# 区块链革新与智能合约的经济影响

丛林　何治国

区块链，一类具有去中心化特征的分布式账本技术，从作为比特币这一加密货币的支撑技术之后得到广泛普及。此后，它虽以各种形式出现，但通常具有存储数据和执行计算机程序的功能，该功能使得它在其他很多方面也得到了广泛应用，如智能合约、具有防篡改功能的支付技术，以及通过首次发行货币的融资等。业内很多人认为，区块链技术有望像互联网重塑线下商业那样颠覆

* 丛林（Lin William Cong），美国康奈尔大学 SC Johnson 商学院 Rudd Family 商业管理讲席教授，金融学副教授及金融科技计划主任，Kauffman 创业基金会青年学者，华尔街区块链联盟顾问，中国基金业协会特邀讲师，美欧经济金融协会和计量经济协会等多组织成员。研究领域包括金融经济学、信息经济学、金融科技、商业和经济学中大数据人工智能应用、创业学和中国经济。何治国，美国芝加哥大学布斯商学院 Fuji Bank and Heller 金融学讲席教授，清华大学经济管理学院阿里巴巴公益基金特聘教授，美国国民经济研究局教授研究员。主要研究领域为银行和公司金融、金融市场和危机、资产定价、契约理论、中国金融市场和金融科技。
本文翻译和改编自“Blockchain Disruption and Smart Contract”，原文起稿于2016年初并被*Review of Financial Studies*接受发表于2018年5月。作者在原文创作和本文编译中都深刻意识到区块链技术及其商业应用日新月异，所以文中提到的例子或者趋势估测可能与最终的实际发展不符。但是，其严谨分析中反映的经济力量以及机制应该是超越区块链具体实现方式和时间而通用长存的。作者感谢 Matthieu Bouvard、Alex Edmans、Andreas Park、Maureen O'Hara、Edward“Ned” Prescott、Hongda Zhong 以及匿名审稿人对本文极富洞见的讨论。感谢 Jingtao Zheng 出色的研究助理工作，该工作对于形成本文初稿有着非常重要的帮助。感谢 Susan Athey、Tom Ding、Itay Goldstein、Brett Green、Campbell Harvey、Gur Huberman、Wei Jiang、Andrew Karolyi、Jiasun Li、Minyu Peng、Chung-Hua Shen、Dominic Williams、David Yermack 等人（转下页）

现有的商业与金融服务。但很多人也对该技术真正的创新性与适用性保持怀疑，就更别提它经常与洗钱和贩毒交易相关了。① 图 1 左边的谷歌搜索指数显示出近些年来区块链技术的迅速普及，右图显示出与区块链和智能合约相关的开源项目在过去几年间经历的快速增长。

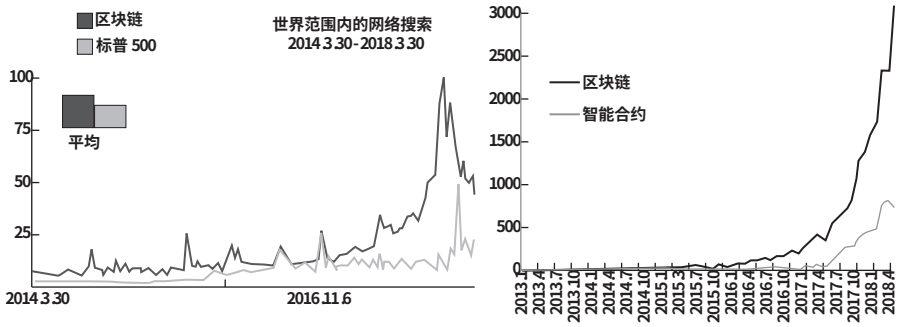


**图 1　区块链与智能合约的趋势**

注：左图显示了谷歌相对搜索指数，绘制了每个条目在时间序列上相对于其峰值（标准化为 100）的变化情况。右图显示了从 2013 年 1 月到 2018 年 4 月，Github（全球编码程序的一个主要开源开发平台）上关于区块链和智能合约的项目数量。

本文认为，尽管关于区块链和分布式账本有着非常多的定义、描述及其应用，但是该技术以及它的各类化身都有一个共同的核心功能，即提供“分布式共识”，也可以称作“去中心化共识”。分布式共识是对世界状态的一种描述，该状态被系统中的所有参与者一致性接受并据此采取行动，如货物是否交付、支付是否完成等。经济学家一直认为，共识就好像提供了“真理”一样，它让持有不同观点和动机的参与者得以互动，这对包括道德、合同签署以及法

在芝加哥大学布斯商学院、哈佛商学院、圣母大学门多萨商学院、香港中文大学经济学院、蚂蚁金服、美国经济学会年会、美国国民经济研究局证券市场竞争与产业组织研究中心、金融研究评论金融科技研讨会、纽约大学斯特恩商学院金融科技会议、美国联邦储备银行（费城）金融科技会议、南加州大学 FOM 会议、第 25 届 SFM 会议、中欧国际工商学院行为金融学与金融科技论坛、SFS Calvacade 亚太会议、AMAC 金融科技与智能投资研讨会、TAU 金融会议，以及美国国民经济研究局金融市场监管会议上提出的中肯建议和意见。原文受到中国国家自然科学基金（项目号 71503183）的部分资助。

① 《经济学人》（2015）的一篇文章声称“比特币背后的技术可以改变经济运行”，Netscape 的共同创始人 Marc Andreessen 甚至说：“就是它！分布式信任网络正是互联网一直需要但从未拥有过的技术！”（Fung，2014）然而，也存在批评区块链的声音，可参见 Narayanan and Clark（2017）、Jeffries（2018）以及 Stinchcombe（2017）。

律执行在内的诸类社会功能都具有重要意义。关键的是，这种共识是以去中心化的方式产生并维护的，由此区块链的倡导者认为，该技术可以提高系统的弹性、减少中心化第三方抽取的租金等。② 例如，在比特币的区块链上，参与者可以检查和验证历史交易记录，从而避免数字货币的“双重花费”问题，并且使每个人都不再需要一个值得信赖的中心化仲裁或第三方。③ 当然，我们所说的去中心化并不是非黑即白，而是相对于传统系统来说的相对去中心化。

在公有链、很多许可链与分散的记录者使用最新的技术进行互动，以达到分布式共识的过程中，产生了两种经济力量：一方面，得益于区块链的防篡改与自动化特征，程序化分布式共识的达成使得对或有事件的合同订立变得更加容易；另一方面，形成上述分布式共识需要大量的信息分发进行验证。一个很直接的结果是，区块链在应用过程中伴随着“分布式共识”与“信息分发”之间的根本冲突。前者增强了合同的可缔约性、改善了社会福利，而后者可能对社会有害。最近，一些媒体和行业研究也认识到了这一点。例如，2017 年加拿大银行在 Jasper 项目中指出：“更强大的数据验证需要更广泛的信息共享。而一旦系统的核心定义特征受到限制，信息透明与维护隐私之间的平衡就成为这类系统可行性的根本问题。”④

本文首次分析了区块链去中心化过程引发的这一核心冲突。正如我们在文献综述中更详细地讨论的，区块链与经济相关的研究领域有两个：（1）生成和维护分布式共识的区块链机制；（2）区块链技术运用对真实世界的影响。通过强调区块链技术中普遍存在的权衡问题（而不是分析比特币协议中特定的策略性挖矿博弈）以及研究该技术对产业组织的影响，本文在这两个前沿领域上都有所贡献。

首先，我们提供了一个简单的框架来思考在贸易金融中区块链是如何帮助达成分布式共识的。与现实世界中的第三方仲裁者相似，区块链的记录者会收

---

② 正如比特币创始人中本聪所言，“由于 20 世纪 90 年代以来，与电子货币有关的公司纷纷倒闭，这让很多人很自然地认为电子货币是一项失败的事业。而我认为，正是这些系统的集中控制性摧毁了它们。比特币是我们第一次尝试一个不基于信任的去中心化系统。”

