。



Case Study 案例研究

研究与事件扫描

John G Baird, 英国研究工程与物理科学研究委员会 RCUK 数字经济课题领导人

英国研究工程与物理科学研究委员会（Engineering and Physical Sciences Research Council）代表英国研究理事会（Research Councils UK）发起了数字经济项目。从 2008 年起，数字经济项目在应用性多学科研究课题上共计投入了超过 1.7 亿英镑的资金。这个项目主要关注经济数字化带来的社会挑战以及其对于社会融合、农村经济、个人信息、安全、身份、可信赖性及隐私所带来的影响。在 2015 年 3 月的预算中，数字经济项目提及数字货币与物联网相关的研究活动。截止到目前为止，在分布式账本技术上，我们已经资助了以下一个方面的研究活动：

- 1、 加密货币对于数字化进程的影响项目（Cryptocurrency Effects in Digital Transformations, CREDIT）¹。这是一个时长为 18 个月的研究金额为 40 万英镑的研究项目，主要目的是从电子转移、隐私、社区、机构四个方面来研究加密货币现象及其底层技术—区块链技术。预期的主要研究成果为：
 - 帮助创业公司及现有公司考虑在他们现有的产品及服务中整合区块链技术可能出现的问题的帮助文档；
 - 与关注加密货币潜在影响的公司的共同进行的小型前瞻性研究；
 - 能够进一步开发这项早期技术的学术研究者与专业人员的社区；
- 2、 CREDIT 项目是基于我们之前支持的两

个研究结果进行的。这两个研究分别是：“加密货币的颠覆性角色”² 与 “ICT 与金融服务的未来”³。这两个项目都评估了对于加密货币目前的理解，以及揭露了加密货币对于社会、道德、法律及监管的影响的理解空白。因此，我们近期发布了一个预算为 1 千万英镑的“数字经济的信任、身份、隐私与安全”⁴ 为主题的研究计划。而“更加广阔的分布式账本技术应用”是其中的六大研究领域之一。个人、社区或者政府想要对这项系统产生信任并予以使用则需要对于社会、道德、法律以及商业架构都有着深刻的理解。而这个研究领域就是研究如何融合与权衡这种理解与分布式账本系统的先进技术。最终，我们希望这项研究能够为可以支持不同场景下的个人、组织之间，甚至是智能物件之间的货币或非货币的价值交换的智能经济做准备。

3、 最后，我们向“资本的第三方去实物化与重新实物化”（3rd Party Dematerialisation and Rematerialisation of Capital, 3DaRoC）⁵ 项目资助了 26 万英镑。这个项目旨在基于对于两个零售金融组织（Zopa Limited 与 Bristol Pound）的研究来建立一个高效的数字零售金融服务。其中 Zopa Limited 是一个 P2P 借贷公司，而 Bristol Pound 是一个社区货币。这个项目已经建立了一个在线的工具包以帮助那些有兴趣解决会对数字金融产品设计与使用会产生影响的用户与企业。

值得强调的是分布式账本技术还处于非常早期的阶段。在这些应用可以被实现之前，还有很多问题需要解决，包括隐私的问题、性能与可扩展性。这个技术是否完善到可以得到银行的信任？谁又会来建立这样一个共享的、不容易收费的平台呢？

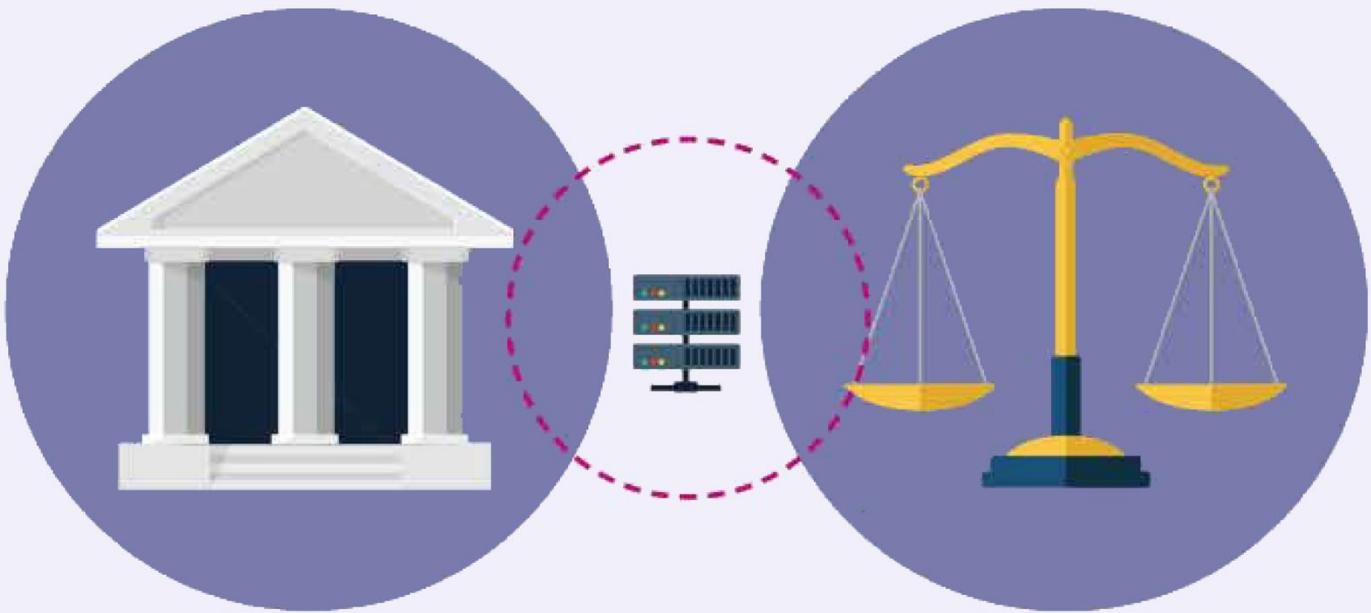
但是这个领域发展非常快，很多问题已经在解决当中。目前已经可以区分出这个技术的哪些部分是可以随着时间改变的，那些部分是固有不能被改变的。我们已经看出分布式账本技术可以使得公司与政府更高效的运行，而且不用再担心高昂的对账及备份成本。这个技术可以使得现有企业与新进入者在提供新的基于开放的安全的共享数据服务与产品上可以进行平等的竞争。

除了带来抗审查的电子现金以外，分布式账本技术还可以带来更多的可以改变世界的变革。



治理和监管

Governance and Regulation



法律和数字领域都是由一些规范所管治着 ,但这些规则的本质并不相同。在数字环境下 ,法律(法律规则) 和软硬件 (技术规则) 均管理着行为活动。在罗列针对分布式账本体系的规范时 ,前述两者的影响均需要被考虑。



Author

Vili Lehdonvirta, Oxford Internet Institute, University of Oxford;
Robleh Ali, Manager – Digital Currencies, Bank of England

第三章 治理和监管

引言

本章针对的是分布式账本体系的规范和规范制定问题。我们将区分法律规则（由法律义务组成的规范）和技术规则（软件和协议）。我们同时还将区分治理（某一系统的业主方或参与者制定规范，以保护他们的私人权益）和监管（外部机关制定规范，以代表公众利益）。

法律规则和技术规则：两种不同的规范

所谓金融系统，既是机构之间的一系列法律义务，又是这些义务的一系列数字记录。法律和数字领域都是由一些规范所管治着，但这些规范的本质并不相同。

在数字环境下，法律（法律规则）和软硬件（技术规则）均管理着行为活动。在罗列针对分布式账本体系的规范时，前述两者的影响均需要被考虑。在关于这个主题的一份独创性文献中，哈佛大学的 Lawrence Lessig 论述了这些法律和技术规则如何互动性地管理着行为活动。Lessig 主张：在数字环境中，法律（法律规则）和软硬件（电脑代码）均规治着行为活动，而在构建监管理论，该两者的影响均需要被纳入考虑范围。在本章中，我们使用技术规则一词而不是电脑代码。该定义同时涵盖了软件和协议，因为分布式账本需要同时依赖这两者才能发挥作用。

法律规则和技术规则的一个根本区别在于：它们各自影响行为活动的机制有所不同。法律规则是“外部施加的”：该规范可以被违反，但相应地会引发特定后果，这样才能确保规范被遵守。而相比之下，技术规则是“内在固有的”：如果该规范被违反，那么就会反馈出来错误，导致没有行为会发生，因此是通过代码自身的运行确保了该规范被遵守。软件的另一特征是：机器会刚性严格地执行规则，哪怕遵守规则会导致产生那些未预见的或不想要的结果。这导致了运行分布式账本系统和当前金融系统两者之间存在着显著差别。

1. 当前金融系统：法律规则之治

现代金融系统早已很大程度上被数字化了，而且严重依赖着技术规则。机构之间法律义务的数字记录的创造和修改，都由该技术规则来管辖。金融监管所瞄准的是这些法律义务产生的效果：例如一个银行是否有充足的资本或流动性。金融系统早已被技术规则和法律规则两者的这一套组合拳所管治起来，但金融治理和监管在传统上更侧重于后者。

法律规则之中公共要素的执行属于金融监管部门的一个专业团体，负责确保系统的参与者遵守法律规则。参与者必须提供监管者所需要的信息，以供评估参与者是否遵守系统的规则。如果某一机构未能遵守，则监管者可以采取行动让它们守规矩。但这不是说技术规则在



现有监管过程中就没有影响力了 - 而只是说：治理和监管目标是通过提供法律规则（而不是改变技术规则）而实现的。

2. 分布式账本系统：技术规则之治

像比特币这样的分布式账本系统已经显示了它们能够在没有法律规则的情况下发挥作用。每一参与者必须遵循的规范反而是仅仅由技术规则所定义并执行的。网络中的每一参与者运行着相同或兼容的软件，该软件界定了什么样的交易是被允许的。例如，比特币软件只允许参与者花掉他们能够用密钥证明拥有的余额。比特币软件同时监管着新增货币如何发行出来，并对货币池内的总量规模施加了一个刚性上限。既不存在任何内部规章制度或其他法律文件来载明前述规则，也没有人来执行这些规则 - 分布式账本系统完全由它们的技术规则来管治。

为防止参与者通过修改他们的代码副本来签发违反规则的交易，每一交易在登录到账本上之前需要被验证。在诸如比特币这样的一个“无需权限”的分布式账本系统中，验证者（即常说的“矿工”）通过随机的方式来进行选定。通过一个经济激励的系统，账本系统希望确保验证者们的诚实性，这一过程由软件所控制。而在一个“需要权限”的分布式账本系统中，验证者由系统的业主方进行任命，他们的诚实性由常规方式（比如法律契约）进行确保。

综上，分布式账本系统与传统金融系统是不同的，差别在于前者是由技术规则所管治，而不是法律规则。这样做的一个优势在于合规成本很低：参与者仅仅需要使用一个合规的软件包来签发交易。虽然执法成本看上去可能会甚至更低，但这并非必然如此，因为在所有最受欢迎的分布式账本系统之中用于验证交易的挖矿系统消耗了大量计算资源。该成本必然最终由系统的用户承担。（译者注：现时亦有无需耗费大量计算资源的分布式账本方案。）

治理与监管：两种制定规则的方式

由于当前金融系统和分布式账本系统主要由不同种类的规则所管治，我们因此必须问这样一个问题：谁来制定规则？

1. 当前金融系统：私人和公共的规则制定的协调配合

在当前的金融系统，法律规则被制定存在于许多地方，但粗略地可以把它们分为两类：私人的规则制定（治理）和公共的规则制定（监管）。私人的规则制定之典型例子是金融服务公司 Visa Inc. 颁布的“Visa 核心规则”，旨在管治 Visa 系统全体参与者的行为。这一私人的规则制定的制定人是 Visa 这样的私人金融网络的业主方，以及希望能够互惠互利地协调一致行为活动的金融机构的私人协会。而公共的规则制定的例子是英格兰银行对于 Visa 欧洲支付系统的法定监督。

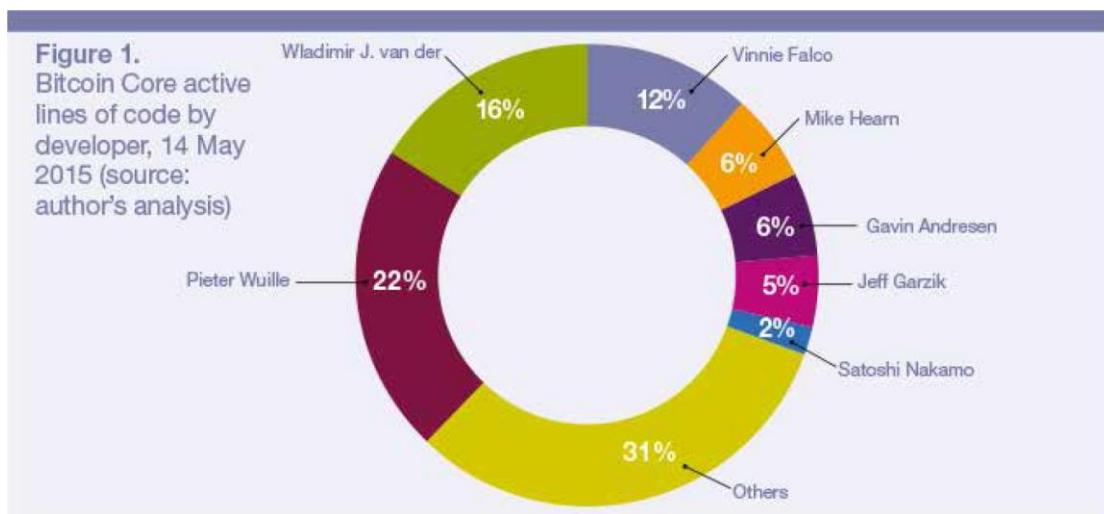
当前金融系统中公共法律规则的设计是政策制定者的领域，政策制定者需要考虑对金融系统中不同机构的规范效果（“微观审慎”方法）和对系统整体的影响（“宏观审慎”方法）。