③ 简称“双花问题”（double spending），是数字货币系统的潜在缺陷，它是指在对历史交易记录缺乏共识的情况下，一个相同的电子货币可以被多次使用。该问题的产生可能是由于电子记录被复制或者伪造。

④ 参见 Gillis and Trusca（2017）以及 Chapman et al.（2017）。de Vilaca Burgos et al.（2017）同样强调了这一点。

到有关真实世界状态的信号，但他们也存在误报（篡改或操纵）信号的动机。在快速发展的实时通信技术的帮助下，一份精心设计的区块链协议可以有效地降低个人操纵和误报信息的可能，从而使信息的聚集更加有效。与传统合同相比，区块链技术可以帮助产生分布式共识，从而更好地反映真实世界的或有状态，并使或有合同的订立变得更加容易。但是，有效共识的形成取决于分散的记录者观察和接收到更多的信息。⑤ 尤为重要的是这一信息分发过程会改变信息环境，从而改变区块链参与者的经济行为。

其次，我们分析了区块链技术对市场竞争和产业组织的影响。具体而言，我们的模型中有两个诚实型在位者卖方，以及一个可能为诚实型进入者卖方。诚实型卖方总是会交付货物，而欺诈型卖方则不会。在每个时期，买方以固定的概率集体出现（显示了集中化的市场行情），根据卖方报价决定是否购买商品，随后退出市场。每个卖方仅可以观察到自己的顾客，而不能观察到其他卖方提供的报价及其客户情况；我们将这一经济环境称为“传统世界”。根据格林和波特（Green and Porter，1984）的研究，在传统世界的经济环境中，行为人之间不能进行有效的信息沟通。

在传统世界中，一方面，由于合同的不完备性，卖方无法根据货物是否成功交付而进行市场定价，此时由于柠檬问题（也就是次品问题）的存在，市场进入不会发生。另一方面，在均衡的时候，两个在位者很可能会达成合谋。然而，由于在位者卖方无法区分是买方没有出现还是另一个卖方窃取了其市场份额，因此激进的价格战会经常发生，使得在位者卖方之间的合谋变得很难维持。

相比之下，通过分布式共识，区块链技术使得行为人能够根据服务结果签订合同并自动进行附条件的转账。在“区块链世界”中，诚实型进入者现在能够充分证明其诚实性，并进入市场。这消除了信息不对称，加强了竞争，改善了社会福利和消费者剩余。即使在假定卖方质量为私有信息的情况下，我们仍然发现，分布式共识可以缓解关于服务质量的信息不对称，从而提升消费者剩余和整体福利。

但是，如前所述，分布式共识形成的过程中，也不可避免地会使记录在区块链上的整体服务活动更容易被观察到，进而促使卖方之间形成隐性合谋。与

---

⑤ 部分信息可以被加密。在公有链（如区块链）中，共识一般由所有用户一起形成。

传统世界中的卖方无法观察到其他人的经济活动不同，在区块链世界中，卖方通过充当记录者，可以有效地推断出区块链上的整体服务活动，因此能够在任何合谋均衡中完美地发现违背合谋的行为。与该直觉一致的是，我们的确发现，相对于传统世界而言，在只有在位者可以参与的区块链上，卖方之间总是更有可能维持合谋均衡。

由此，本文的模型刻画了由区块链技术导致的潜在的竞争增加与合谋加剧之间此消彼长的关系。更为一般化地，我们发现，在引入区块链（在位者和进入者均可在链上）和智能合约之后，可能的动态均衡结果集合被扩大，与传统世界相比，区块链世界中均衡的社会福利和消费者剩余可能会更高或更低。

本文的发现与现在广泛存在的对区块链可能严重危害市场竞争的担忧如出一辙，尤其对于以强大的金融机构为专属会员的许可链而言，这一发现尤为重要（Kaminska，2015）。本文强调了区块链可能会造成合谋的重要机制，并探究了模型的政策含义。例如，一个经常被忽略的监管方案是：对区块链的使用者和共识生成者予以分离，这样卖方就不能通过使用与共识生成相关的信息来达成合谋。

通过从经济和金融角度对区块链和智能合约进行概念化描述，本文旨在证明区块链不仅仅是降低数据存储成本或共享成本的数据库技术，相反，它对于共识生成、产业组织、智能合约设计以及反垄断政策等也具有深远的经济含义。总之，本文证明了在区块链降低信息不对称、促进市场进入的同时，也同样会导致更多的合谋行为。

本文的研究对于区块链这一新兴领域的文献具有重要贡献，目前，该领域文献主要来自计算机科学家。在与经济相关的区块链研究中，主要包括两方面：（1）用于生成和维护分布式共识的区块链机制；（2）区块链技术对真实世界的影响。第一个领域又可以进一步分为两类：一类是分析区块链共识形成的一般过程，强调去中心化过程中的权衡取舍等；另一类则是分析博弈论中行为人的互动，其中包括区块链协议（例如比特币挖矿协议）中激励条款的设置与市场微观结构等。目前大多数研究都集中于后一类研究，而本文在补充第一类研究的同时，也丰富了区块链技术对实体经济影响的文献。作为最早描述各类区块链和智能合约在经济和商业环境中应用的论文，本文也对之后的学术研究提供相关的制度背景参考。

在关于区块链技术的应用与经济影响的研究中，哈维（Harvey，2016）对于加密金融的机制和运用进行了早期综述。⑥ 耶马克（Yermack，2017）评估了区块链技术对公司治理的潜在影响。与本文关于智能合约的讨论相互补充的文献有巴托莱蒂和蓬皮亚努（Bartoletti and Pompianu，2017）的研究，两位作者运用实证研究方法，验证了智能合约在各种区块链平台上是如何被解释和编程的。而本文通过仔细考察区块链的典型特征，分析它们如何与信息不对称相互作用，以及如何影响市场竞争这两大重要问题，对区块链在智能合约上的应用进行研究。

与本文关于分布式共识形成机制的分析相关的，是对比特币挖矿博弈的研究。克罗尔等人（Kroll et al.，2013）指出，比特币矿工遵循的“最长链条规则”，本质上是一个纳什均衡。比艾等人（Biais et al.，2019）一般化了挖矿博弈并分析了多重均衡的情况。⑦ 不同于研究特定的区块链协议（如比特币），或研究矿工之间的策略性行为或市场微观结构，本文以全局化的视角分析了区块链的一般化特征，并直接关注去中心化过程中的信息分发如何影响分布式共识的质量。与之相关的，阿巴迪和布伦纳梅尔（Abadi and Brunnermeier，2018）的研究表明，在许多区块链中，市场进入都会提高竞争程度，从而对用户产生正向效应。更重要的是，去中心化这一区块链的核心功能同时具有优势和劣势。在信息分发过程中形成的力量会使本应该去中心化的系统反而变得更加中心化。此外，在本文中，我们关注的是信息渠道，而丛林等人（Cong et al.，2018a）关注的是风险分担渠道和矿池的产业组织。陈龙、丛林和肖弋舟（Chen et al.，2019）对区块链和分布式系统的经济研究和未来发展做出了归纳总结。

本文对合谋的分析还补充了有关产业组织和有监督的重复博弈等方面的文

---

⑥ 其他关于区块链运用的文章包括：Malinova and Park（2018）对于交易的研究；Tinn（2018）对于时间戳与合同订立的研究；Cao et al.(2018）关于审计的研究；Chiu and Koeppl（2019）以及 Khapko and Zoican（2018）关于清算的研究；Cong et al.（2018b，c）关于加密代币的估值和平台发展的研究。

⑦ Eyal and Sirer（2014）以及 Nayak et al.(2016）研究了比特币区块链中含有挖矿者发起的扣块攻击的“自私挖矿”，以及相关的“顽固挖矿”。Easley et al.(2017）以及 Huberman et al.(2017）分析了比特币系统的交易费用，并探讨了在挖矿和交易中伴随的低效率和基础设施融资拥挤等问题。Cong et al.(2018a）分析了矿池如何加剧了挖矿军备竞赛和能源消耗，以及与之相关的产业组织问题。

献（可参见 Tirole，1988）。我们在模型构建部分借鉴了波特（Porter，1983）以及格林和波特（Green and Porter，1984）的研究，他们使用古诺模型研究了不完美公共监督下的合谋。最近波伏瓦等人（Bourveau et al.，2017）实证研究了合谋如何影响企业的金融信息披露（本文称之为信息分发）。本文使用伯特兰德模型，通过将技术创新背景下有监督的重复博弈与其他可观察到或可订立合同的信息联系起来，从而对合谋行为进行研究。⑧

## 1. 区块链的分布式共识

众所周知，区块链有很多功能，如分布式数据存储、数据匿名、数据混淆和共享账本等。由于除区块链之外，解决这些问题的方法众多，所以尽管区块链在这些方面有着很重要的影响，但这只是它的附加功能。本文致力于探讨区块链的核心功能，即提供分布式共识。因此，本文的模型并不适用于某些使用传统中心化方法形成共识的私有链或许可链。换言之，本文不分析各种协议的技术细节或技术带来的好处，而是强调分布式共识的经济含义，以及去中心化过程中伴随的信息分发。

在本节中，我们首先概述区块链这一技术，强调该技术的核心功能在于形成分布式共识，并分析该过程中可能引发的权衡问题。随后，我们对分布式共识的形成和信息分发过程建模，并探讨区块链技术在金融行业中的各类应用。

### 1.1 区块链与智能合约

关于区块链的研究可以追溯到 20 世纪 90 年代（Haber and Stornetta，1990）。然而，直到 2008 年，由于中本聪应用区块链技术提出比特币这一加密货币之后，才让这一概念变得非常流行（Satoshi Nakamoto，2008）。⑨ 区块链最简单的形式就是一个分布式数据库，该数据库以“区块”为单位，对不断

---

⑧ 本文关于稳定性均衡的分析与 Fudenberg and Maskin（1986）的研究相关；本文关于区块链和智能合约在金融服务和交易中的应用与最优合同理论相关，尤其是与信息不对称和不完全信息下的最优合同理论相关（可参见 Baron and Myerson，1982；Hart and Moore，1988；Tirole，1999）。

⑨ Böhme et al.(2015) 对比特币的设计原理、特征、风险和监管等方面进行了综述。Narayanan et al.(2016) 对比特币的技术细节进行了深入分析。正如“施蒂格勒的命名法则”中揭示的那样，关于比特币的内涵和法则早在很久之前就被人提出，中本聪只不过是将各种因素汇集在一起而已。具体内容可参见 Narayanan and Clark（2017）。

增长的公共交易记录进行自动维护，从而防止公共信息被篡改或修订。每个区块都包含一个时间戳，及其到前一个区块的链接。此后，市面上又逐渐出现了其他形式的区块链，它们在排他性、透明性和记录维护方面各有不同。

所有类型的区块链都不同程度地旨在创建一个数据库系统，在该系统中，各个参与方都可以用去中心化的方式维护和编辑数据，而没有任何个人可以对系统进行集中控制。因此，区块链架构的一个重要特征就是，它能够以一个统一的视角更加有效地维护世界发展的状态和事件发生的顺序，即共识。

共识对于许多经济功能和社会功能至关重要，它为共享和信任同一账本的每个人带来的好处显而易见。在有共识的情况下，问题的解决不再需要若干天，柠檬问题和欺诈问题可以被有效缓解，公共记录列表也会被不断更新，这些结果都非常有可能改变参与者的事前动机。在传统世界中，法院、政府、公证机构等为我们提供了这样的共识，但该共识的实现通常需要很多的劳动力投入，不仅成本较高，而且易于出现篡改、垄断等问题。从这点上考虑，尽管有些人提出区块链在电力消耗、信息分发（本文关注的重点）等方面存在劣势，但区块链的支持者仍然认为该技术通过实现分布式共识可以对现在的很多行业起到颠覆作用。

### 1.1.1 分布式共识

为了在不完全依赖某个中心化权威下生成并维持分布式共识，区块链协议在设计的时候，就需要对分散的区块链记录者做出的负责又准确的记录工作进行奖励，奖励机制的设计通常符合激励相容约束。从某种意义上说，尽管在不同的项目和应用中，区块链的算法各不相同，但所有的分布式共识本质上都是不同形式下的“多数表决”。

工作量证明（Proof-of-Work，PoF）和权益证明（Proof-of-Stake，PoS）是维护共识的两个重要设计。工作量证明用来奖励那些通过解决复杂密码难题从而验证交易并创建了新区块（即挖矿）的记录者。它防止诸如拒绝服务（Denial-of-service，DoS）之类的攻击，并确保一旦有一个人观察到账本的有效状态，在该区块之前的交易就不能被拒绝。通过这样的设计可以保证参与者对交易的有效性达成防篡改的可靠共识，因为一旦存在恶意实体想篡改交易记录，他就必须具备足以与整个现有网络竞争的算力。不同于工作量证明，在权益证明中，哪一个账户是下一个区块的创建者取决于账户拥有的原始加密货币

(即权益)。此外，其他比较有名的设计包括实用拜占庭容错算法（Practical Byzantine Fault Tolerance，PBFT）、股权授权证明（Delegated Proof-of-Stake，DPoS）等。⑩ 本文并不打算对具体的设计进行比较，而是打算将分布式共识算法进行抽象并加以建模，以期对现有的大多数算法设计都有所启示。

虽然许多算法的设计在当前看来都不够完美，但与过去相比，这些算法已经有了非常大的提升。例如，虽然区块链上发生过几起黑客攻击事件，比特币也因为浪费电力而受到批评，但各方已提出通过改进协议设计和进一步分权等建议来解决这些问题。⑪ 此外，从业人员也正在积极地研究另一个问题，即在修改区块链协议时缺乏有效共识，而该问题会导致用户在选择遵循哪些区块链时造成分叉和暂时混淆。

### 1.1.2 智能合约

智能合约的概念最早是由尼克·萨博（Nick Szabo）在1994年构想出来的(可参见 Tapscott and Tapscott，2016)。尽管智能合约尚未有一个被大家公认的定义，但关于它的核心功能却是明确的，即低成本传输，或基于分布式共识实现的自动化传输。上述事实使得智能合约天然就有一个功能性定义，即智能合约是数字化合同，它允许合同中的条款可以基于防篡改的分布式共识而自动执行。

本文对智能合约的定义与法律学者对它的定义（Lauslahti et al.，2016；Szabo，1997，1998）基本一致。值得一提的是，智能合约并不只是数字化合同(许多数字化合同依赖于中心化的权威机构实现共识，进而决定是否执行)，也不需要人工智能（相反，他们非常像机器人)。

如果没有分布式共识，那么提供共识的一方通常拥有巨大的市场势力(如拥有数据垄断权力的第三方)。而传统的第三方，如法院或仲裁机构，通常需要很多难以用算法处理的人工干预，这可能会更大程度地导致较高的不确定性和执行成本。相反，智能合约可以增加合同的可订立性，便于以自动化算

---

⑩ 股权授权证明（DPoS）与权益证明（PoS）的工作原理基本一致，除了在DPoS中，个体可以通过投票的方式选举一个首要用户，从而让该用户代为执行自己的股权。实用拜占庭容错算法（PBFT）在处理恶意节点的时候使用的是稳健的同步协议。

⑪ Lighting是在比特币区块链基础上构建的一个数字货币系统，它通过大幅降低在区块链上加载的信息从而增加了系统算力。初创公司BOINC也通过输送算力致力于解决科学问题来减少挖矿的资源浪费。

法和无冲突的方式交换金钱、财产、股份、服务或任何有价值的东西。⑫

区块链达成的分布式共识能大大减少不能合约化的或有事件的范围，而这也正是不完备合同理论中备受关注的一点（Hart，1995）。尤其是，智能合约可以提高附条件合同的可签约性与可实施性，适用范围可以是基金赎回的锁定期要求，也可以是进口商在收到货物之后的自动转账等。换句话说，合同可订立性的增强需要更多的信息分发，而该过程对总体社会的影响远非显而易见。