由于金融系统是全球性的，像巴塞尔银行监督委员会这样的国际组织从全球各地召集政策制定者，以达成能被转化进入各个特定司法辖区的立法中去的自愿性协定。

2. 分布式账本系统：非制度化的私人的规则制定

“无需许可权限”的分布式账本系统有时被视为独立地存在于人类规则制定之外，且仅由数学算法进行治理。这是一个错误的想法。就像法律规则一样，技术规则需要由那些定义了代码所体现的规则的人类造出来并进行维护。用比特币来举例，该软件的初始版本由中本聪（一个化名）发布。2010年，中本聪把项目的控制权移交给了 Gavin Andresen，一个澳大利亚出生且在美国生活的程序员。和任何软件一样，比特币需要定期更新来解决缺陷、安全问题和操作环境的变化。每次更新在原则上可以改变软件的所有方面，包括记账和所有权规则。因此，谁来写这个软件、如何管控该等流程，就成了对分布式账本系统中所有参与者至关重要的大事。

就比特币而言，其软件由一个非制度化的流程所管控，其中涉及一批非正式的机构和实权大户。图1展示了写了最多比特币代码的人。该软件是开源的，任何人可以提议修改，但对于软件官方版本的修改进行承认的技术权力掌握在一个由 Andresen 任命的五个核心开发者所组成的团队手中。核心开发者的权力由一份非正式的自我施加的章程所约束，其中规定了规则的重大改变需要获得社区的广泛共识。对该软件的任何更新必须进一步由大多数矿工（按照他们贡献的算力来计算）所安装后才能让修改生效。因此，在决定矿工们是否以此方式批准该软件的一项更新时，控制着所谓矿池的那一批人具有很大影响力。



当修改代码是并无争议的修改缺陷时，上述治理程序运作得很好。但近期开始有了崩溃的迹象，因为某些决定需要抉择出持币人的哪些利益需要置于其他利益之上。Andresen 和其他人声明这一程序需要变得更正式化。社区正在争论这一正式的治理系统应该是什么样的，但这问题很复杂，因为事实是比特币的建立基础乃是一种反体制化的精神。这是一个有意思的进退两难，因为它证明了法律规则的价值，并显示单单用技术规则无法产生最优结果。



在“需要许可权限”的分布式账本系统中，软件的治理较为简单，因为通常已存在一个对代码拥有着明确法律和技术权力的业主方。由业主方来决定代码如何修改，而由用户（通常是接受服务的客户）决定他们是否愿意让业主方行使对于软件的权力。服务等级合同和其他常规手段可以用于建立责任制和对之予以执行。“需要许可权限”的分布式账本系统在此方面，与诸如 Visa 这样的传统私人金融网络或是“软件即服务”（SaaS）之间的差别并不大。

我们应当如何监管分布式账本系统

上文所描述的分布式账本系统中的治理涉及到了系统中权益持有人的利益，但分布式账本系统如何运作也可能牵扯到更广范围的社会利益。例如，监管者可能希望征税、起诉犯罪分子以及限制分布式账本系统用于犯罪目的。如果一项系统被采用后，开始对社会的其他地方产生潜在的撞击效应，则监管者可能同时希望确保该系统对于系统性风险和市场失灵具有抵抗力。这一监管方式可以通过法律规则或技术规则而得以应用。

1. 通过法律规则来监管分布式账本系统

监管一个“需要许可权限”的分布式账本系统，就是简单地把法律义务施加给其业主方。而通过法律规则来监管一个“无需许可权限”的分布式账本系统（比如比特币）就比较复杂了，因为没有一个单一的法律实体控制着系统。对于人们被允许在电脑上安装什么软件，这很难进行监管。尝试通过法律规则来监管比特币因此转而侧重于监管那些处理比特币的企业，比如交易所和钱包服务商。对于这些企业，可以对它们本身进行监管（例如防止钱包服务商卷了客户的钱而消失），或者以此作为手段来间接地监管相关账本的用途（例如确保反洗钱规定被遵守）。

一个通过法律规则来监管比特币的知名案例是“数字货币许可证（Bitlicense）”，它由纽约州金融服务部门向为纽约居民提供数字货币服务的企业颁发。企业获取该许可证的截止期限是 2015 年 8 月 8 日，未获得许可证的服务提供商会被处罚。

2. 通过技术规则来监管分布式账本系统

比特币这样的分布式账本系统的技术规则目前由私人通过非制度化的程序来制定。但包含了软件和协议的技术规则，同样可以从公共部门出现。例如，TCP/IP 和其他一些互联网核心协议就是政府出资的研究项目的成果，现在则在互联网协会（一个国际非营利性组织，具有基于地域和特别利益的开放式成员结构）的资助下进行维护。互联网基础设施的其他部分由国际性的多方权益人程序进行维护，而一些部分仍旧在美国公共监管者的监督之下。

虽然这一东拼西凑出来的东西远非完美的解决方案，但它指出了在制作技术规则方面的公共参与和民主代议的可能性 - 通过技术规则而不是法律规则进行公共监管。

表一： 由私人制定的与由公共部门制定的法律条款与计算机协议示例	法律条款	协议
由私人制定的	Visa核心准则	金融信息交换 (FIX) 协议
	快速支付服务准则	比特币
由公共部门制定的	欧洲市场基础设施管理规定	互联网 (TCP/IP)
	BitLicense	万维网 (HTTP)

若运用于分布式账本系统，这可能意味着任何事情都能发生，无论是启动正式的多方权益人程序来维护技术规则，还是开发代码的公共标准。如果通过影响内嵌入电脑代码的规则，这能直接让政府或公众达成法定监管目标，那么就可能不那么需要由一个新的法律规则的机关部门来监管这些系统了。

另一种选择是公共部门也可以开发出一个“需要许可权限”的系统，这样能通过法律和技术规则的组合拳来发挥出公共监管的影响力，而不是像现在那样仅仅通过法律规则。互联网的某些核心技术已经显示了政府的确有可能成功地催化出私人部门行为活动的基础性技术规则。

结论

与传统的私人金融网络（诸如 Visa）所不同，像比特币这样的“无需许可权限”的分布式账本系统不存在一个对于整个系统承担责任的法律实体中心。相反，它们由非制度化的程序来进行治理，通常以创作了系统软件代码的那一小撮软件开发者为中心。如果这些系统的价值和影响力得以成长，它们就很可能需要发展出更加强健的内部治理程序。缺乏法律实体中心也会使得公共监管者在通过法律规则来监管分布式账本系统时更具挑战性。政府因此也应当考虑对那些定义了分布式账本系统之运行规则的技术规则施加影响，以此方式来监管分布式账本系统。要掌握良好的平衡，政府应当考虑技术规则和法律规则的各自优缺点，承认它们两者互相影响并且需要相应地作出设计。

比特币和分布式账本系统的出现，也把技术规则的问题带到了当前金融系统环境下的最前沿。分布式账本系统表明了金融系统除了能用法律规则外，还能用技术规则来治理和监管。政策制定者需要承认技术规则对于金融系统的影响，并要考虑如何才能把这种影响力纳入监管体系之中以成为其中的一部分，这能潜在地带来诸如降低合规成本之类的好处。



CHAPTER 4

Security 安全性和隐私性 and Privacy

分布式账本系统有很多种实现形式，每一种在安全性和隐私上都带来了不同的机会和挑战。在决定使用某种类型的账本系统前，应该要分析清楚相关的商业和安全需求。



Author

M. Angela Sasse, University College London, with contributions from: George Danezis and Sarah Meiklejohn, UCL; Daniel Shiu, Government Communications Headquarters; Phil Godsiff, University of Surrey

第四章 安全性和隐私性

引言

安全性可以简单地定义成：“应该发生的事情最终应该发生；不应该发生的事情则不应该发生”。对于任何特定的分布式账本技术和区块链技术的实施方案，技术如何设计、实施和治理决定了可以预见或无法预见的结果及其相关的风险。不同的参与者会有不同类型和不同程度的风险。

系统的风险不仅来自外部实体的攻击，也可能有来自内部参与者的攻击，以及组件的失效（如软件故障）。在实施之前，需要制定一个风险模型，并认清特殊的安全需求，以确保对风险和应对方案的准确把握。

有效的安全措施对保护个人或者组织的参与者来说是必须的，但并不足够。我们必须考虑到在特定的实施方案中披露出来的信息有可能会与其他来源的信息一起，被人们用于鉴别个人或者组织的身份，或者用来监视他们的活动。

创新的优势

比特币和其他加密货币的主要安全特性是网络的去中心化控制。这些系统是由一个全球的节点网络通过共识机制进行运作的（参考“定义”一节），所以没有一个中心的信任机构或者是单点失效的问题。这意味着任何恶意的攻击者都需要花费大量的资源才能对系统进行攻击。对个体用户来说，这个系统也能达到高度的安全性——为了转移钱包里存放的比特币，攻击者必须先知道与公钥相关联的私钥（只有私钥才能控制比特币）。因此，攻击者必须先要破解一个已有的密码学标准的安全性（椭圆曲线数字签名算法，ECDSA），才能盗取某人的比特币。

比特币和类似的“山寨币”使用了一个范围更广的计算机安全性基础设施——主要是分布式账本——被证明是有高度的完整性和一致性。这样的账本使用密码学技术去确保任何人可以检查账本内是否存在某个特定的记录，前提是他们掌握少量的关键信息。同时，复杂的共识协议确保系统中的任何人看到的账本都是一样的。这是比特币防止双重支付的重要手段，不过在类似记录合约或者契约的分布式账本应用的场合，这种特性也是很重要的。分布式账本账本技术可用于整合高级的服务，如公证、时间戳、高度完整性的档案管理，并通过自动化、轻松切换服务提供商和点对点交易降低使用上述服务的成本。

在线通讯的安全性依赖于确保某个公钥属于用户希望访问的服务商。公钥基础设施(PKI)



是一个自从 90 年代就开始使用的流行机制——实质上是一组被信任的第三方提供证书，去证明服务与钥匙之间的联系。不过这些证书机构已经被证明有可能出问题的；当这些机构被攻克（译者注：无论是来自外部的还是内部的），都有可能悄悄地发出无效的证书。

“透明证书¹”（CT）系统（最近由 Google 牵头，现在由一个工作组监管）使用分布式账本技术去缓解这个问题。所有的证书会被附加到一个分布式账本上，任何用户或服务都可以检查他们将要使用的证书就是账本里存放的证书。相应地，伪造的证书会被快速地发现——这会让那些寻求攻克或滥用 PKI 系统的人失去动力。

当用户想保护个人信息和通讯记录时，在钥匙和实体机构间建立权威的联系会碰到一些问题。不过当前的方案（如 PGP 可信网页或者中心化方案）要么就是不可用，要么就是有一些脆弱的安全特性。一个看上去不错的替代方案是 CONIKS²，它依赖于一个特别构造的分布式账本，去存储和调取用户的公钥，这些公钥可用于加密或者对邮件进行签名。与透明证书技术不同的是，透明证书技术依赖于第三方构成的网络去维护和审查分布式账本的完整性，而 CONIKS 使用通讯服务提供商和他们已有的用户数据库去建立一个具有高度完整性的账本。

安全性挑战

上面展示出来的分布式系统在安全性上的优势——具体来说是抵抗攻击的特性和健壮性——只对根据全球信任理论而设的无需许可的账本（译者注：公有链）完全适用。对基于许可的账本（译者注：私有链或者联盟链）或者其他中心化方案来说，抵抗攻击的特性和健壮性会弱一些，不过这有利于保证中心的控制及中心提供的功能。

实际上，就如第二章所述，在如比特币这样的完全去中心化系统和完全基于许可管理的私有专用网络之间是有一些范围很广的中间路线的。其中一个中间路线解决方案能够吸取两种特性的优点，就是英国伦敦大学学院的 George Danezis 和 Sarah Meiklejohn 提出的央行背书的加密货币³——依赖于一个中心化控制的服务器去建立区块链，同时使用分布式的“铸币节点”去吸收交易。

考虑到解决方案的多样性，在决定使用哪种类型的账本前先分析好业务和安全性的要求是非常重要的。

例如，若要为英国就业与退休保障部设计一个用于处理福利资金发放系统，维持服务的可用性和抵抗网络中断的能力是最重要的因素（参考第六章）。这其中最大的威胁会来自那些为谋取经济利益而攻击个体用户的高科技罪犯。因此：

- 因此，这个系统必须为用户设计成“傻瓜式”，用户不需要了解太多关于这个系统的知识也能够良好地使用这个系统，因此系统需要有数量适中的配置选项和参数，并明确地为用户展示出这些选项和参数可能会带来什么结果。
- 如果使用了一些像智能手机这样的商用设备，要确保证书和钥匙是通过安全的方式去访

问的，而且对其他应用程序是不可见的。

- 账本自身应该在广范围的服务器构成的网络中进行维护，以避免网络中断带来的影响。
- 若用于更大范围的部署，支付授权服务应该是在专用的硬件上放置的，而且要有防御攻击的手段。

若一个系统要用于分发对外经济援助，则需要确保交易的完整性（以防止资金被挪用到其他用途上）；并在灾难援助的情况下保持系统的可用性。这期间的威胁可能来自那些为地缘优势而干扰交易的国家，或者来自受援助国家的不诚实的人（译者注：政府雇员、机构或公民）。因此：

- 这个系统应当在一个小型的、巩固的和专有的服务器组成的网络上运行，这个网络建立了带有离线备份功能的、政府掌管的账本副本。
- 应该鼓励使用者去设立自己的账本网络，并给出如何做好安全性的建议，这些建议要考虑到让他们可以接受来自政府服务器的定期更新或者修正。
- 在怀疑严重网络攻击将要发生的时候，应该可以将系统切换到离线的状态。

可以说，对任何政府运作的系统来说，最大的威胁会是“被荒废”。如果太难使用，或者不能提供人们需要的功能，则不会被人们采用。

另一个最近呈现出的威胁，是在已有的系统内因不同软件的实施而创造出来的“分裂”让入侵成为可能。伦敦大学学院的密码分析研究员 Nicolas Courtois 之前密切关注过比特币，在 2015 年 8 月指出：

“使用新的版本号和新规则去挖掘区块是有可能的。这意味着让比特币变得更民主：更大容量的区块，更多的每秒交易性能，更低的费用，更广泛的采用。当前的比特币系统已经到了性能的上限了（这几个月里每秒不超过 3 次转账），比特币的开发者社区在修复这个问题时显得无能为力。”

这展示出任何由政府实施的系统，都要在治理这个问题上有前瞻的思维，考虑到可能存在的技术进展，以及如何防止其他善意或恶意的实体获取对这个系统的控制。

安全性建议

对技术的每个特定用途来说，政府应该仔细地分析相关的风险。虽然没有国家有兴趣破坏比特币的系统，但他们可能有兴趣去破坏英国发行的数字货币——如果塑造一个伪造的账本记录能够带来经济收益的话，那么有组织的罪犯可能会攻击那些忽视安全措施的用户。

根据已经明确的威胁，政府应该决定针对这些可能的攻击者制定合适的安全措施，以及某个具体系统的生命周期。若政府预期高科技的攻击者会针对这个系统，那么一开始这个系



统就应该考虑到相应的对抗手段。例如，无需许可的账本网络（译者注：公有链）有可能让一些人通过增加自己的服务器（译者注：可能是指算力攻击）或者是对合法的服务器发动拒绝服务攻击（D.D.O.S）；为了应对这些可能性，一个涉及国家利益的、长期续存的账本系统，可能需要抵抗量子计算机破解的签名技术。

将现有的基础设施采用到新的安全应用中要比直接创建一个安全的基础设施困难。因此，一组专用的、新型的、基于许可的服务器会比重新利用现有的互联网服务器更容易去配置和使用。建造这些安全服务器应该从英国政府通讯总部（GCHQ）或者有信誉的产业提供商获取建议。

为了创建一个可用于长期的系统，初始的设计应该包含在生命周期内可更新部件的功能（如可以将网络的节点更换成更先进的硬件；可以更换那些已经不再安全的加密算法）。

在技术的尝试过程中，应该提供专门的资金支持，去在系统层面和用户层面分别进行渗透试验。真实世界的攻击者或许不会有兴趣攻击一个小范围的概念验证系统，但当应用程序在大范围内部署时，这些攻击者就可能成为系统的威胁了。

隐私挑战

比特币这种加密货币从设计之初就是为了提供某种形式的别名身份⁵（它的创建者中本聪将这个特性称为“匿名性”，不过这是一种误解）。

用户可以创建一些钱包去存放比特币，这些钱包的数量并没有限制，也没有“了解你的顾客”（KYC）政策去限制创建钱包的行为。比特币是从一个钱包转移到另一个，而钱包与真实世界身份之间的隔阂会提供一定程度的隐私性。

允许别名身份及不将钱包与现实世界身份关联的决定，从实用主义的角度看，成为了比特币在世界上如此流行的原因。大多数辖区并没有将现实世界身份与在线交易关联起来的有效方法，若要将比特币挂靠到这样的验证机制的话，比特币可能也不会如此流行了。还有，考虑到比特币网络的国际性，目前还不明确哪个辖区应该被信任去承担这样的验证任务，而且也不知道一个法律辖区是否有权去识别某个用户。

最后，若设立钱包时需要提供身份验证的话，则会影响比特币作为一种货币用于兑换价值时的运作：如果身份验证提供商需要牵涉到交易授权的话，那么他们就有可能阻挡这些交易，或者选择性地拒绝某个用户的比特币对应的价值。其他参与者则会对比特币存储的价值将来是否能够无条件兑现产生疑虑。因此，比特币的别名身份让快速的采用成为可能（通过避开对仍未面世的或碎片化的身份验证基础设施的依赖），同时也保留了比特币作为货币的一些重要特性（如无条件地存储价值的特性）。

不过，用户与钱包之间的别名身份，并不是完全匿名的。钱包来往的交易记录构成的链

条对所有人都是可见的，公众可以跟踪这些交易。伦敦大学学院的 Sarah Meiklejohn 与同事一起，展示出交易的链条可以通过比特币的区块链实现跟踪，例如，通过交易所去盗窃比特币并提走的话，是有可能被跟踪的⁶。这个过程可用于强化一些“知道你的顾客”（KYC）的规则，因为当一个特定的钱包地址是联系到某个真实的个人，那么就很容易揭示出他们所有的交易记录。

这样的别名身份在匿名性上其实是很弱的，加上比特币区块链交易的透明性，在隐私性问题上带来了一些挑战。与传统的在线支付业务不同的是，传统业务只能被交易处理方和金融机构看到，而比特币的支付——从涉及到的钱包到交易的时间以及交易的价值——都记录在一个公开的区块链上。任何人可以通过观察区块链得出关于某事的结论，如某个在线商户的营业额、某个特定顾客的购物喜好甚至是私人之间进行的多次交易——以往有金融机构和法律执行部门去限制这些情况。

隐私性建议

有一些技术和加密货币项目提出了一些缓和完全透明区块链上的隐私问题的方案。

第一种技术引入了“混币”系统。它们从一些用户中提取一定数量的币，并将币发送到与原始用户无关的不同地址里面。通过切断发送者和接收者钱包之间的联系，提供了一定程度的匿名性。不过，设计这样的系统面临着两个关键的挑战。第一种问题是，这种匿名性并不是完美的：虽然币被发送到多个地址里了，但仍无法完美地隐藏所有的踪迹。这样的少量信息的泄露让“对泄露的信息进行统计学攻击⁷”成为可能，主要是用统计学的手段去在重复的交易中发现特定的模式，从而破解匿名性。其次，不诚实的“混币服务商”有可能收到币后不发送出去，实际上就等于盗窃了。一些比特币混币设计（如 Mixcoin⁸）尝试通过对混币过程某些部分的公开透明化去确保自己的正直性，而不影响对隐私保护的程度。

另一类系统在比特币支付的运作模式以及在区块链上记录的数据方式上作出了不少的改变，以提供更强的隐私保护。例如，Zerocoin⁹，Zerocash¹⁰，Pinocchio Coin¹¹，或者一些 Sigma 协议¹²在加密货币交易的设置中采用了群组签名算法。支付者提供一个“零知识证明”的证据，以展示他们拥有从一个列表中存放的一些币，但不透露具体是哪些币，而又对全网提供足够的信息去防止双重支付。这让他们可以在无需链接到先前的交易时就可以支付一个币。就如混币系统一样，这些技术可能只隐藏来自某个潜在用户列表里的收款人而不是所有的，因此还是有可能通过多个交易去对身份进行跟踪的。不过，这种技术确实可以脱离混币服务，因此能够降低混币服务商带来的处理性能限制或信任瓶颈。



CHAPTER 5

Disruptive Potential

颠覆性

潜力



分布式账本对于现有商业和政府管理模式显然是一个挑战。类似于分布式账本技术这样的创新，能够对现有商业架构进行颠覆，最终这样巨大的变化会让经济和社会本身被重组和变革。这样的变化远远超越了通常在产品、服务和操作系统上的创新。



Author

Phil Godsiff, Senior Research Fellow, Surrey Centre for the Digital Economy, Surrey Business School, University of Surrey

第五章 颠覆性潜力

引言

技术创新可以对企业的运作模式带来巨大的影响。新技术可以让企业提供新的产品和服务、能够获取新的收入来源、降低运营成本、并精简其组织结构。如果现在的企业开始逐渐采取新的技术，或者试图建立新的进入壁垒，新进入者就可以利用创新优势来取代目前在职人员。

足够激进的技术创新可能会导致革命性的变化，不仅是商业模式或者是整个行业，也许会最终改变社会的组织和管理方式。例如，蒸汽机导致了铁路的发展，而带来的人口流动使得城市中心得以建立。

分布式账本技术（DLT, Distributed ledger technologies）已经在现有的行业框架中，在产品、服务收入来源和操作系统等方面显示出具有颠覆性创新的潜力。他们有颠覆现有整个经济和社会的潜力。理解这些，可以帮助了解分布式账本技术带来机遇和威胁的整体状况——以及他们可以重塑政府的角色，和政府提供的服务。

创新的角色

FAQ

组织通过不断的创新来提升他们自己的竞争优势。我们倾向于认为，通常新的创新是发生在产品和流程层面：制造业专注于产品创新，而服务行业会发展流程工艺创新。即使是很小的创新都有会影响整个行业结构。创新也可以发生在商业模式，通常是在行业中建立“竞合关系”，这是一种企业之间既竞争又合作的关系。

什么是分布式账本技术的颠覆式潜力？

分布式账本有一种较为激进的颠覆性潜力。这部分是因为它们已经促成和与生俱来的（例如在密码学和软件工程）；它们可能进行创新的行业和服务（例如金融服务、房地产、医疗保健、身份管理）；和它们的处理能力（如低成本、实时、无法篡改）。但是它们的颠覆性潜力还在于它们分布式共识、开源、透明度和社群的基本理念。

数字革命带来了越来越深入的认识，创新可以发生在商业模式的层面，甚至是整合行业——你只要想一下Uber这个应用，通过让客户在他们周围雇佣司



机，将会彻底打破出租车行业。从短期的利益到长期的创造财富方式，将会改变一个组织的观点，将会导致从根本上改变活动方式和对于未来的看法，例如通过使用开源软件来建立平台，让任何都可以修改和使用。

技术创新，就像应用软件，现在让客户可以资金进行资源整合，通过“拉”这样的解决方要，而不是让供应商来“推”。这也许将会挑战目前对于价值创造的假说，例如，“产销”（这是一种让同一个人既是生产者优势消费者的模式，就像共享乘车服务BlaBlairCar和住宿租赁服务应用AirBnb），以及P2P借贷和众包模式。

这种形式的创新最终会影响整个行业的机构，并有潜力来建立一个新的行业；它改变了“谁做了什么”和“谁得到什么”。新进入者开发的移动支付系统，正在开辟新的客户基础（例如通过让小商户可以把自己的手机变成银行读卡器）；以前没有使用的数据可以发送到给新的利益相关者，从而创造新的收入来源，以获取价值；并且有越来越多的人开始使用数字钱包，并且使用不同的操作系统，例如使用移动手机服务（如M-Pesa），而不是银行。但是在许多情况下，目前的交易依旧是使用旧系统（如清算银行和像Visa和Mastercad互相竞争的信用卡方案）。M-Pesa挑战了这种情况，即交换价值必须通过银行这种传统思想，而新的创新可以实现跨越式发展。但是，这些创新也是与现有的传统结构相结合，也是使用特定的技术和值得信赖的中介机构。尽管能够提高用户的便利性，显著降低成本，对用户和消费者而言，这更像是一次进步而不是革命。

技术革命

创新往往带来增量，但是通常会以非常激进的方式出现，经济学家熊彼得称之为“颠覆式创新”，也被Carlota Perez称为“技术革命”。这些创新在许多技术、经济和社会之间以复杂动态的方式出现，某些时候创新有可能会从根本上改变特定社会或者经济的组织形式。

在过去的几个世纪，我们已经看到了这些技术革命：原来的工业革命、铁路革命和石油革命。这每一次都改变了产业结构，带来了能源的全新形式，并且影响了社会的组织方式。现在我们处于信息革命中，其特征是信息强度、连接度和专业化和全球化。

这些革命通常有三大特征：显著降低成本、全新的通信方式、和改变基础设置和逻辑。大规模降低投入的成本会让市场变得紧张——并且经常会导致金融泡沫崩溃——这最终将会让形成对现有机构进行全面检查。根据Perez的说法，革命性创新的特征是“由一组相关联的事物出现根本性的突破，形成一个

互相依赖的技术组合”和“强大的参与系统在他们技术和市场中互联，并且会深刻的改变经济的其他部分（最终改变社会）”。

每一种技术革命都带来一组不同的“常识原则”，改变企业和社会的运作。这些从工厂的机制开始；通过经济的规模和垂直整合，大规模生产和标准化；到功能出现专业化，出现层级的金字塔和官僚结构；而今天信息强度和去中心化的网络，特征是“异质性、多样性、适应性和合作”。这些革命最终会导致新技术经济的范式转变，具有不同的成本结构，不同的创新机会，并建立明显不同的组织原则。在每一次范式革命，组织会沿“S”曲线发展，从颠覆式创新，通过使用和利用（和反抗），变得成熟直到替换。改变现有的思想，并且用新的取而代之是需要一个巨大的转变过程，需要新的技能、能力和知识，从而从根本上改变企业的运作方式。

前面技术革新对于金字塔、组织的层级系统、以及政府几乎没有影响。但是现在有些人建议，我们新技术时代也许会出现一个目前还不明显的“普遍协作”，因为社会是由合作利益驱动的而不是个人利益。这就是意味着变成分布式的共识社群结构，不需要有层级的中介（例如银行和政府）。分布式账本技术正是代表了这种挑战。

	描述	年份	新技术和行业	新基础设施	常识原则
第1次	工业革命	1770	机械化工业	运河和水利	工业制造、生产力、本地网络
第2次	蒸汽和铁路	1830	蒸汽机、铁机械	铁路、电报、港口	集聚效应、标准化零件、城市化
第3次	钢铁、电子、重型机器制造业	1875	低价钢铁、重化工业	电网、全球航运	规模经济和垂直整合，科学是生产力, 效率
第4次	石油、汽车、大规模制造	1910	汽车、低价石油、石化、家用电器	公路网络、通用地	大规模制造、横向集成、标准化产品、能源强度、郊区化
第5次	信息和电信	1970	低价微电子、计算机、移动电话	全球范围的数字通信	信息强度、去中心化网络、知识即资本、专业化经济、全球化

表1：五次技术革命 (Perez整理)



分布式账本技术

分布式账本技术参与一些相关领域潜在革命性创新：数字货币、分布式开发和透明的记录保存、不分等级的网络系统、密码学和软件工程。分布式账本技术代表一种朝着激进方向的创新，因为它有潜力影响到大范围的商业模式：从新的产品到服务，通过操作系统和组织结构，并且还有许多潜在的行业可能会影响。因此，他们会互相关联，并且和内部关联突破，形成一次技术革命。

案例研究1

钻石

Everledger的创始人和首席执行官，Leanne Kemp

钻石行业是一个很容易出现犯罪活动的行业。钻石体积很小，而且能够以隐藏的方式来传输，交易可以被保密，而且钻石在很长的时间内都是保值的。因此，钻石经常被卷入到全球范围的洗钱或者恐怖主义融资行为中。

努力遏制这种非法活动，包括通过纸质文件来追踪钻石和确认它们的来源。但是，文件篡改是非常普遍的行为——事实上，文件经常用于创建来掩盖非法交易的一目前几个主要进行钻石交易的国家，仍旧没有足够的法律来防止这些犯罪。

为了解决这个问题，钻石行业开始实施一个名为Everledger，基于区块链技术的系统，它能够为每一颗钻石建立一个数字“护照”。能够记录来源、经历，和通过一个唯一的数字加密“指纹”进行交易。