#### 1.1.3 信息分发

达成分布式共识需要将信息分发给系统中的部分参与者。无论是从实践还是从监管的角度看，信息分发伴随的经济权衡都非常值得关注。就比特币而言，生成并维护共识的方式是将所有交易信息（使用公钥加密的所有者地址）分发给区块链上的所有用户，因此共识中记录的所有交易细节（除身份信息之外）都是公开信息。在推动区块链在现实世界应用的过程中，一个很直接的问题就是如何保护商业隐私。例如，金融机构通常不愿意向其他无关方透露交易细节；交易者也希望隐藏自己的身份以防止被抢先交易等（Malinova and Park，2018）。此外，正如本文讨论的，更多的信息分发还可能影响产业组织和市场竞争等。

面对分布式共识与信息分发之间的权衡，很多人提议在分布式共识形成的过程中运用更先进的加密技术从而更加有效地隐藏敏感信息。例如，有学者（Cao et al.，2019，2020）提供了在审计领域的应用、经济影响和技术实施方案。另一个直接的折中方案是，只在部分重要状态的子集上达成分布式共识，或要求对区块链网络中较少的节点（记录者）进行状态验证。⑬ 除了隐私问题以外，信息分发还会带来哪些问题？这些问题会降低区块链共识的有效性吗？现有的研究在这些方面还知之甚少。

---

⑫ 尽管关于智能合约的一个更弱的定义要求中心化的一方执行合同，但是拥有共识仍然能够显著地降低合同在订立和执行过程中的摩擦，如最近佐治亚州通过使用智能合约进行土地注册等（Weiss and Corsi，2017）。

⑬ 如 Aune et al.(2017）讨论了如何使用第一阶段哈希运算来确保时间优先，此时交易者无须披露交易细节，也不用在之后披露交易信息。该做法可以防止其他人在交易被记录到分布式账本之前抢先交易。与该技术直接相关的是计算机科学中的“零知识证明合约”，该合约允许参与者在不披露任何细节信息的情况下就某些事实达成共识。

### 1.2 分布式共识与信息分发的模型

我们构建了一个简单的经济学模型来描述分布式共识的机制，强调记录者在其中发挥的作用以及在该过程中不可避免的信息分发。模型设定以区块链在贸易金融中的应用为背景，该场景被大家广为熟知。

#### 1.2.1 贸易金融的例子

想象如下场景：对很多国际出口商（卖方）而言，他们需要在运送商品时格外小心（如红酒，运送温度对于保持红酒的品质而言非常重要）。能否成功地将这些商品卖给进口商（买方）需要许多其他相关各方的参与，如物流提供商、国际港口、公证机构、金融中介等。

下面我们将分析在卖方将商品运送给买方的过程中，信息流是如何形成共识的。图2中我们使用 $\tilde{\omega}$ 代表商品运送过程中的一种或有状态。参与交易的各方，如卖方和买方，可以通过点对点的信息收集来监督商品的状态（如地点、运输温度等）。上述信息收集工作可通过传感器、智能输入设备、实时数据处理或更为一般化的物联网（Internet-of-Things，IoT）来完成。为了更好地进行监督，物联网的传感器还可以安装在任何与物流相关的其他参与方上。这样，买卖双方就可以全程收到关于商品运送的信息。

区块链上的其他各方可能也会接收到相关的信息，这些信息可以帮助买卖双方更好地监督商品的运送过程。如其他卖方也可以安装物联网传感器，从而更有效地监督商品的交付状态。即使没有安装物联网传感器，对于在同一港口收取其他商品的其他买方而言，他们也可以收集到有关该商品移交的信息。此时，这些信息还没有被记录在区块链上。值得指出的是，（通过物联网和提供离线信息的价值中介“Oracles”）信息上链是当前智能合约发展的主要挑战和瓶颈之一，许多技术细节有待解决。⑭

区块链上很重要的一步，就是要生成关于“该商品是否已被成功交付”的分布式共识，这就需要联系区块链上的验证者，通过汇总他们收集到的信息，让商品的状态被整个社区知道和承认，进而才能将这些信息记录在区块链上。在本文关于贸易金融的例子里，信息收集过程中需要联系买卖双方、物流提供方、港口等相关各方。此外，还需要联系其他装有物联网传感器的卖方，

⑭ 关于物联网的应用和经济研究，Cong et al.(2019）提供了简单综述。

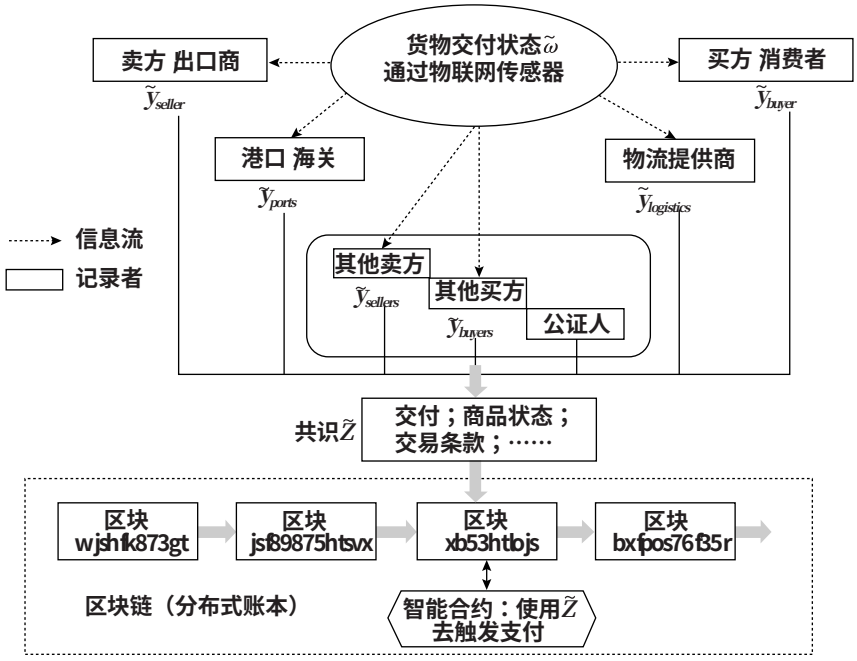


**图 2　区块链在国际金融中的应用流程图**

注：卖方将商品发送给买方，$\tilde{\omega}$ 代表货物是否被成功交付这一或有状态。通过使用实时的物联网技术，记录者可以监督商品的交付状态，并提交他们的信息报告 $\tilde{y}_k$。区块链协议将这些报告汇总在一起形成分布式共识 $\tilde{z}$。该共识与其他智能合约一起被储存在一个新的区块里，并最终被加入区块链中。

因为这些卖方在发生纠纷的时候可以较为专业地核验交付是否成功。在区块链的应用场景中，我们称这些被联系的参与人为“记录者”。被联系的各方可能不一定会真实地报告他们收集到的信息（本文的模型允许该情况的存在）。最后，其他买方也可以相互沟通信息，这是为了“一致性核查”的目的。

被联系的各方将他们各自收集到的信息 $\tilde{y}_k$ 提交到区块链上，随后区块链协议根据各方提供的信息 $\{\tilde{y}_k\}$ 生成分布式共识 $\tilde{z}$。这样，一个新生成的区块就被加入到之前的整个链条之中，正如图 2 的下半部分所示。而在更多区块被加进来之前，当前被新加入的区块需要通过一系列的检验，从而保证该区块的共识信息与之前区块链上的共识信息（可以理解为基于之前输入的信息而生成的共识）是一致的。⑮

⑮　正如在比特币的例子中一样，该处理方式涵盖了新加入的区块仍然需要进一步验证的情形，所以这里“新加入的”也可以理解为“敲定的”或“确定的”。

在这个例子中，其他卖方可以通过两种方式在区块链上接收信息，一种是通过他们自己装有的物联网传感器，还有一种是在被联系核查交易信息时接收到的额外信息。在我们看来，这两种方式有所不同，而第二种方式作为生成分布式共识的关键步骤，对区块链技术更为关键。暂且不谈信息分发导致的合谋，这些专业化的卖方接收的信息越多，形成高质量分布式共识的可能性也越大。需要提醒的是，信息分发存在一个下限：即便所有需要被验证的信息都被加密了，仅仅核查信息这一行为也可以透露一些信息（这一点至关重要，将会在我们的经济学模型中有所体现）。

### 1.2.2 模型设定

为了阐述去中心化如何在生成有效共识的同时导致更多的信息分发，我们现在将上述贸易金融的例子模型化。该模型分析对于公有链和使用分布式共识机制的许可链同样适用。我们的模型不是为了还原某一具体共识机制的细节，而是抽象刻画大多数机制的共同特征和经济学原理。

假设一份智能合约提及某一或有结果 $\tilde{\omega}$，该结果对应于商品或服务的交付状态。如果商品或服务成功交付，则随机变量 $\tilde{\omega}$ 取值为 1，否则为 0。我们用 $\tilde{z}$ 表示区块链上关于或有结果 $\tilde{\omega}$ 的分布式共识，$\tilde{z}$ 的取值范围同样为 $\{0,1\}$。

正如在贸易金融的例子中描述的那样，区块链的参与者在实时物联网技术的帮助下，可以接收到很多信息。[16] 尽管我们可以设定参与人接收到的信息是否为真实信息 $\tilde{\omega}$，但是给定我们在其后会引入参与人报告虚假信息这一动机，该设定带来的复杂性就显得不太必要。（实际上，附录 A 在更为一般化的模型设定下考虑了这一可能的情况，并且使用多种线性模型证明了结果的稳健性。）

在实践中，为了形成分布式共识，区块链关联了一系列记录者，这些记录者都是分散化的区块链参与者（体现了区块链的去中心化特征）。[17] 挖扩过程中保持对记录的共识是加密货币（如比特币、以太坊等）的重要特征。Ripple 和 R3 CEV 虽然使用它们自己的共识过程，但仍然依赖于众多的记录者。记录过程通常包括竞争、记录保存以及块后验证的分配等，它本身就是一个有趣的研究领域。

假设区块链协议关联了一组数量为 $K$ 的潜在记录者，他们属于集合 $\mathbb{K} \equiv$

---

⑯ 显然，该技术并不适用于验证主观感受。

⑰ Zurrer（2017）的表 1 中更细致地展示了更多有关记录者的例子。

$\{1,2,\cdots,K\}$，所有记录者都具备同质性。简便起见，我们将共识的有效性记为 $-\mathrm{Var}(\tilde{\omega}-\tilde{z})$。[18] 共识的有效性是许多金融科技公司广泛标榜的信任基石。

一旦被联系，每个记录者 $k\in\mathbb{K}$ 提交一份取值为 $\{0,1\}$ 的报告 $\tilde{y}_k$，由此产生一个报告的集合 $Y\equiv\{\tilde{y}_k\}_{k\in\mathbb{K}}$。正如我们在之后阐述的，记录者可能会谎报信息，即 $\tilde{y}_k\neq\tilde{\omega}$。更为一般化地，我们研究如下情形，在该情形下，共识函数为：

$$\tilde{z}(Y)=\begin{cases}1,\omega.p.\ \sum_k \omega_k\tilde{y}_k\\ 0,\text{其他}\end{cases}$$

记录者 $k$ 报告真实信息的概率为 $\omega_k$，$\omega_k$ 是非负数，且和为1。我们也假定当 $K\to\infty$ 时，$\omega_k\to 0$，以此来刻画去中心化这一关键概念。该共识函数表明，如果大部分记录者都报告了商品成功交付的信息，那最终形成的共识就更可能是商品交付成功。在模型中，我们关注去中心化的度量参数 $K$ 如何影响共识的质量以及整个系统的信息分发。[19]

### 1.2.3 记录者的信息与信息误报

假设区块链上每个记录者都观察到了 $\tilde{\omega}$ 的实现，即交付状态的实现。虽然关于比特币的支付验证通常涉及双重花费问题，并且要求有限的信息分发（如交易方的真实身份需要被隐藏），而对一般经济活动的信息验证通常更为复杂，并且需要更细致的信息。如许多贸易金融的区块链需要使用来自当地船舶、港口、银行和边境海关的信息以追踪商品的交付状态，这些信息的收集通常需要借用传感器或者物联网设备，而且交易细节也并非完全公开（例如，Corda 或者一些超级账本区块链）。[20] 此外，记录者还可能会收到一些关于交易

---

[18] 在现实中，共识的有效性取决于共识的目的以及共识在每个区块链中具体的使用情况。本文的设定从定性角度刻画了一个普遍特征，即参与者各方希望提高对真理反映的确定性。

[19] 对于更一般化的设定 $\tilde{z}(Y)=\tilde{z}(\sum_k\omega_k\tilde{y}_k)$，其中 $\tilde{z}$ 是在 $\{0,1\}$ 内取值的函数，我们的结果仍成立，而且满足 $E(\tilde{z})$ 是可微和递增的性质。此外，当参数取值为0或1时，函数也相应地取值为0或1。这意味着，如果记录者的报告全部都是准确的，那么共识就反映了真实世界。这些要求与当前的区块链协议基本一致。

[20] 对于更复杂的商业情形，记录者很可能只能观测到关于真实世界的含有噪音的信息。此外，其他关于区块链公共信息披露的规则也可能会影响记录者的信息质量，进而影响分布式共识的质量。我们在附录 A 中通过引入一般线性模型，从而对这些问题进行探讨。

的额外信息。例如，IBM 目前正在开发为记录者提供更多发运货状态信息的贸易金融区块链，其背后的原因就是为了生成关于货物是否已交付的共识记录，这就需要与链下的合作、与货运公司的交叉验证以及进出口控制等。

记录者还可能有谎报信息的动机，如在贸易金融的例子中，记录者可能是参与交易的相关方；在比特币的例子中，矿工很可能会为了“自私挖矿”或双重花费而隐藏自己的私有信息。[21] 此类动机在传统世界中也可能存在，如商业仲裁者可能会偏袒某个当事人，传统在线支付面临着双重花费问题（也正是这个问题激发了比特币最初的诞生）。事实上，媒体和从业人员的讨论主要集中在区块链如何帮助减少信息篡改、操纵以及黑客攻击等方面。

在本文的简化模型中，我们假定每个风险中性的记录者提交一 份$y_k$ 的报告，从而最大化其标准化效用函数 $U$（ $y_k$;$Y$），具体地，记录者面临的最大化问题如下：

$$\max_{y_k \in \{0,1\}} U(y_k;Y) = b_k \cdot \left| \tilde{z}(Y) - \tilde{\omega} \right| - h_k \mid y_k - \tilde{\omega} \mid \tag{1}$$

其中 $b_k$ 和 $h_k$ 是正数，对于所有的 $k$ 而言，这两个系数都一致地有上界并且以0 为下界。$b_k$ 描述了记录者 $k$ 从误报（当真实状态为 $\tilde{\omega}$ 时，报告的却是1 − $\tilde{\omega}$）中获得的收益。$h_k$ 表示了误报的成本，该参数取决于贸易金融中不同的协议设计，$h_k$ 可能是在一个区块链联盟中的名誉损失，也可能是在物联网传感器中伪造信号的成本。而在比特币的例子中，这一成本体现在不准确的记录需要更长时间才能得到确认，并且被逆转的可能性很高，就更不要提在工作量证明中篡改记录所需的巨大算力了。

#### 1.2.4 信息分发和共识质量

每个被联系的记录者选择报告 $y_k$ 从而最大化自己的效用，在均衡处，我们有：

$$\tilde{y}_k^* = \begin{cases} \tilde{\omega}, 若 b_k \omega_k < h_k \\ 1 - \tilde{\omega}, 其他情况 \end{cases} \tag{2}$$

由于在给定其他人的均衡策略的情况下，记录者 $k$ 误报信息从而改变共识的可能性为 $\omega_k$ ，所以误报的收益为 $b_k \omega_k$ 。而误报的成本为 $h_k$ 。此时，均衡的共识为：