这个系统有三个阶段：

- 为每一个钻石建立一个e-ID（电子身份），通过数字化它的属性，将激光

刻下的序列号放置在一个可以认证的区块链账本上。

- 为钻石指定一个数字护照来记录它的履历，交易历史和起源
- 检测和防范非法活动或者欺诈行为。

通过使用不可更改的区块链来保存数据，分布式账本可以完全透明的提供所有钻石、揭示它们的来源，跟踪它们的所有权，以及它们可能经历的过程。这种账本可以作为钻石行业、政府、消费者市场、边境管制和执法力量的一个单独可以验证的强大工具。

这个系统也能够使用智能合约——能够将钻石销售和传输的条款和条件相关联，就能自动开始执行。通过使用区块链来建立一个分布式账本，智能合约可以用于追踪，验证业务关系和协议。区块链的透明度能确保合同得以执行，根据钻石所有权，钻石的融资情况，保险条款，注册权等等。通过真实性证明文件的认证交易，将会为政府和支付机构提供重要的证据线索。

分布式账本技术对于操作成本上有巨大的好处。它们不仅内部成本很低，还能够避免重复和无效率的管理和协作，通过一个通用、公开、能够完成工业级的操作，就像通过在每个个人持有的账本和数据库进行交叉检查，这样可以降低因为流程造成的技术。它可以数字化和安全的存储任何资产的信息，从钻石到几袋大米，能让企业标识并跟踪他们的所有权和位置（参见钻石认证的案例）。通过使用分布式账本技术，通过开发可编程的智能合约来进行记录和传递价值：例如以太坊（Ethereum），是一种称为“智能合约（Smart Contracts）”的去中心化平台。他们具有颠覆性的潜力可能会扩展到任何一个新的场景，只要存在具有信任或者被垄断经营的中介——一个“中心辐射”模式——都会被涉及，或者被更开放的模式取代，基于更加扁平社区的共识结构（参见公司行为案例）。

分布式账本技术的开发和相关联的技术提供实时记录交易的可能性，使得交易更加快捷、成本更低（参见SETL案例研究）。例如，汽车保险可以基于汽车和它驾驶者的情况，保险可以根据行为、价格和风险偏好来进行动态改变。由此将会诞生“可编程经济”，通过智能合约，依靠去中心化的网络和机构，只需要很少的人参与，作为一种分布式自治组织来大范围提供产品和服务。

分布式账本技术最好的例子就是数字货币——比特币，也是金融服务领域中最让人印象深刻的创造新货币。分布式账本技术将会在现有结构和治理下，能以很低的成本进行运作，提供减少整个系统成本和复杂度的机会。他们可以通过去除重复和独立专有系统的成本，并且挑战这些系统中心化的架构。例如，货币创造也许以后不再是某个单一国家政府的责任或者特权。相反，获得这种全新的货币形式，也许还能够让货币和身份结合在一起，并且链接人群，成为社群内认可和交易的手段。

技术进步能够继续进一步发展，有可能在基础的比特币增加其它特定的属性（例如，物理资产或合约），就变成所谓的“彩色币”。这开辟了货币的多种可能性，不仅仅是价值尺度：它可以有许多特别的属性，比如可以指定用途、有效期或者允许使用的地址。例如，货币可能会限制购买用于购买几种物品和服务，可以被用于某种指定用途（兼第六章）；或者某人可以通过Airbnb

FAQ

什么是分布式账本带来的威胁？

如同任何激进的创新，分布式账本也给了传统机构机会，但也会威胁到那些没有或者无法回应的机构。尽管分布式共识的属性会威胁那些在层级系统中处于控制地位、可信任的中介角色。区块链有能力来创造一种货币，例如比特币，将会挑战当局在管理国家的权威，以及全球经济和货币体系。



租用一件房屋，如果他们不能按时支付或者合约已经到期，则电子门径锁就会被关闭。

政府的考量

由于有着广泛的利益相关者、服务和角色，政府显然需要有各种不同的操作方式。有些是在分配价值而不是创在价值，而其他有些事在创建和保持有效的监管制度。许多这些活动都会由创新企业通过分布式账本来突破，并且改变其它的领域。改变是可能发生在产品和服务层面，然后会在运营和组织层面。

案例分析2

公司行为

COOConnect创始人，Dominic Hobson

上市企业必须要以结构化格式来提供他们的年度账目，但是任何企业的公告需要投资者或者他们的代表同意后——这被称为“公司行为（Corporate actions）”——通常发表为一份非结构文本，或者是PDF格式。那些以来这些信息来采取行动的人，必须通过人工阅读和解释相关数据。

超过90%的公司行为是由数据供应商来发布的，然后由代表投资者的代理机构来进行处理，如托管人或者是基金经理。信息是从来源人工提取的、解释和重新录入的。不仅自动化水平很低，而且错误频繁，处理效率非常低下。有人估计，公司行为处理成本每年大约高达100亿美元。托管人经常需要因为错过了或者不正确执行，从而赔偿客户损失。

区块链技术能够让整个过程变得更有效率。公司行为代表了合同化信息和价值，原则上能够直接自动在收付款人之间进行传输，而不需要有中介参与，为各方提供可以信任的数据源，并且具有必要的经验来处理收到的信息。

如果区块链能够连接一个应用，用于捕获和存储结构化格式的企业行为公告，它就能够用于确保该数据是来自一个可以验证的来源，并且验证它发布时候的时间戳。这也能够用于反向执行来完成。一个基于区块链技术的分布式账本，能够让参与的各方来确保信息的是精确、及时的，而且从发布者到他们手上都是未经篡改过的。

从理论上讲，它可以消除发布者和基金经理之间的所有中介机构，保证信息的准确性和及时性。

重要的问题是，这些是不是都可以通过一种完全去中心化的方式来组织完成的。企业行动信息不同于简单的合约信息（例如资金易手），因为投资者和股东们经常需要使用中介机构所拥有的专业知识来采取他们的行动。

这些中介机构可能会在信息通过他们前修改或者变更数据，经常会出现原始公司行为已经被改变，通过后续发布公告将会要求取代较早时间发布的公告。当数据提供商和他们客户进行分享，或者将其数

据进行打包，这些修改的数据能够快速失去其来源，让整个过程难以自动化执行。1

就其本身而言，区块链技术目前在处理不断变化的数据包时，速度还是比较缓慢。比特币区块链每小时只能处理2万笔交易，必须要长达一个小时的时间才能信任一笔交易。这对于公司行为过程是非常不方便的，由于受到最后期限的问题，基金进行往往需要需要尽可能长的时间。

位于Monmouth的公司Code1，正在处理公司行为数据，其提供的基于区块链系统的数字认证软件，已经克服了这些问题。这个系统将创建一个不可更改的审计追踪，让链上的各方能够参考，来鉴定其真伪，提供有关数据来源的有价值保证。

他们在行业参与者和Code1之间有一个协作企业，一个可以搜索的企业行动信息并且登记在注册表中。这个注册表数据是以ISO 15022和ISO 20022格式进行存储，并且对金融信息提供提取的规范，能够转变为机器可以读取的格式，这意味着注册表能够根据公司行为对信息进行修改或者替代，实时进行更新。这保证了信息的完整性和精确性，通过SWIFT安全网络，能够让参与公司行为链的各方都可以使用。这克服了单独使用区块链造成的验证延迟，和信息——作为分布式账本有效分享——能够被更新、发布和实时修正，确保是正确和最新的。

政府可以通过改变规则，要求企业来发布企业行为信息时启用分布式账本接口，来让该系统获得进行更好的发展。

例如，确保资金转移的过程，就像将福利支出在正确的時候发给到正确的人，这个流程可以有许多方式进行提升（参见第六章）。在单个保险账本中记录身份和潜在受益者信息，实时进行更新，将会是一个更加激进有效的创新，同时降低运营和开发的成本。在一个特定支付中添加属性，意味着数量、目的和支出的时间可以被指定和追踪。这当然，需要和所有利益相关方进行广泛磋商，并且能够对这种形式的数字货币进行一定的管理，确保各方期望都能获得满足。

还有许多创新，通过分布式系统可能会取代目前的分层级组织。政府和它的机构往往维系着权威性，包括内部和他们各自的系统中：例如，公民是被他们本地所选举的政府机构，国家或者超国家机构所代表的；金融事务是由清算银行、清算所、中央银行和政府运营的。与其依靠这种主要基于纸张记录的投票机制，民主可以通过基于区块链的投标系统完成，每个选举人有一个数字钱包和一个“投票币（vote-coin）”。这能够有效降低欺诈（因为每一个选民都可以检查他们的投票是否被计算在内），而且还可以引入实时民主，对任何问题都可以进行表决。这又提出了社会责任和参与度的重大问题，但是至少能够创建更具有去中心化形式的民主。



案例分析3

SETL交易

COO Connect 创始人, Dominic Hobson

清算、结算、托管和注册服务，对于发行、交易和持有证券都会增加显著的成本。有大量的专业代理和交易对手参与到投资者的证券和现金活动中。不仅这些服务有特定的收费，也有相关处理各种不同系统接口的业务集成和流程的辅助成本。总体而言，全球金融行业每年在交易后“post-trade”成本大约是650-800亿美元。

区块链技术提供了一个显著降低这些复杂性和交易后的服务成本，参与者来操作存在于大量作为节点来运行的服务器上存储的共享式账本。而执行交易的权利是由密码学设置的公私钥来决定的。

交易能够被添加到数据库中的块，每一个区块都会由节点进行审查。如果所有节点达成共识，认为该区块包含有效交易时就会被添加到数据库中。此外建立和维护这些节点，这个区块链网络应该是完全自治的，不允许任何一个控制或者监管实体存在。

SETL解决方案

一个名为SETL私人投资企业打算开发和部署一个专用的区块链，能够让金融市场参与者在一个点对点基础上来结算证券交易，并且维护一个分布式证券“金”账本和现金余额。特别是，SETL目标是让央行能够在区块链上发行货币。它的区块链运行在一个自治基础上，能够和现有金融市场、支付和交易所基础设施进行整合，

STEL将能够同时处理证券和现金端的每一笔交易，允许单边传输证券和现金，无论简单的支付，还是结算定制合同、公司行为、股息和优惠券。

SETL设计的目标是，将成本昂贵、具有风险的清算结算流程，变成一个对手方之间实时结算流程，此外，通过建立一个所有权的金账本，SETL能够大大降低证券登记托管的开销。

STEL区块链将有以下的特征：

- SETL区块链中公钥将需要由认证机构发布，能非常清楚的确认拥有每一把认证私钥的区块链使用者。认证机构将会保留每个公钥使用者在现实世界的详细信息，符合反洗钱和KYC规则的要求。STEL表示，如果有司法上的要求，认证机构将会透露这些信息。
- 将能够处理多种资产类别，包括现金和各种有价证券。
- 它将会使用多重签名交易，按照用户指定的用户群来完成授权。
- 将会使用“原子交易”（即所有的交易一旦发生，要么完成要么未完成），这样，只有所有阶段被提交和被认证过，那么交易才能够处理。
- 它将包含一个特别的功能，特别为参与者管理流动性而设计。
- 出于简化监管记录保管、交易报告和审计的目的，它将会保留交易的完整记录和余额历史。

更多的优势

现金余额和其他资产倾向于保管在特定的系统，仅仅处于特定的目的而部署：换句话说，他们是“系统特殊部分”。现金和资产放在一个区块链上，相反，能够由于任何目的来进行部署。这将会减少

量，这样银行不得不部署流动性储备，并简化其流动性管理。

SETL系统能够提供一个解决方案，将会同时和现有的英国央行实时总结算系统(RTGS, Real Time Gross Settlement)一起运行，在RTGS不可用的时候提供一个安全和可靠的选择。RTGS有些时间段是不工作，例如在晚上和周末的时候，SETL将

会是在任何时候都是可以工作的，减少的中间银行累积的风险。

SETL支付和结算系统是简单的，统一和直接的。如果英国是第一个部署类似系统的，它将让伦敦和英镑成为金融服务行业未来的首选位置和货币。伦敦可能是全球首个建立类似系统的城市，系统可能越来越被广泛采用，将会进一步巩固伦敦的地位，成为国际金融的全球领导者。

威胁

由分布式账本建立的创新是非常有吸引力的，但这不意味着没有更大的威胁，包括可能涉及货币属性，以及层级系统的角色和信任。

分布式账本可能会颠覆传统金融服务，传统金融服务其核心业务就是货币和价值转移。但是货币的形式首先就已经被类似于比特币这样的数字货币所打乱了，比特币是一种没有任何政府背书的数字货币；还有“彩色币”，这让货币可以有多种不同的属性。通过经济对货币的管理，被许多人视为是政府的主要职能，因此替代货币系统很可能被视为是对政府的一种威胁。

分布式账本系统对于任何层级结构都带来了挑战，因为它建立的是一个分布式网络，没有任何需要被信任或者必要的中介结构存在。层级系统有许多严重的缺陷：重复，增加成本，权利可能会被滥用，财政管理不善。但是，层级结构却是也有优点，一个中心的讨论机构也是必要的；例如，代议民主制度。

代议民主制度提供了一个相对稳定和持续的文官政府制度，但是将会被日益广泛的分布式账本技术所挑战。许多国家已经开始面临由于全球化和边境问题所带来的威胁，现在还将面对一些比特币的早期开发者和追随者提出一些极端反政府观点。尽管面临挑战，但是分布式账本和它相关的创新将有可能会促成一个可连接的、有生产力的社会，并为此提供可以支撑的基础建设。

结论

创意和技术的结合，会导致目前商业模式，以及与之相关的组织结构彻底改变。分布式账本目前也许会给现有架构带来尽可能多的挑战和问题，但更重



要的是，它也提供了一系列答案和可以实际操作的可能性。这看来至少是有质量的挑战，并且在适当的范围内，能够产生革命般的大范围变化。

分布式账本提供了挑战正统和过去最佳实践的假设，它带来的远远不止是记录交易和一堆账本。他们有可能会改变组织结构，并且是值得为之实践的操作——来进行技术或者非技术项目的演示——这些实践、相关法律和对政策的影响值得去探索。

对商业模式的激进创新，特别是结构和操作系统方面，可以在一个较为宽松和有效的监管下进行试验。在一个低成本的运营模式的环境中，能够来探索相关组织结构变化，政府应该考虑在何种监管制度能够更好的鼓励和利用这些全新的技术，并且让新的参加者可以自由的参与。