---

[21] 在本文的模型中，虚假报告会产生信息噪音，而记录者被黑客攻击同样可能会产生噪音信息。

$$\breve{z} = \begin{cases} \tilde{\omega}, \omega.\, p. \sum_{k \in \mathbb{K}^*} \omega_k \\ 1 - \tilde{\omega}, \text{其他情况} \end{cases} \tag{3}$$

其中 $\mathbb{K}^* \equiv \{k \in \mathbb{K}: b_k \omega_k < h_k\}$ 是真实报告的记录者的集合。分布式共识的质量为：

$$-Var(\tilde{\omega} - \tilde{z}) = -Var(2\tilde{\omega} - 1)\left(1 - \sum_{k \in \mathbb{K}^*} \omega_k\right)^2, \text{其中} \mathbb{K}^* \equiv \{k \in \mathbb{K}: b_k \omega_k < h_k\} \tag{4}$$

由于 $Var(2\tilde{\omega} - 1)$ 与 $K$ 相互独立，因此，集合 $\mathbb{K}^*$ 越大，分布式共识的质量就越高。去中心化的好处体现为：被联系的记录者的数量（$K$）可以提高共识的质量。具体地，$K$ 通过弱化每个记录者操纵信息的动机，使得真实报告的记录者的集合 $\mathbb{K}^*$ 逐渐地趋近$\mathbb{K}$。如当 $b_k = b > 0$、$h_k = h > 0$ 以及$\omega_k = 1/K$ 时，共识的质量与 $-\mathbb{I}_{\{K \leqslant \frac{b}{h}\}}$ 成比例，即 $K$ 越大，共识的质量也越高。

对于更一般化的满足约束条件的 $b_k$ 和 $h_k$，共识具有完美性，即当 $K \to \infty$ 时，$\tilde{z} = \tilde{\omega}$。本文的第 2 节将重点关注该情形，讨论在完美情况下，分布式共识如何改善合同的可订立性并增加市场进入（进而加强市场竞争）。此外，我们还将在第 3 节中讨论不完美共识。

#### 1.2.5 与之相关的信息经济学文献

值得强调的是，本文的分析有别于将信息经济学应用于金融和贸易领域的现有文献。这其中最主要的区别在于：本文分析的区块链的核心功能，即记录者可以通过分发信息达成分布式共识，是“去中心化”的第一个阶段。这对应图 2 关于贸易金融的例子中，系统将交易双方、港口、其他卖方或买方的信息关联起来，共同创造了一个分布式共识的过程。随后，这一共识被进一步分发给区块链上的所有行为人，这涉及的是信息分发的第二阶段。

之前关于金融经济学的文献通常研究的是已有信息的分发，即信息分发的第二阶段。这之间最典型的就是关于信息披露及其透明度的研究，如美国关于公司债券市场信息披露的 TRACE 系统。[22] 虽然透明度会影响交易者的动机和市场运作的效率，但即使没有 TRACE 在事前和事后关于透明度的要求，交易行为和信息的聚集仍会发生。换句话说，在传统世界中，当更多的公共信息有

---

[22] 具体可参见 Goldstein et al.（2006）以及 Bessembinder and Maxwell（2008）。此外，Bloomfield and O'Hara（1999）同样发现做市商可以运用交易信息维持合谋。

害的时候，监管者或行为人可以选择分发更少的信息。

与此相反，本文强调了信息分发的第一个阶段：共识形成过程中的信息分发，该过程是分布式共识以及防篡改功能得以实现的重要环节。信息分发越多，共识的质量越高。这一点与查普曼等人（Chapman et al.，2017）的思想一致，他们也发现，为了减少信息分发而做出的限制去中心化的尝试，往往会降低系统操作的弹性，而操作弹性本应该是区块链技术相比于中心化平台的一个重要优势。

总体而言，共识的质量和信息分发的程度取决于具体的区块链协议，而叙述不同的共识机制或推导最优的区块链设计不在本文的讨论范围内。本文的主要工作是概述区块链在金融行业的应用，并强调去中心化过程中的信息分发问题。

### 1.3 区块链在金融行业的应用

区块链技术和智能合约在现实世界中得到了广泛应用，有时甚至超出了金融科技行业的范畴。本小节将主要讨论区块链在现实世界中的各类应用，这里的讨论不仅仅是区块链应用的概念证明。[23] 熟悉区块链应用的读者可以跳过本小节，直接阅读本文的第1.4小节。

#### 1.3.1 贸易和贸易金融

让我们回到本文第1.2节中关于国际贸易的例子，及与之相关的融资活动。根据WTO（世界贸易组织）近期的报告，国际贸易及其相关融资活动达到了每年10万亿美元以上。[24] 尽管技术进步推进了众多金融服务领域的发展，但贸易金融很大程度上还是以纸张为基础的人工过程，它涉及世界各地不同司法辖区的众多参与者，而且在供应链上出现的人为错误与延误也时有发生。[25] 一个进口商无法达成交易的原因可能是为其提供信用证的银行在出口商所在国家的知名度不高；而一个出口商无法提前获得融资的原因可能是银行担心货物

---

[23] Bartoletti and Pompianu（2017）使用1673271笔交易分析了834份来自比特币和以太坊的智能合约。他们分析了智能合约的五个主要使用场景（金融、公证、游戏、钱包和图书馆），其中三个与货币转移和交易有关，其余两个与记录共识信息有关。超过2/3的用户使用智能合约进行资金的管理、收集或分配。

[24] 如参见《2017年世界贸易统计报告》，https：//www.wto.org/english/res_e/statis_e/wts2017_e/wts17_toc_e.htm。

[25] 小的供应商要等60—90天才能收到货款。缓慢的支付过程阻碍了它们获得流动性资金。

不能及时且成功地交付，担心进口商不能如期支付货款等。

区块链技术可以帮助缓解上述贸易摩擦。具体地，该技术可以提供两类解决方案。一类是货物流动，通过使用现代通信技术，如物联网、提供离线信息的“价值中介”（Oracles）等，区块链可以更好地跟踪货物的运输、储存和交付过程（例如，货物的物理位置与移动、货物保存的温度是否适当等）。另一类是与贸易有关的资金流动（例如，信用证和贸易金融等）。尽管目前这两类解决方案还自成一体，但预计业界在之后会开发出一套整合的系统，该系统由托运人、货运代理人、海运承运人、港口和海关当局以及银行等部门组成，是一个参与各方在区块链上相互关联实时交互的网络。

2016 年，巴克莱（Barclays）和金融科技初创企业 Wave 声称，它们将成为最先使用 Wave 区块链平台完成全球贸易交易的机构（Taylor，2016）。软件巨头 IBM 在区块链应用以及贸易金融的智能合约方面一直处于领先地位（Haswell，2018）。2017 年 3 月，IBM、马士基（Maersk）与 Hyperledger Fabric 合作，宣布完成了基于区块链技术的端到端数字化供应链试点项目，该供应链包括各贸易方、港口和海关当局（Allison，2017）。[26] 2017 年初，IBM 进一步为中国制药行业推出了 Yijian 区块链技术应用系统，并与一家集团公司合作开发了一个基于区块链的原油贸易融资平台（Higgins，2017a）。[27]

近期，区块链技术在货运和物流行业的应用也取得了一些进展。2017 年 9 月，马士基携手安永、微软、韦莱韬悦（Willis Towers Watson）和一些保险公司，试图在 Guardtime 开发的区块链 KSI 上安全地共享货运数据（Hackett，2017）。2017 年 11 月，有报道称，包括 ShipChain 这类初创企业在内的全球区块链货运联盟吸引了传统货运行业中全球巨头的加入，如思爱普（SAP）和联邦快递（UPS）等。

### 1.3.2 可信支付

由于缺乏信任，长距离以及陌生个体之间的支付通常非常困难。环球银行

---

[26] 这个试点项目是 Schneider Electric 从里昂发往纽瓦克的一批货物，涉及鹿特丹港、纽瓦克港、荷兰海关总署、美国国土安全部科学技术理事会以及美国海关和边境保护局（Allison，2017）。