需要在整个系统的范围内，对财富成本和采用分布式账本技术的好处，开展更多的研究。这将会能让政府来能够确认，哪些摩擦成本的确是可以被避免的，并且哪些节省成本和其他重大机会可以被发现。



CHAPTER 6



Applications in Government

分布式账本技术已经对私营公司如何管理数据、如何与顾客和供应商进行互动这些方面产生了深远的影响。如果在政府内应用这种技术，它可以降低成本、提高透明度、提高公民普惠金融的程度，最终刺激创新和经济增长。这章会给出五个用户案例，它们将会描绘这些好处。



Author

Catherine Mulligan, Research Fellow, Imperial College London and Head of Digital Strategy and Economics, Future Cities Catapult. Additional contributions from Simon Taylor, VP for Blockchain R+D, Barclays; and Mike Halsall, Global Grand Challenges, Singularity University, NASA Research Park, California



第六章 政府中的应用

引言

分布式账本应用可以实现更多的用途，而不仅仅是管理像比特币这样的数字货币。分布式账本技术的概念及架构以及所使用的区块链技术是可以移植到其他领域的经济和社会活动中的。因此，在政府内部的运作中，这些技术有着深远的应用潜力——分布式账本技术对英国社会影响的显著性甚至有可能与英国当年《大宪章¹》的创建那样的大事相比较。

如果能够恰当地利用——而且能够重视和解决隐私、安全性、身份和信任等问题（参考第四章）——分布式账本技术能够给政府、其他地方性和区域性权力机构带来如下的机会：

- 降低运作成本，包括减少付款过程的欺诈与错误。
- 政府机构与公民之间的交易有更高的透明度。
- 对当前游走于金融系统边缘的人们能带来更高的普惠金融。
- 在降低保护公民数据的成本同时让不同的实体共享数据成为可能，并让信息交易市场的创建成为可能。
- 保护如大桥、隧道这样的重要基础设施。
- 降低市场摩擦，让中心企业更容易与地方和国家的权力机构互动。

这些好处是通过将分布式账本技术应用的三个方面实现的：

- 货币应用。
- 管理合约、创造新型的合约。
- 通过第三方推广新的应用，并提供更高效的方法用于构建和执行业务。

在这章内，我们会通过五个不同的学习案例去描绘这些机会、应用及不同的技术实施路线：

- 保护关键的基础设施，抵御网络攻击。
- 降低福利体系的运作耗费和跟踪受益人是否合格，促进普惠金融。
- 提高救助资金的透明性和可追踪性。
- 创造经济增长的机会，支持中小企业的发展，增加就业率。

- 减少税收欺诈。

案例 1：保护重要的基础设施

概览

分布式账本可让英国政府更好地保护关键的民用基础设施并抵御网络攻击。

背景

各国的关键基础设施越来越多地采用了数字技术，而很多这样的系统是连接到互联网上的。这带来了来自黑客或其他国家秘密地入侵已有的网络防护系统的风险。这样，攻击者就有可能取得某些关键的路由器的控制权，实现对其监控和控制。这会让路由器背后发生的公司和政府机构间的通讯被截取。还有，一些技术已经被嵌入到民用的基础设施中，包括桥梁、铁路、隧道、防洪大坝和能源装置（译者注：包括核电站、水电站等）——这样的话，攻击可能会带来财产和人命的损失。

分布式账本技术能够提供的

分布式账本技术可用于确保某个重要的基础设施的操作系统和固件没有被篡改。分布式账本可以监控软件的状态和完整性，发现不良的篡改，并确保使用了物联网（IoT）技术的系统所传输出来的数据没有经过篡改。

结果

- 在大型的基础设施内提高效率，更好地保护人命。
- 在关键的基础设施间来往的数据可以确保其完整性。

成熟程度

就绪

案例 2：英国就业和退休保障部

概览

新型的付款方式会让英国财政部、英国就业和退休保障部更高效地分发社会福利金，同时优化政策制定的过程。通过在政府的资金、福利的注册和分发过程中使用分布式账本技术，英国就业和退休保障部将可以更好地：



- 防止欺诈和失误带来的财政损失。
- 通过提供全面的普惠金融服务，给社会的弱势群体提供支持。
- 支持政府更大范围的政策目标的实现，特别是用可持续的方式扶贫。
- 提供最高的性价比，保证公共事业费用的可持续性。

背景

英国就业和退休保障部在福利保障项目上每年要付出约 1660 亿英镑的财政收入。其中的 35 亿英镑是多付出去的——福利诈骗（12 亿英镑）、申请错误（15 亿英镑）和官方错误（7 亿英镑²），这些多付的里面有 9.3 亿英镑被找回来了。若要把当前的税收抵免政策存在的诈骗行为和错误加上去的话，这会让英国就业和退休保障部在未来几年内都会成为新的“通用福利金体系”中的“最大负担”，这样算的话每年多付的钱甚至超过了 50 亿英镑。

除了给那些不符合资格的人多付的钱造成的直接财政损失外，纳税人还得承担付款后的干预工作（债务收集、调查、起诉、申请查询和纷争解决）。

还有，虽然目前还不能进行量化，但可以推断的是部分福利开支并不能达到政策的目标。例如，这些开支可能会付给那些钻政策空子的人，开支最终为非银行债务而服务，并付出了“贫困溢价”³。

分布式账本能够提供的

在那些领取福利金的人当中，有不少的人无法或者不方便使用银行服务⁴，若要让他们享受更高程度的普惠金融会面临着如下的困难——没有办法进行信用记录检查、无法使用传统的金融产品、在进行未经授权的交易时产生的高耗费。分布式账本技术为这些人进入福利系统提供了一个廉价的、辅助性的方法。

数字身份可以通过运行在安全编码设备上的分布式账本进行确认——甚至通过运行在移动设备上的软件确认——这会让终端用户直接接收到福利金，而且降低转账过程中发生在银行或当地权力机构上的耗费。这让他们通过一个比现有的银行账户更可靠的安全分发点接入到金融体系中。

这样的一个解决方案可以与其他系统连接在一起，随着越来越难地伪造身份，可以实现 在送达福利的过程中降低欺诈和人为错误的程度。

这些事情或许能帮助英国就业和退休保障部实现其主要的政策目标：让人们从贫困的循环中脱离出来，不再一味地依赖国家。通过这种技术的各种创新性应用，若与需要福利金的人达成协议的话——有可能在接收者和福利金转账最终到达的商家两端设定一系列的规则。这让部长们可以通过设定福利金使用的规则去优化福利金的分发过程，从而实现更好的政策效果。

结果

- 降低因欺诈和人为错误造成的损失
- 让部长们可以向纳税人展示公共资金被更高效地使用了，并用在指定的用途上了。

成熟程度

- 需要对福利金的接收者进行大量的教育。
- 需要将英镑整合到一个用于福利分发的分布式账本上。
- 可能会创造一个有“福利币”的经济子集。

案例 3：加强国际援助体系

概览

分布式账本技术可以让政府更好地控制对外援助的分发，确保资金到达设定的接收者。这也会帮助部长们提高透明度和带来高效的财政管理。分布式账本技术的使用可以帮助英国政府履行对国际社会作出的参与“Global Goals”行动的承诺。（译者注：Global Goals，直译是“全球目标”，是将近两百个国家为实现可持续发展而成立的一个全球行动。）

背景

为了履行国际责任，各国需要支持“全球目标”的行动纲领，引入透明性、可追责性和正直性的措施⁵。国际援助的捐赠者强调要帮助建造一个更透明、更健壮的援助体系。为阻止欺诈、盗窃和挪用援助资金的行为，可能需要很高的耗费。若技术上的进步能够帮助预防这些事情，对大范围的援助体系是有好处的。

欺诈和腐败降低了缓解贫困的机会，减少了内部投资，同时与低水平的教育普及率也有很大的关联。因此，将分布式账本技术用于国际援助体系以提高其资金使用的透明性和可追踪性是一个很大的机会。如果能证明资金被良好地使用，那么就可以鼓励各国投入更多的援助，也能让出资国家高效地实现预设的援助目标。

分布式账本能提供的

这个事情会使用到分布式账本技术的三个方面。第一，让国际援助者可以发行有货币价值的代币，而不需要经过传统银行业里的很多官僚主义障碍。分布式账本与地理限制无关的特性可以实现这个目标——在全球的任何国家里，它都是以同样的方式运作。因此，这能让国际援助节省货币处理的费用（要比标准的交易耗费低）。还有，它可以用于创造智能合约，这样的智能合约可实现“在陌生人之间创造自我执行的合约，为民众提供一个不依赖国内的



司法和行政部门的交易处理框架。⁶”

其次，国际上的捐赠者可以利用分布式账本技术的特点去降低现金的重要性，提供一种可靠的、不可逆转的数字资产转移方式——在这个例子里就是援助资金的发放。

还有，数字账本解决了双重支付的问题——数字货币或许能让终端用户重复支付同样单位的货币，数字账本解决了这个问题，因为每一个“币”都是独特的。这让脱离中介去处理支付成为可能⁶。在一些专门将资金定向捐助给终端使用者的案例中，可以通过点对点的资金转移，跳过货币和银行服务之间的某些局限。

第三，与货币链接在一起的代币，可以防止用在一些不合适、与国际援助目标不一致的场合上。例如，用于建造基础设施以降低贫困率的资金不应用在其他事情上。分布式账本技术有能力追查货币到底花在什么地方、由谁花的。

结果

在“全球目标”体系中提高专项资金的透明性，以降低腐败，更好地实现发展的目标。

成熟程度

- 捐赠者们各种不可预测的要求可能比欺诈和腐败更难处理，因此系统要高效地运作的话，必须要与捐赠者们达成一致，在系统设计时就考虑到这些问题。
- 在国际援助的每一个案例里，国际上的捐赠者都需要与受捐国的政府维护良好的关系。当腐败的问题与特定部门或者政府系统内部有关时，分布式账本系统必须得到受捐国政府有关方面的认同和协助，才能顺利推行。
- 若要将分布式账本技术在这类场景中应用的话，还需要根据这种应用场景的特点去创建很多辅助性的功能。

案例 4：降低市场摩擦和促进创新

概览

分布式账本最大的潜力之一，就是移除市场中的障碍和摩擦并让一种新型的信息交易市场⁷成为可能。就如第一章谈到过的那样，不同的经济实体通过分布式账本技术可以促进新型的创新成果。这会让政府部长们通过有效地利用技术的创新去辅助政策的制定，从而促进中小企业的成长。

背景

若能够降低中小企业与地方和国家层面的政府部门打交道时的交易成本，将会让这些企

业在市场中更灵活，并降低整体的运作成本。同时，让这些企业在分布式账本内登记知识产权，以取代传统的专利登记方式的话，有可能降低合同相关争议的数量。在英国，合同相关的争议占据了所有诉讼案件的 57%，这比任何其他类型的法律争议都要多。

分布式账本能提供的

分布式账本可用于很广泛的领域，特别是在智能合约和资产登记。通过在分布式账本上注册资产，所有的财产都可以等同于“智能资产”，可以为多种服务提供健壮的、可信的证据记录，与当前的方案相比，能为中小企业降低时间和经济成本。这些例子包含知识产权与专利登记、遗嘱、公证服务、英国国民健康保险制度数据和个人投资养老金/退休金。分布式账本提供了一个协调这些服务的新方法，是一个真正的由数字技术驱动的方法，适用范围广，并富有效率。

分布式账本技术可用于处理微支付、去中心化交易、代币赚取和花费以及转移，所能够达到的效果是今天的网络方案无法比拟的⁸。因此，分布式账本有潜力通过改革以下的方面去重塑地方辖区和商业部门的运作成本⁹：

- 商业牌照发放
- 注册
- 保险
- 在市政和监管的层面的税务管理
- 退休金数据

分布式账本技术有可能会取代上面的某些服务。商业部门将有可能为他们的公司和资产注册身份。更重要的是，公民也可以对自己的数据资产（如健康数据）有更高度的控制权，而这些数据以往是由政府保管的。这会让公民可以看到他们的数据被谁访问过，并用作什么用途。

还有，分布式账本技术可以让数据在新型的信息交易市场上进行共享——甚至是共享数据的实用性，——如共享退休金的数据。

结果

- 降低中小企业的交易成本，降低中小企业与地方和国家级政府打交道的成本。还有，若能够为知识产权这样的数字资产提供一个可靠的所有权证明，则会降低诉讼的几率，从而为英国社会的整体利益服务。

成熟程度

- 需要地方和国家级的权力机构去采用分布式账本技术



案例 5：欧洲的增值税

概览

经济从大体上可以分成三类，包括(i)遵守税收管理的经济，(ii)一定程度上遵守税收管理的经济，以及(iii)完全不遵守税收管理的经济（又称为黑市）。增值税在这三种经济类型里面都可能被偷逃，这其中原因有很多，包括企业倒闭、利用国际法的规则调整公司架构去绕过税收管理、只用现金去处理业务等。据估算，欧洲每年因此少收的增值税约在 1510 亿至 1930 亿欧元之间¹⁰。

分布式账本技术有指数增长的特性，有潜力让交易更加透明。英国可以在支持这个技术发展的过程中扮演一个关键的角色，提供分布式账本的协议和实施方案，以降低欧洲的增值税被偷逃的问题。

背景

在几十年前，摩尔定律就正确地预告了计算机运算能力呈指数式增长的特性。实际上，信息科技从十九世纪开始就已经呈指数式增长了，当前的预测表明摩尔定律在 21 世纪仍然有效。

信息科技是一种“自生的”技术，因为它可以通过科学发现去协助解决更多未知领域的问题。这又让我们可以开发出更快、更有性价比的技术，从而解答出更多自然界的谜团，而这些谜团的解答又会带来技术能力上的进化。（译者注：例如，计算机科学提高了科学家们工作的效率，让他们在自然领域的量子力学上取得突破，而这些突破又带来了量子计算机领域的进展，这就是信息科技“自生”的一个例子。）

分布式账本能提供的

创建一个欧洲全境的增值税标准和协议可以让分布式账本技术在欧洲全境部署，从收据到银行存单，将所有的增值税会计交易统一起来。这个系统会包括强化税收监管的智能合约，也会考虑到欧洲的各成员国不同的增值税起征额的问题。