[27] 其他以区块链为基础的平台还对贷款、签发信用证、出口信贷和保险等服务提供支持，如香港贸易金融区块链、TradeSafe、数字商业链（Digital Trade Chain，DTC）等。最近，由区块链初创公司 R3、金融贸易的技术支持者 TradeIX，以及其他几家大型银行构建的“Marco Polo 贸易金融平台”进入了试点阶段（Pamler，2018）。

金融电信协会（SWIFT）虽然可以缓解该困难，但是通常伴随着多个机构之间的低效率协作以及高昂的费用。在电子支付体系中，由于双重花费问题的存在，支付问题也变得更加严重。

而比特币通过点对点的匿名交易有效解决了双重花费问题。这一解决方案不仅安全而且带有时间戳，从而使交易不会被篡改（Nakamoto，2008）。[28] 更重要的是，通过向全网中的参与者广播比特币交易，以及让矿工通过不断竞争新区块的记录权从而赚取比特币的设计，这类分布式账本技术可以提供关于交易是否发生的实时分布式共识。

根据设计，要维持比特币区块链上的分布式共识记录，挖矿者需要解决棘手的 NP－完全计算问题（即挖矿，PoW 的一种形式）。由于解决该问题需要非常大的算力，这也使得比特币区块链不太适用于大规模的金融交易。随后的平台，如 Lightning（建立在比特币区块链上）和 Stellar（一个独立的区块链），通过本地渠道和多重签名账户等方式提高了计算机的处理能力，使得很多不必要的信息不必作为分布式共识的一部分而存储在区块链上。[29]

也就是说，区块链的脚本语言是受限的。以太坊是市值仅次于比特币区块链的第二大区块链平台，它通过允许使用图灵完备语言和更复杂的应急操作（Turing，1937），提供了智能合约的原型（Buterin，2014）。所有关于合约状态的有效更新都可以得到记录和自动执行。一组自愿参与者（以太坊的矿工）维护分布式共识中状态的记录，而其他交互方利用共识信息自动执行合同条款。就像网站构建在 Internet（互联网）协议上一样，其他应用［如 Monax 和 Phi（String Lab）］，也通过构建在以太坊上，丰富和优化其智能合约的功能与执行能力。

传统的金融行业参与者也在积极采用区块链技术解决支付问题。如越来越多的大银行和支付网络开始采用 Ripple 这一结算基础设施工具（Ripple 成立于 2012 年，最初被称为 Ripple Labs），辅助其开展全球金融交易和实时跨境支付服务；一组验证节点（通常数量很大）使用 Ripple 的交易协议 RTXP 以实现分布式共识（RTXP 是一个替代工作证明的迭代共识过程，交易在各个验证节

---

[28] 日本的很多零售商已经开始接受比特币作为支付工具（具体可参见 *The Economist*，2017）。

[29] 交易对手也建立在比特币区块链上，但是允许他们使用更灵活的智能合约，如通过“销毁证明”（Proof-of-burn，POB）来形成共识。销毁证明是指客户支付的比特币会被销毁，而节点通过验证货币升值获得奖励。

点上被反复广播，直到达成协议）；数字转账通过电子化方式连接到银行账户，或使用其自带的加密货币 Ripples（XRP）自动实现。

### 1.3.3 其他应用

除了在支付和贸易金融方面的应用，区块链和智能合约还可应用于交易所和交易平台、投票甚至银团贷款等方面。2015 年，纳斯达克推出 Linq 平台来管理和交易上市前的股份；2017 年初，纳斯达克在爱沙尼亚塔林股票交易所运用区块链技术成功完成了代理投票的测试（Shin，2017）。智能合约还通过为金融衍生品制定标准交易规则，简化了场外交易的金融协议。Symbiont 提供了一个界面非常简单的产品，该产品被用于在发行智能证券时规定相关的条款和条件，以及整合市场数据等方面。[30] 此外，由瑞银（Credit Suisse）、12 家其他银行和 Symbiont 主导的一个区块链项目被用于开展银团贷款（Terekhova，2017）。最后，沃尔玛与 IBM、京东合作，最近推出了用于跟踪食品生产、安全和分销的区块链。

## 1.4 实践过程中的验证与信息问题

本文的理论证明了在形成分布式共识过程中信息分发的负面作用。业内人士也表达出对区块链在信息分发和信息隐私方面的关注，如 R3 CEV（一个活跃的区块链联盟）非常直率地表示，R3 的 Corda 系统试图通过只允许参与交易的各方以及有正当理由需要了解交易的人获得交易细节，解决信息分发问题。但即使如此，证明交易唯一性的请求（它本身就是一种信息）还是被分发给一些独立的观察者，使得市场的信息环境发生了局部改变。

尽管上述措施有可能确保信息的保密，但目前的讨论忽略了两个重要方面。第一，只联系较少的记录者可能会降低共识的有效性。第二，加密数据意味着这些数据在某些状态下不能被验证，因此它们不能被用于智能合约；进一步地，加密数据也仍然是数据，因为即使单纯的验证请求行为仍然会将与真实状态相关的信息传递给记录者（后文的模型将体现这一点）。正如德维拉卡·布尔戈斯等人（de Vilaca Burgos et al.，2017）在递交给巴西央行的一份报告中指出的那样，单纯地将敏感数据加密并不是一个可行的解决方案，因为在该情形下智能合约将无法

---

[30] Symbiont 是超级账本项目（Hyperledger project）的成员之一，这是一个跨行业的开源合作项目，由非营利机构 Linux 基金会主导，旨在通过制定通用标准来推进区块链技术的发展。

决定交易是否有效。

上述观察表明，限制信息分发往往是以牺牲共识体系的有效性为代价的。如 R3 的 Corda 验证模型将信息分发限制在公证人范围之内。[31] 但正如上文提到的加拿大银行的报告所述，查普曼等人（Chapman et al.，2017）认为，与很多公有链中每个节点都为系统提供信息不同，Corda 的模型需要从公证人那里复制数据以确保业务的连续性，这使系统再一次变得集中化，而这可能导致“单点故障”（SPoF）问题的发生。事实上，在 Jasper 项目的第二阶段，Corda 中的公证员角色就是由加拿大银行扮演的，而如果银行的服务发生中断，就会阻碍所有支付交易的进程。

本文强调了这一冲突，即关联较少的记录者会减少信息分发，但会以牺牲高质量的分布式共识为代价。在第 2 节中我们将进一步分析信息分发会对产业组织和市场竞争带来什么影响。

## 2. 区块链冲击与产业组织

为了理解区块链对现实世界的影响，我们借鉴格林和波特（1984）的研究，在标准动态产业组织的模型下刻画了分布式共识的形成过程。我们发现，去中心化的智能合约有助于市场进入、促进竞争，但更多的信息分发也可能助长合谋，损害竞争。

### 2.1 模型设定

考虑一个风险中性的世界，其中时间是无限和离散的，我们标记为 $t$，$t = 0,1,2\cdots$。每个行为人都有一个贴现因子 $\delta \in (0,1)$。在每个 $t \geqslant 0$ 的时期，买方出现的概率为 $\lambda$，每个买方需要一单位的商品。买方会在向卖方询价之后，选择最有吸引力的报价。这里我们用 $\mathbb{I}_t$ 指代买方是否在 $t$ 期出现这一总体经济状态。在本文的论述中，“买方”、“顾客”和“消费者”始终可以互换。

商品在买卖双方交付的过程与本文第 1.2 节中的描述类似。值得说明的是，尽管本文以贸易金融为背景建模，但是本文的商品还可以被理解为一种服务，如资金转移、贷款发放或贸易融资等。买方（如果存在的话）只存在一

[31] 这一限制是为了防止拒绝服务（DoS）攻击，即在知情的情况下，节点通过使用一些现有状态集构建无效的交易，并将其发送给公证员，从而导致这些状态被标记为已消费。

期，之后退出经济。

有三个卖方长期存在，他们要么是诚实型的，要么是欺诈型的。欺诈型卖方不会发货，而诚实型卖方总是发货。买方从与卖方 $i$ 的交易中获得的期望收益为 $q_i$。具体地，有 $q_i$ 的概率，消费者获得 1 单位的效用，有 $1-q_i$ 的概率，消费者获得的效用为 0。