通过“机器学习”设备，这个系统可以实时读取欧洲全境的增值税交易，那些错误的交易（包括所谓的“旋转木马欺诈”——译者注：即虚构一个在欧洲内各国流转的交易以实现增值税欺诈）在这种情况下会比传统的会计方法更容易检测出来。还能提高可追踪性和透明性——包括支付处理商、银行和其他金融机构——这会让那些黑市经济更难隐藏起来。

结果

- 降低行政部门为对公司和其他机构征收增值税的行政成本
- 实时地提高经济体里进行交易的透明性
- 创造了精确评估信用风险的机会，降低破产所带来的损失

- 为给中小企业贷款的机构提供数据，包括保理业务。
- 在国债和商业之间创建智能合约

成熟程度

- 技术上已经准备就绪。
- 应该在早期将支付机构引入这个体系里面，这是提高支付结算的透明度所必须的。
- 政府机构应该要有用分布式账本技术处理税务的能力。
- 终端用户和小企业主需要了解如何用分布式账本技术去高效地处理税务问题。

结论

分布式账本技术对政府来说无疑是有价值的，它可以通过新型的运作方式去降低欺诈、失误及给社会边缘人群提供服务的成本。同时，这些技术通过新型的创新为英国的中小企业提供了降低交易费用的机会。这章只谈到了一些可能的用户案例。随着分布式账本技术的广泛使用，政府运作的新模式可能会随之诞生。



Global 全球视野 Perspectives

任何一个在数字空间中的组织如果开展活动，就需要能够和他们的合作伙伴建立信任，以及被信任的关系。他们还需要能够和全球其它庞大和快速增长的社区进行协作，而区块链技术在这两方面都有巨大的潜力。



Author

Patrick Curry, Director of the British Business Federation Authority; Christopher Sier, Director, FiNexus; and Mike Halsall, Global Grand Challenges, Singularity University, NASA Research Park, California

第七章 全球视野

引言

全球正在发生快速的变化——包括好的和不好的变化都在快速发生，通过互联网驱动的全球化，社会的期望，以及对于资源竞争的加剧。不同于发展中国家，发达国家和它的公民所具有的消费主义倾向和隐私保护，与传统社会价值观以及个人行为准则发生冲突。这已经不仅仅是国家和社区中，负责帮助那些处于困境和艰难时刻的人们。各国政府都在努力满足那些不断增长的消费预期，和看似深不见底的社会救助需求。美国总统肯尼迪曾经发出呼吁“不要问我你的国家能够为你做什么，要问你能为你的国家做什么”——这句话在今天会变得越来越重要：许多公民非常希望能够帮助自己的国家，但在这个数字时代，他们目前还是缺乏参与进去手段。他们希望成为其中的一部分，而不是一个无助的旁观者。

由于缺乏整个社会参与的手段，就会导致一个结果，即出现两极分化的态度，把不同的期望和看法合并在一起，就会出现把复杂问题简单化的粗暴倾向，从而导致出一系列完全割裂的话题。然而，全球的现实是复杂和混乱的，现实世界、虚拟世界、法律、历史、地理、社会、行为、经济、信息和技术因素交织在一起。而变化还在时刻进行中，不断有新的颠覆性的技术出现，更增加了情况的复杂度。

规模、速度、复杂性都必须综合考虑，这就让那些行业领导者，各国政府，如果希望能够理解这种混乱的局面，如果还是在规划、使用传统的、非协作的组织架构，就变得尤其困难。这特别体现在那些更加灵活的领域，例如在面对金融市场和有组织犯罪的情形下尤其如此。而越来越多的发展中国家，就像肯尼亚和卢旺达，他们没有许多包袱，正在借助新技术实现跨越式发展。

而在发达国家，一些更小的，更同源的国家正在获得巨大的优势，他们通过提供跨国的国际服务来获利，特别是在欧洲（请参见之后的欧洲能源市场和爱沙尼亚案例）。

这些数字国家的特点包括如下：

- 有数字信息获取能力的领导部门。
- 一个强大，能够集中力量对全国政府部门进行数字改造的政府，需要具有国际视野，并



且能够和所有行业紧密协作。

- 一个实时、能协作的国家规划，通过国家投资并且由行业主导。
- 每个政府机构需要有对技术了解、合格且经验丰富的政府官员。
- 有工程师和 IT 企业领导经验的政治家。

如果英国希望成为最为先进的数字国家之一，那么在这些领域中，英国还有许多工作要做。然而世界越来越依赖于数字经济。这就需要我们在现有的经济模型中使用更多的计算机技术；并且，我们必须重新评估我们对于数字经济的理解正在如何变化，而且它的组成部分和相关活动。这就有些类似从以现金为基础的审计方式转变为以资产为基础的审计方式，这就需要每个组织有更广阔的视野，能够理解供应链、服务和市场的复杂性，还需要有不同的方式来进行协作方式管理、决策制定、获取分享和责任分担机制。

要在网络空间开展实现数字业务，一个组织必须能够信任和值得被信任。这都需要让大型和发展的各类社区与其它组织能够进行协作。信任和协作将会是网络空间中最重要的因素，远远超过在物理世界中的需求。而区块链在这两方面都能够起到巨大作用，但更神奇的不是它的技术——而是我们如何在国家层面使用它。

信任和交互协作

信任是两个或者多个人、组织或国家之间的风险判断。

在网络空间，信任是基于两个基础因素：

- 证明给我看，你就是你（认证）
- 证明给我看，你有必要的权限来做你要求的（授权）

如果我没有获得满意的答复，我仍然可以选择让你继续，但是我来承担风险。然后，在这之间并没有非常牢靠的信任关系，除非别人也信任我。从这个意义上来说，值得信赖也就等同于信誉良好。

- 交互协作包括下面几个因素：
- 数据交互操作性。为了能够一起协作，我们需要了解对方，所以我们的数据必须是使用相同规则和语义基础。
- 政策交互操作性。我们的政策需要有一致性，或者是基于相同的政策基础，只有这样，

我才能相信你会以我期待的方式来对待我提供的信息（反之亦然）。

- 有效、协同实施，并且使用国际标准

信息保护有关的访问控制，需要认证、授权或者更多。认证需要所有人都参加的身份管理（通常包括所有人、组织、设备和软件），根据给出的，符合国际定义的保证等级（LoA，Level of Assurance，预期使用者对确证或查证所要求的保证程度），认证需要能够实现跨多个认证机构和组织，实现联合身份管理（Federated Identity Management，FIM，是一种可以在多个企业之间制定的方案。该方案让用户使用同样的标识数据来获得组织中所有企业网络的进入许可）。

在国际范围内，类似于FIM目前仅仅有“低级保证”，这是国际标准中的LoA 1。主要用于社交网络中，因此多司法管辖对于它而言，并不是一个主要的问题。Google，GakuNin（日本大学网络）、微软、Ping Identity（企业身份安全认证服务商）、日经新闻、东京急行电铁（Tokyu Corporation），mini、雅虎日本和软银都部署了FIM系统；还有更多其他组织，如德国电信，美国在线和Salesforce.com正在部署类似的成熟系统。

中级保证（LoA2）需要身份证明等级，在消费者和企业进行金融消费时。目前有一些LoA 2的联盟组织，主要集中在银行系统。

一些行业使用基于公约基础设施（PKI，Public Key Infrastructure）联盟的安全系统，这是一种称为X.509的加密标准。这能够提供高和极高的保证级别（LoA 3和LoA 4）来进行员工身份认证，特别是应用于航空、制药工业、国防、银行，以及越来越多的电子健康行业。美国和中国都部署了最大规模的国际标准PKI联盟，紧随其后的是韩国（因为法规对所有企业有强制要求），爱沙尼亚、荷兰和其他一些国家。在LoA 3，它可以将用户身份链接到其他可信任的功能，例如有法律支持的数字签名，链接身份的加密算法，建筑物的物理访问控制。PKI联盟是高保证级别供应链合作和大规模共享敏感信息的唯一选择，到今天为止已经是事实上的标准了。

但是区块链提供了另外一个选择，能够和PKI联盟结合，并且区块链联盟通过结合最新的技术，能够提供更强大的数字审计能力，保证性和商业流程中的可信度，从而也许会有更大的吸引力。

在英国，目前只有警察服务部门使用大规模的PKI联盟来符合国际标准，尽管只是一种基础形式。通过与政府部门的最佳实践，将会能够扩展，来支持许多英国政府服务，包括紧急服务；还有一些国际合作领域，诸如跨国贸易、边境管制和难民移民问题，能够与有着相同PKI联盟的国家进行协作。目前，在公共服务网络针对员工认证的PKI联盟战略还没有开始实施，但是，没有足



够高的对于员工身份安全保证身份管理，或者是跨政府组织之间的协作，基于国际标准，可以让行业合作伙伴或者国家合作伙伴建立联盟，就像美国、法国和荷兰之间。通过结合区块链，PKI联盟可以提供更强大的服务，能够扩展到身份数据的保密性，和支付的可追溯服务。

NHS（National Health Service，即英国国家医疗服务体系）使用了非常庞大的PKI，但是并不符合国际标准，因此还不能形成联盟。国防部拥有国际义务来和美国为中心的国防供应链建立PKI，同样根据北约网络防御行动计划

（NATO Cyber Defence Action Plan）也有类似的义务，但是没有公布具体的实施方案。行业还在考虑PKI联盟在其他一些潜在领域，比如食品造假网络。并且和韩国政府机构达成了谅解备忘录，让英国公司可以拥有能在韩国企业供应链中使用的PKI证书，例如在三星、起亚、现代和大宇（这是目前全球最大的集装箱船制造商）。联合国国际海事组织正在开发海上网络安全的国际准则，并且可以利用英国和韩国的PKI联盟。在其他领域还有更多的例子，受益于一个论坛，这些讨论能够集中在这些协作。

欧盟议会已经在2014年9月批准了电子识别（Electronic Identification）、身份验证（Authentication）和信托服务规范（Trust Services Regulation，eIDAS），并且每个国家有三年时间来遵守这些规范。在eIDAS之下，如果任何国家“通报”了对公民的电子身份证件计划，处于电子公共目的，e-IDs在司法上要求所有其他成员国必须接受。其中还有巨大的工作有待完成，但是eIDAS迫使政府和业界考虑，让他们整体规划使用FIM来获得社会和商业利益。

在英国，政府已经出台了一个可以联盟合作、基于标准的方式来实现身份确认：GOV.UK Verify。GOV.UK Verify已经内置到最近市场中最新开发的，由竞争服务商提供者提供的身份服务，并且能够让用户选择使用哪一个方案。把GOV.UK Verify和区块链增强，并且链接到区块链，以及连接到PKI联盟，将可以增加GOV.UK Verify的价值。区块链和高安全性的PKI联盟解决方案可以用于GOV.UK Verify的隐私友好输入。总之，以不同的方式，他们都会对英国数字经济、边境控制和打击网络犯罪带来巨大的好处。

在网络空间，每个实体和交易都绑定或者链接到一个组织。建立一个符合所需要LoA的组织，关于实时或者准实时的信息，这是最基础的数字要求。越来越多使用区块链将会大大提升这个规定，因为可以避免区块链上的任何记录会被篡改。一个新的国际标准正在被开发作为数字组织认证，这被称为“法律组织登记册Register of Legal Organisations（ROLO）”。一些国家，包括美国在内，都已经考虑来适应ROLO规范，以满足他们的需求。

研究案例1

欧洲能源零售市场

欧洲会员会联合研究中心, *Igor Nai Fovino 和 Jean-Pierre Nordvik*

欧盟能源联合框架战略 (European Commission Energy Union Framework Strategy) 规定了“能源联盟”的愿景。“以人民为核心, 人民能够有能源转化的所有权, 能够从新技术中受益从而节省支出, 参与市场的活动, 并且保护弱势消费者。”

然而, 尽管智能电网的发展也在稳步推进中, 但是能源零售市场还在等待现代化。该委员会的正在启动“新能源市场设计”将需要面对几个至关重要的问题:

- 如何在成本和消费等信息适当的传达给消费者, 这样他们能够在一个完全整合的大陆能源市场中确认新机会。
- 如何奖励积极参与者, 有利于合同交换和管理, 根据需求提供相应的动态价格。
- 如何确保市场中对于住宅性能源服务的交互操作, 扩大消费者的选择, 能够从自生产和自消费中获利, 形成局部的微生产。

在这种情况下, 分布式账本能够成为一个全新的驱动力, 用以帮助能源市场进行整合发展。欧盟的联合中心正在调查以下案例中的实际应用可能性,

1、微发电的能源市场。微型发电是消费者在住宅内或者在一个当地社区进行发电。这个“市场”概念意味着, 那些微发电产生的能源将可以在消费者和产消者(既是生产者也是消费者)之间进行交易。以往传统的方式, 这个市场已经被产消者和能源零售商预先定义的双边协议确定。直到现在为止, 发电的产消者还没有能够真正进入能源市场, 这依旧是机构能源供应

者特权垄断的领域。这就极大的限制了微发电对于终端用户的经济优势。分布式账本, 通过和智能电表系统结合, 以及下一代电池(能够本地存储电量), 已经有潜力向能源市场提供产销一体的生产潜力。智能电表可以被用于注册和在分布式账本记录微发电的数据(成为“能量货币”系统的代币)。

自发电能够用于房屋内的消耗, 也可以被存储在下一代电池中以供以后使用, 或者简单的返回到智能电池。另外, 感谢账本的分布式和通用性, 所产生的能量可以在任何地方被赎回, 例如可以在国外对电动汽车充电时; 或者卖给价格最好的买家, 类似于股票交易市场提供一个相似的机制。

2、能源合同台账。一个消费者打算改变能源供应商需要结束目前供应商之间的合约, 再和新的能源供应商建立新的合约, 并且重新访问由第三方提供的所有补充能源服务的合同条款。这些业务的复杂程度已经成为一个真正的障碍, 阻碍成为一个有竞争力的能源零售市场, 这会成为能源供应商和分销商需要承担的成本。这将会让消费者最终从一个供应商过度到另外一个供应商, 只需要在电脑和移动设备上点击几下鼠标就可以完成。同样, 能源供应商和能源服务提供商将能够节省资源, 无需提供更多的管理操作成本。

这些可扩展、安全且稳定的应用肯定还会有各种各样的问题。但是, 从它的优势来看, 肯定是值得团队展开进一步的调查。



今天，全球化和缺乏数字化企业登记就造成现在的情况，特别是在欧盟，有大量金融活动的组织并没有在某个国家注册，甚至没有在任何国家注册。英国行业和政府职责，包括执法机关和网络安全机构，迫切需要把ROLO UK作为数字信任锚。行业正在开发ROLO UK，随着更多的政府用户组织参与将会从中受益。

数字经济

数字经济正在寻求利用速度、范围和效率。联盟信任能够增强信息和降低风险。互操作能够提升效率和具有重用能力。在一个成熟的供应链当中，每次一个公司在一个新的项目或者领域竞争，重用能力让它变得更加灵活和具有竞争上的优势：类似于像空客、波音、BAE系统公司、洛克希德·马丁、Northrop Grumman和Raytheon²，像他们这样在航空领域和国防领域的企业就是持有这样的观点。

在2014年2月，欧盟委员会和其数字议程委员会副主席，Neelie Kroes表示“民主必须谈技术”。她认为，我们正在一个数据驱动的世界里，信任是最关键的，“没有安全就没有隐私”。她指出，对于欧洲单一数字市场（Europe's Single Digital Market）而言，强大的网络安全是非常重要的，而欧盟网络安全战略（EU Cyber Security Strategy）正在提供正确的基石。她总结说，如果没有这样的计划，民主将“无法管理技术”。

这些主题涉及欧盟、美国和东南亚国家协会（ASEAN），逐步覆盖银行、电子、制药、视频、航运、航空、网络空间和执法机构。通过联合国和类似于欧洲委员会这样的组织，发达国家会越来越自觉的推动帮助发展中国家，因为他们已经成为全球数字经济中的一部分。但是缺乏数字化管理的手段将会阻碍发展中国家，为网络犯罪和恐怖主义创造了良好的机会，从而最终将目标对中发达国家。联盟可以在这种情况下发挥重要的作用。而其中协作是关键。

去中心化账本和区块链的潜力

经济依赖于政府之间的协作，在金融市场中提供信任，确保所有的参与者都遵守规则。数字经济同样如此。区块链之所以和网络犯罪有关联就是因为，该行业缺乏战略管理来建立的各种规则，并且确保每个人都遵守这些规则。一旦这种管理（通过政策、程序和机制），并且能确保执行，则区块链的社会效益能够真正得到体现。

政府担心的是数字货币和相关交易所的不稳定性，以及可能存在的相关漏洞，这让政府对使用区块链抱着非常谨慎的态度。一般来说，他们更希望行业能够朝着更好的局面进行发展。

到目前为止发展的主要领域

- 不受控制的区块链被用于不受监管和犯罪活动，特别是参与者都是匿名，从而不用承担任何责任。
- 初创企业正在和一些主要的银行来开发可信任的数字货币和区块链技术，例如“可信任的比特币”。这能够让在线消费类的企业获得很大的好处。
- 私有链正在被一些不对外的商业社区所使用，能够利用数字信任机制，并且设立他们自己的规则。这些都是不能进行交互操作的，并且不能扩展以支持供应链。

最近政府和业界开始探索区块链的战略潜力。通过四个主要的推动者，将让实施加快：

- 通过一种类似于 PKI 的方式提供一个基础的加密信任机制。这意味着区块链将能够和彼此之间联合，还能够现有的 PKI 体系打通。区块链能够利用 PKI 进行规模化部署和管理，而 PKI 能够利用区块链的支付和账本功能。这样，协同效应将会开辟全新的机会，智能、协作管理将会加速发展。
- 许可区块链将会包含无限大小的数据字段。和交易相关的信息，包括合约、版权许可证，都可以包含在内，为信任提供一个强大的额外因素。这就让“智能合约”（即合约与交易结合在一起），变得更有效率和不可抵赖。
- 利用新的协议，就像全新的统一经济传输协议（UETP,Uniform Economic Transfer Protocol），能够把载体、消费者、产品、支付和银行连接起来，还包括智能合约。荷兰在这方面已经成为领导者，和银行产业以及包括警察一起参与。美国也开始介入，并且他们的对于整个供应链上的网络安全法规出台后，速度会变得很快。而其他国家，如韩国、日本预计也会很快介入。
- 智能手机事实上已经成为可以信任的用户设备。最新的智能手机已经包含一些全新的安全功能：可信平台模块，能够有安全数字证书和认证密钥，加密和签名；可信任的执行环境，确保在处理时和操作系统无关，从而不会受到恶意软件攻击；可信任的用户界面，能够阻止用户和设备之间收到攻击。通过使用近场通信，智能手机已经可以和某些国家的 e-ID 卡和电子护照进行互动，这样的话，用户能够安全的登录政府机构，如边境或者警察。消费者和员工首次有了可以使用安全可信任的设备，他们可用于对交易签名（使用区块链）和支付（使用“可信任比特币”）。三星、HTC 和 LG 已经销售出了数千万部含有安全功能的智能手机，并且在 2016 年早中期也会部署这样的软件。苹果和其他品牌的手机预计也会很快推出。



强大的合作和主动的监管，能确保这些功能不会被滥用或者无用。这四个主要的推动因素，将能够鼓励更多的处于金融目的而使用区块链和分布式账本，并且其他以数字、数据为中心的目标，横跨供应链的应用范围正在日益扩大。当这样的系统成熟之后，它的能力将会大大延伸，通过四个因素能够帮助解决许多棘手的社会问题和全球挑战。其中的例子有：

- **透明和诚实的政府。**相对于在一个稳定、有负责人的法律和监管结构，从而促使有更好的社区和社会行为的国家，公民在发展中国家的信任是比较脆弱的。如果人民生活在一个被战争和专制政权蹂躏的国家，人们很难去信任他们的政府或者免于受到腐败的困扰。而通过（使用区块链、FIM 及其他相关能力）问责制和保证机制，嵌入到业务流程，确保所有行为能够有效实施，确保执法机关、警察能够执行法律，社会结构能够得到维护。
- **逃税和洗钱。**当一个国家的财富分配曲线变得过陡时，资金和资产的所有者就去寻求通过跨国转移财富来躲避监管，从而降低了国内市场的金融流动性，并由此会让处于财富分布边缘的人减少更多的经济机会。最后，当资本匮乏就会造成经济危机，让更多的年轻人失业，因此会造成他们整整一代人对政府长期的不信任。这最终将会颠覆民主制度，为社会断层创造了条件，造成国家和人道主义危机。因此，问责制和保证制度都是需要谨慎解决的问题。
- **非法贸易和环境破坏。**大约 50% 的海洋物种在最近的 30 年里濒临灭绝。根据《濒危野生动植物种国际贸易公约》（Convention on International Trade in Endangered Species of Wild Fauna and Flora），尽管国际社会努力，但有证据表明我们正面临着第六次地球物种大灭绝。如果我们有机会能够挽救目前全球的情况，我们就必须执行更加强大的物种资产勘察追踪机制，同样，我们需要问责制和保证制度。
- **食品造假和供应链破坏。**英国比以往任何时候更加依赖食品进口，甚至比 1917 或者 1942 更容易遭到食品危机。食品供应链非常难以追踪——可以参考一下 2013 年发生的食品掺假时间（被称为“马肉丑闻”）——有太多可以造假的机会。国际和英国食品供应链，除了找寻最佳的供应链安全保证机制之外别无选择，用以落实问责制和最小环节可追踪。
- **供应链威胁。**随着网络犯罪和国际知识产权盗窃案的增加（全球涉及总额超过 7 万亿美元），供应链正在受到越来越多的监管，市场和社会的压力迫使提供基于协作风险管理的更有效的保证制度，包括问责制度和联合身份管理。随着其他先进国家和国际专家，英国可以对欧盟、世界银行、G20 和联合国安理会施加影响，通过区块链为客户提供问责制和保证。但是英国政府无法单独做到这一点。业界希望政府能够让国家变得更有活力，充分施展国家的能力和先发优势，通过与业界进行充分合作，能够确保英国成为全球的领导者。

案例2

爱沙尼亚区块链转向支付、交易和签名

塔林英国大使馆, *Alastair Brockbank*

对于爱沙尼亚而言, 使用区块链技术进行试验是一个合乎逻辑的步骤。通过提供一个分布式和不可改变信息的账本, 在存储和管理公钥方面它具有完美的特性。这是一种密钥的形式, 通过提供一个指定机构, 能够和私钥结合来有效地的加密信息, 并且用于验证数字签名。爱沙尼亚现在是全球最经常使用国家级PKI (Public Key Infrastructure, 公约基础设施) 的国家。

此外, 作为一个去中心化的解决方案, 一个区块链非常轻便, 并具有很强的扩展性。它能够每秒计算海量数据, 并且可以无缝跨境协作。对于一个人口只有130万的国家, 区块链从而提供一个国家解决方案, 这远比作为一个全球解决方案要容易得多。他们的计算能力也会让他们变得更快, 在某些情况下, 该技术具有的颠覆性力量会让目前的中介变得毫无价值。

下面有三个研究案例——分别是银行、初创企业和网络安全服务提供商——显示了区块链技术在许多范围内的变革力量。这三个案例是需要区块链对用户表现很友好。用户完全不需要知道他们正在使用“彩色币”技术进行交易, 也不需要知道他们的ID卡登录使用了哈希加密算法。从这个层面上来看, 区块链的动作是完全看不出来的, 比我们熟悉的解决方案会更

有效率; 一个移动支付app, 一个在线众筹和交易平台, 或者是一个登陆入口。

和英国一样, 对于监管的必要性和程度是爱沙尼亞当局最首要考虑的问题。他们理解犹豫不决和优柔寡断对于创新有很大的伤害。创新者的风险将会转移到全新和更少监管的司法管辖区域——特别是, 缺少收入将会造成未来商业机会的损失, 并且诱使出现犯罪行为——这是显而易见的。

一个超前的银行发行数字货币证券

在今年早些时候, LHV银行——爱沙尼亞最大独立银行——是全球首家尝试可编程货币的银行, 发行了价值约10万欧元的加密保护的存款凭证。这个实验是继LHV的一家新子公司, Cuber Technology, 他们专注于基于比特币的数字证券。Cuber的业务由两部分组成: CUBER证券和Cuber钱包。

CUBER (Cryptographic Universal Blockchain Entered Receivable, 加密-通用-区块链-可输入-可接受) 证券是一种基于比特币区块链的, 简单的银行存款记录凭证。他们已经在欧洲进行展示, 在很多场景下都能适用, 并让人很感兴趣——作为价值存储, 交易所中介, 可信任的中介服务, 甚至可以用于机机交流 (M2M) ,



在物联网上有很大的前景。LHV认为，CUBER证券对于未来金融创新而言，将会是不可获取的基石。

Cuber钱包是CUBER首个用于展示的用例。这是一个移动手机上的应用，能够实时和免费进行点对点交易，可以极低成本的在商户和消费者之间完成支付行为，而这之间是使用CUBER有价证券。

用户可以在自己的智能手机保存私钥，来确保安全性和移动性。为了防止服务器出现问题的状况，Cuber钱包实现了服务器的去中心化信任机制，让用户使用自己的比特币客户端。这个app使用了SPV

(简单支付验证，Simplified Payment Verification) ——一种轻客户端安全——意味着用户永远不需要完全复制整个区块链副本。因此他们只需要下载一小部分称为“区块头”的数据，将把交易会链接到区块链上的某处。这将让他们能看到某个网络节点已经接受该笔交易，区块会首先将交易添加到区块，然后网络会在确认该笔交易后接受它。

钱包将会把某些比特币作为一个数据载体，并且通过添加唯一的标识字符串来对它进行“染色”。这意味着当它们进入数据库和进入传统银行系统时，代表LHV银行的一部分资产。通过使用法币，钱包不仅可以用于个人传输，还可以用于零售支付——商户必须同意这种支付手段，就像他们必须同意信用卡一样。LHV目前正在一些现实场所测试，但是希望能够在更广泛的在线网站中使用，特别是在一些微支付领域。

能够使用法币无疑对于用户而言更加有吸引力。LHV断言这种技术就是银行所需

要的：用户和商户完全不需要看到或者知道，Cuber使用比特币区块链。

Cuber是完全开放源代码，应用程序界面对第三方也是在线开放的，邀请其它数字货币交易所和开发者来使用。无论是LHV还是它的开发合作伙伴，ChromaWay，都更加希望小型软件开发者和初创企业参与创新，而不是那些大型银行。

当LHV也很清楚他们面临的挑战：监管的不确定性风险有可能会扼杀Cuber的变革力量，只要通过几条严厉的限制就可以做到这一点。银行应该督促监管者接受和适应区块链技术，而不是应该害怕它。

在它面前，通过银行的支持可以让Cuber提供巨大的优势，因为从一个传统银行将资金传输到一个数字货币钱包（以及传回）将会大大简化。CUBER从技术上来看是非常安全的——这是银行交易最基础的需求——尽管是通过去中心化的方式保存记录。但现实中，作为一个银行依旧是需要面临监管的障碍，因为相对于创新者，他们会面临更多的司法限制。就像欧盟的KYC规定，当银行需要开设一个新账户是需要面对面才行，而像Cuber当需要使用在线支付服务，例如TransferWise和Holvi，仅仅需要快速在线注册就行。如果银行在市场上有效地参与竞争，监管者需要不再为银行施加额外的障碍，也不应该增加他们招募用户的难度。

诚然，LHV具有一个不同寻常的位置：一个“对创新很友好”的银行来参与扮演自己的角色，而目前继续发展面临监管不确定性的限制。如果没有采取积极行动，Cuber将不得不远离LHV执照和由此带来的银行优势，或者将从欧洲到另外一个司法

管辖权。开发一个在数字货币和传统银行之间，简单、安全且有法律合规性的桥梁，证明将会有对所有的参与者是一个挑战。但是，没有人比LHV更加接近这个目标。

提供初创企业投资后市场的流动性

初创企业投资的流动性是透视投资者和创业者经常都会抱怨的一问题。那些提供资金的支持者一般至少将会拿出1万欧元左右，通常必须等待5年或者更长的时间才能退出。

Funderbeam——一个针对投资者的知名商务智能平台——很可能已经找到了这个问题的解决方案：一个基于区块链技术的投资在市场，让初创企业可以买卖代表股份的彩色币方案。

投资者很快就可以使用Funderbeam的在线平台，来打造一个针对一个或者多个初创企业的“投资集团”。可以建立各种形式的投资组合，对这个投资集团大小完全没有任何限制。一个10万英镑的股份可能包括1各主要投资者和99个跟投者；一个主要投资者投资75000英镑，5个跟投者分别是5000英镑；或者任何其他组着。就类似于众筹，但是减少了投资者投资初创企业门槛。

而FunderBeam和众筹的主要区别是，所发行的“彩色币”代表着集团成员的股份，这些股份可以立即被买卖，在投资者之间进行交易。这让投资组合具有更好的流动性，并且能够让初创企业获得更快的资金。而比特币区块链则为市场提供支

持，从而实现对资产所有权进行更快，更有效和透明的跟踪。

每个投资集团都会有一个微基金（microfund）。一旦一个投资集团完成，初创企业就获得了资金，Funderbeam的售后市场使用彩色币，给予每个参与集团的成员一个数字凭证代表其股份，并且立即可以流通交易。投资者一旦他们决定收回他们的投资货币或者希望减少他们的损失，可以卖出他们全部股份，也可以仅仅卖出一部分。

基于区块链的解决方案提供的好处绝不仅仅是灵活性。FunderBeam的首席执行官，Kaidi Ruusalpp，指出分布式账本技术绕过了传统官僚机构的缓慢效率。“我们其实不需要一个企业注册处，一个中心化的机构，或者是其他授权的机构来确认交易的完成性。通过区块链技术，每个投资，每次的所有权变成都可以以一种安全、分布式的审计来完成。”

Skype的联合创始人，Jaan Talinn也是Funderbeam的一位投资者，称赞它为在线交易提供了额外的安全和验证层。由于是去中心化、不可更改的特性，区块链能够在资产市场上更多的透明度，但是却不会损害任何人的隐私。

FunderBeam提供了灵活的、快速的、安全和透明的服务，让分布式账本能够提供一种可选的方案，这是让小型或者中小型企业能够在21世纪中，让资金更加灵活的基础。

下一代的公钥基础



自从2013年以来，爱沙尼亚登记处——包括所有托管所有公民和企业相关的信息——已经使用了Guardtime来认证数据库中的所有数据。他们的无钥签名基础设施（KSI, Keyless Signature Infrastructure）能够和密码学的“哈希算法（见下文）”配合来使用分布式账本，将会能让爱沙尼亚政府来监管网络和数据存储中任何组件的状态记录。

这是一个不小的的任务。爱沙尼亚是全世界最经常使用PKI的国家。在他们的身份证、处方订购、投票、网上银行、审查孩子的学校记录，申请国家福利、提交报税申报、提交计划申请、应用服务于军队，大约在3000多项事务中会使用它。企业家使用ID卡来提交其年报，发布股东文档，申请牌照等等。政府官员可以使用ID卡来加密文件来进行安全通信，审查和批准许可、合同和应用程序、和并且信息给支付机关。部长甚至可以使用它们的ID来准备和进行内阁会议，让他们来审查议程、提交立场和反对意见和回顾纪要。

数字认证因此对于政府来说非常重要，企业和公众服务都是如此，从政策起草到立法，从资产宣布到登记资产和继承权。超过2亿数字签名已经被用于ID卡：并且每年都在以39%的速度在增长。目前当务之急是，政府需要知道它的记录是正确的

记录，并且这些记录并没有被内部篡改，或者被网络攻击。

那么区块链能如何帮忙呢？它能够提供帮助，因为每次微小的变动都会被记录。通过提供时间戳、特征和真实性证明。KSI签名提供了数据完整性、回溯保护和可验证的方式来确保数据是没有被篡改的。它是以完全透明的方式来工作，确保用户的利益：公民可以知道是谁在审查他的数据，为什么以及何时；任何改动他们数据的行为必须获得授权。此外，通过使用哈希算法，而不是类似于大多数PKI，KSI这样的对称加密算法，不会被量子计算来攻破。

它具有可扩展性，它可以每秒签名一个额外字节数字，而使用可以忽略不计的计算能力和网络开销。它不再需要依赖一个可信任的权威机构，它签名数据能够跨地域进行验证，并且可以彻底保护隐私，因为它不会自己窃取用户的数据。很明显，该系统标志着PKI领域的一大进步。

最终，KSI区块链意味着当爱沙尼亚ID卡永远不可能出现信息泄露（虽然到现在也没有出现这样的情况），政府可以确信任何人试图篡改公共数据都会100%被检测到。



万向区块链实验室介绍

万向区块链实验室是由中国万向控股有限公司出资成立的专注于区块链技术的非盈利性研究机构。创始人为中国万向控股有限公司副董事长兼执行董事肖风博士、以太坊创始人 Vitalik、Bitshares 创始人沈波。实验室聚集了区块链领域内的专家就技术研发、商业应用、产业战略等方面进行研究探讨，为创业者提供指引，为行业发展和政策制定提供参考，促进区块链技术服务于社会经济的进步发展。万向区块链实验室的运作费用由中国万向控股提供。

万向区块链实验室将致力于打造六大服务功能：

- 1) 连接全球业界：汇聚国内和国外区块链技术领域内顶尖的技术专家、研究人员和行业人士，成为产业界和学界的网络和资源连接器。
- 2) 底层技术研发：促进区块链底层技术引入国内以及在国内的进一步研发。
- 3) 行业前沿研究：资助和推进区块链技术、商业应用、产业战略、监管政策等方面的前沿探索和研究。
- 4) 行业社群/社区：凝聚中国区块链生态链的各种力量，打造行业分享和交流的互动平台，形成行业共享发展的自组织。
- 5) 理念推广：通过公开发布研究成果，举办研讨活动、技术展示活动，增进学界、产业界、监管机构和公众对区块链技术的普及理解，提高接受度。
- 6) 商业孵化：孵化和资助基于区块链技术的商业开发和创业项目，推广商业应用和普及。

目前，万向区块链实验室聚集了大批全球区块链技术专家及学者，全球最重要的公共区块链之一，以太坊创始人 Vitalik 担任万向区块链实验室首席科学家。同时，实验室与区块链研究或开发的开源项目保持着良好的合作关系。实验室于 2015 年 10 月在上海举办了“区块链：新经济蓝图”2015 首届全球区块链峰会，该峰会在国内掀起了巨大的反响。同时，实验室也推出了万向区块链丛书，第一本《区块链：新经济蓝图》已经正式出版。为推进区块链技术的

发展，实验室推出了每年约 30 万美元的全球优秀区块链项目资助计划，以支持加密算法、共识机制、交易性能改进等区块链技术基础性研究，目前正在评选第二期赞助项目。

万向区块链实验室还推出了旨在培养国内区块链技术与管理人才的区块链培训课程，第一阶段的基础知识培训已成功在上海与北京推出；针对开发者的专业区块链技术开发培训也将会在近期推出。为了进一步推进国内区块链项目的落地，2016 年 1 月，万向区块链实验室与德勤在上海共同举办了总奖金高达 10 万美元的上海区块链黑客马拉松活动。在本次活动中，共计涌现出了 23 个区块链应用项目，最终 9 个项目获奖。此外，实验室将会于近期正式推出区块链云平台及区块链项目孵化器，进一步推进国内区块链项目的发展及落地。

万向区块链实验室将持续同社会各界合作，推出更多的区块链项目，努力推动区块链技术在中国的发展与应用。

万向区块链实验室联系方式：

电话：021-38529986

网站：www.blockchainlabs.org

邮箱：ydu@blockchainlabs.org

地址：上海浦东新区陆家嘴西路 99 号万向大厦



铅笔 ChainB

ChainB.com是我们网站的域名，其中的B代表Blockchain（区块链）。中文名取英文名的谐音“铅笔”，喻示着我们将会用自己的力量来见证和书写分布式账本技术和区块链行业的发展历史。而我们的微信公众号是“区块链铅笔Blockchain”。



铅笔（ChainB）将会提供全球区块链行业最新最全面的资讯报道，对区块链技术和相关企业事件进行深度分析和研判，探讨去中心化账本技术和相关创业投资机会，以及数字货币与数字资产等相关信息，是了解该行业的权威新媒体。

我们相信区块链技术会像《经济学人》的封面文章《The Trust Machine》中所指出的，区块链技术将会成为未来全球人类信任的基石，在今后深刻的改变每个人的生活。因此，尽管现在很多人觉得“区块链”是一个非常极客的单词，也许关注的人群数量有限，从而导致我们的目标人群也很有限。但是我们相信在今后将会变得和互联网一样，成为许多行业的基础建设，除了金融之外，还会包括医疗、物联网、公证、游戏，甚至是人工智能。因此，我们相信我们的目标客户将会覆盖互联网上大多数人的人。

我们将会为想了解区块链和分布式账本技术的各类人群，提供各个方面和程度的培训课程。无论是技术人员或者是金融机构的人员，都能够获得度身定制的各类相关知识的培训和学习探讨机会，并且了解全球各行业对于区块链技术应用的进展，相关投融资项目的案例分析，全球主要央行和监管机构对于该技术的监管和支持策略。

并且铅笔将会介绍全球各类区块链行业创业项目，创业者和投资者能够知道该行业最近的投融资事件以及最新进展。平台致力于连接创业者和投资人，为优质的创业公司提供股权投资、品牌宣传、社会资源协调等服务，同时为广大投资人提供参与创投、挖掘本行业独角兽的机会。

ChainB的创始人龚鸣，在区块链圈内以网名“暴走恭亲王”而被人所熟知。数学专业毕业，擅长各类IT技术和金融证券分析，有着多年IT和金融的从业背景，在德隆期间长期进行金融服务行业研究。2012年投身于数字货币和区块链行业，致力于推广数字货币和区块链行业的发展，翻译和撰写过大量相关资料和区块链项目白皮书，参与著有《数字货币》《区块链——新经济蓝图》等多部著作，在每年全球数字货币峰会上做过多次专题演讲，参与投资多个区块链和数字资产项目，在区块链行业内具有较大的影响力。

关注微信公众号“区块链铅笔 Blockchain”，回复不同关键词可以查看不同的报告，不断会有新的报告和白皮书加入到列表。

中文报告和白皮书

回复 **广发**，查看广发报告《科技前沿系列报告之一：区块链：正快速走进公众和政策视野》

回复 **兴业**，查看兴业证券报告《周小川谈数字货币：势在必行，路径待定》

回复 **川财 1**，查看川财证券报告《川财证券：区块链技术调研报告之一：具有颠覆所有行业的可能性》

回复 **川财 2**，查看川财证券报告《川财证券：区块链技术调研报告之二：区块链技术进化论-区块链技术的国内实践和展望》

回复 **埃森哲**，查看埃森哲报告《区块链与区块链交易所》

回复 **拜占庭**，查看《拜占庭将军问题详解》

回复 **区块链**，查看《什么是区块链》

回复 **中本聪**，查看中本聪论文《比特币：一种点对点的电子现金系统》

回复 **问答**，查看《区块链和数字货币常见问答》

回复 **论文**，查看《数字货币 2015 年十大论文》

回复 **DAI 中文**，查看 DAI Bond 中文白皮书《去中心化自治“贷券”信贷系统》

回复 **Factom 中文**，查看 Factom 中文白皮书《区块链上建立不可更改的审计公证业务流程》

回复 **以太坊中文**，查看以太坊中文白皮书《下一代智能合约和去中心化应用平台》

回复 **帮助**，查看本公众号全部关键词列表



英语报告和白皮书

回复 [德勤](#)，查看德勤公司报告《区块链技术全面报告》

回复 [Juno](#)，查看摩根大通 Juno 项目技术白皮书《Juno 技术白皮书》

回复 [监管草案](#)，查看欧洲议会报告《虚拟货币监管草案》

回复 [欧洲央行](#)，查看欧洲央行报告《欧元体系的愿景——欧洲金融市场基础设施的未来》

回复 [英国政府](#)，查看英国政府报告《分布式账本技术：超越区块链》

回复 [兰德公司](#)，查看欧洲央行报告《虚拟货币对国家安全的影响》

回复 [dh 报告](#)，查看 D+H 报告《区块链必须做到的五件正确事情》

回复 [普林斯顿](#)，查看普林斯顿大学首本比特币教科书初稿《比特币和数字货币技术 (Bitcoin and Cryptocurrency Technologies)》

回复 [联合国报告](#)，查看联合国报告《数字货币和区块链技术在构建社会和可信金融之间扮演的角色》

回复 [用户特性](#)，查看论文《比特币用户的特性 (Characteristics of Bitcoin Users)》

回复 [普林斯顿](#)，查看普林斯顿大学首本比特币教科书初稿《比特币和数字货币技术》

回复 [IMF](#)，查看国际货币基金组织报告《Virtual Currencies and Beyond: Initial Considerations》

回复 [DTCC](#)，查看美国存管信托清算公司报告《DTCC: 拥抱分布式》

回复 [桑坦德](#)，查看桑坦德银行报告《The Fintech 2.0 Paper: rebooting financial services》

回复 [Blockstack](#)，查看 Blockstack 白皮书《基于区块链全球域名系统的设计和开发》

回复 [论文 1](#)，查看论文《比特币闪电网络：可扩展的离线即时支付》

回复 [论文 1](#)，查看论文《比特币闪电网络：可扩展的离线即时支付》

回复 [论文 2](#)，查看论文《比特币骨干协议》

回复 [论文 3](#)，查看论文《数字货币是否应该进入 Barbados 央行国际储备货币组合中》

回复 [论文 4](#)，查看论文《国际清算银行：数字货币》

回复 [论文 5](#)，查看论文《Bitcoin-NG:可扩展的区块链协议》

回复 [论文 6](#)，查看论文《比特币在伊斯兰银行和金融业》

回复 [论文 7](#)，查看论文《政府在定价中扮演的角色及比特币市场中的跨国证明》

回复 [论文 8](#)，查看论文《机密交易》

回复 [论文 9](#)，查看论文《比特币点对点网络的日蚀攻击》

回复 [论文 10](#)，查看论文《比特币和数字货币的研究视角和挑战》

回复 [论文 11](#)，查看论文《可扩展的去中心化区块链》

回复 [DAI](#)，查看 DAI Bond 白皮书《去中心化自治“债券”信贷系统》

回复 [Factom](#)，查看 Factom 白皮书《区块链上建立不可更改的审计公证业务流程》

回复 [以太坊](#)，查看以太坊白皮书《下一代智能合约和去中心化应用平台》

回复 [BTC](#)，查看比特币白皮书《比特币：一种点对点电子现金系统》