在博弈刚开始的时候，即 $t=0$ 期，已知有两个诚实型卖方 $A$ 和 $B$（他们都已经建立了良好的声誉），以及一个新进入者 $C$，进入者 $C$ 的类型为私有信息，其他人对 $C$ 只有共同的先验信念，即 $C$ 为诚实型卖方的概率为 $\pi$，下文用 $\pi$ 来表示 $C$ 的声誉。

在每个 $t \geqslant 0$ 的时期，每个卖方都被随机分配一个 $q_i, i \in \{A,B,C\}$，$q_i$ 服从独立同分布。产品质量 $q=(q_A,q_B,q_C)$ 为公共信息，刻画了卖方之间的暂时差异。我们会在第 3.3 节中分析当产品质量为卖方私有信息时的情况。我们令 $q$ 中的元素以递减顺序 $q^{(1)}$，$q^{(2)}$ 和 $q^{(3)}$ 排列，这意味着即便买方选择在位卖方，也会对福利产生影响。我们将商品质量分布的累积分布函数和概率密度函数分别记为 $\Phi(q)$ 和 $\phi(q)$，支撑集为 $[\underline{q},\bar{q}]$。卖方的生产成本为 $\mu$，当 $\mu < \underline{q}$ 时，表示诚实型卖方的交易可以提升福利。

卖方 $C$ 可以通过支付一笔任意小的成本 $\epsilon > 0$ 进入市场，这意味着 $C$ 只有在预期进入市场能够获得严格为正的利润的情况下，才会选择进入。[32] 这使我们可以将进入者卖方是否诚实这一信息不对称作为相关的进入壁垒。我们进一步假设，进入者在获得客户之前没有损失吸收能力。[33]

## 2.2 传统世界

如下我们将从合同订立空间与信息环境的关键假设开始，对传统世界中的模型进行分析。

### 2.2.1 合同订立的空间与信息

**假设 1** 在传统世界中，任何付款都不取决于服务交付是否发生。每个卖

---

[32] 给定任意小的进入成本，$C$ 的进入决策是在质量 $q_C$ 实现之前决定还是在实现之后决定并不重要。

[33] 在该情形下，潜在的进入者不能采取激进的渗透定价方案。卖方在没有顾客之前没有吸收损失的能力是排除卖方采取激进的渗透定价方案的充分条件（其中进入者为了进入遭受巨大损失）。该条件是符合现实的，由于缺乏随时间推移而积累的服务利润，新进入者通常没有足够多的初始资本激进地降低价格。实际上，我们需要的全部条件就是 $C$ 对损失 $L$ 的容忍程度不能超过 $[\underline{q}-\pi\bar{q}]^+$。

方只能观察到自己的买方及其相关的交易信息。

假设1的前半部分反映了现实世界中合同的不完备性，这种不完备性要么限制了共识的有效性，要么使得合同订立的成本过高；关于订立和执行完备合同的成本，请参阅哈特（Hart，1995）和梯若尔（Tirole，1999）的研究。在我们的模型中，这意味着卖方会私下向买方报一个不随货物交付状态而变化的价格 $p_i(q)$；[34] 假设1的后半部分意味着卖方不能观测到其他卖方的报价，这可以理解为卖方根据其私有信息以及与买方的私下互动提供了一个“定制化”的报价。换句话说，除了交易信息之外，行为人之间不存在任何形式的信息沟通，这一假设借鉴了格林和波特（1984）以及波特（1983）的模型设定，它在我们求解卖方的合谋均衡时起到一定作用。

### 2.2.2 伯特兰德竞争和市场进入

首先，我们考虑竞争性均衡的情况，在竞争性均衡下，卖方会持续降低报价直到竞争者退出。设想一个诚实型进入者 $C$。如果 $\pi q_c < \max\{q_A, q_B\}$，任何在位者卖方总是会争着将价格降低到 $\mu$，以便在这个时期获得顾客，从而防止 $C$ 在该期进入并引发未来更高程度的市场竞争。由于没有诚实的声誉，进入者 $C$ 只有在 $\pi q_c \geqslant \max\{q_A, q_B\}$ 的情况下，才有机会获得顾客。[35] 实际上，只有当新进入者的品质认知度高于所有在位者的时候，他才能够吸引到顾客。此时，如下命题成立：

**命题 2.1** 在竞争性均衡中，诚实型卖方 $C$ 第一次服务客户的时间为时期 $\tau \equiv \min\{t \geqslant 0 \mid \pi q_{C,t}, \mathbb{I}_t \geqslant max\{q_{A,t}, q_{B,t}\}\}$ 或此之后。因此，如果 $\pi \bar{q} < \underline{q}$，$C$ 永远不会进入市场。

在本文的剩余部分，我们关注 $\underline{q} > \pi \bar{q}$ 的情形；换言之，进入者 $C$ 的声誉非常低，以至于在传统世界中不会发生市场进入。在任意时间 $s$，预期的未来消费者剩余和社会福利分别为：

$$\prod_{buyer} = \mathbb{E}_s\left[\sum_{t=s+1}^{\infty} \delta^{t-s}\, \mathbb{I}_t(\min\{q_{At}, q_{Bt}\} - \mu)\right] = \frac{\delta\lambda}{1-\delta}\mathbb{E}[\min\{q_A, q_B\} - \mu] \qquad (5)$$

---

[34] 卖方发出要约这一假设在消费者或买方是短期存在且分散的情况下是符合现实的。例如，银行通常会对国际转账服务进行报价，然后客户可以决定去哪家银行转账。对于这一特定的交易协议，本文的主要结果是稳健的。

[35] 尽管如此，如果在位者使用渗透定价方式，进入者 $C$ 还是有可能得不到任何市场份额。注意当 $\pi \bar{q} < q$ 时，不管 $q$ 取何值，$C$ 都不会进入市场（即使 $C$ 采取渗透定价），因为此时 $C$ 可以承受的最大损失小于 $q - \pi \bar{q}$。

$$\prod_{total} = \mathbb{E}_s\left[\sum_{t=s+1}^{\infty} \delta^{t-s}\, \mathbb{I}_t(\max\{q_{At}, q_{Bt}\} - \mu)\right] = \frac{\delta\lambda}{1-\delta}\mathbb{E}[\max\{q_A, q_B\} - \mu] \quad (6)$$

欺诈型卖方的存在使得高质量的进入者 $C$ 无法进入市场，造成了典型的柠檬问题。我们稍后将说明，如何借助区块链技术部分或完全地解决该问题。

### 2.2.3 合谋均衡

除了竞争性均衡之外，传统世界中还可能会出现合谋均衡。给定卖方 $C$ 不会进入市场，我们仅需要考虑在位者之间是否会形成合谋策略。

我们将每个卖方的策略限制为格林和波特（1984）讨论过的标准超级博弈策略。具体来说，考虑如下参数为 $\{T, f\}$ 的合谋策略，该策略分为两个阶段：

（1）合谋阶段：每个时期，在卖方的类型实现以后，卖方 $A$ 要价 $q_A$，卖方 $B$ 要价 $q_B$。$A$ 和 $B$ 获得的买方比例分别为 $\mathbb{I}_t f(q_A, q_B)$ 和 $f(q_B, q_A) = \mathbb{I}_t(1 - f(q_A, q_B))$ ㊱，其中 $f(x, y) \in (0,1)$ 是提议的匿名配置函数，它也可以是卖方类型实现的函数。该配置函数 $f$ 包括卖方总是平等划分买方，或所有买方都与更好的卖方交易等情形。

（2）惩罚阶段：一旦其中一个卖方没有任何买方，就会触发惩罚阶段。更具体地说，惩罚阶段可以由以下任意一种情况触发：（i）买方在这段时间没有出现；或者（ii）其中一个卖方偏离合谋均衡，即通过报出更低价格获得了所有买方。一旦惩罚阶段被触发，$A$ 和 $B$ 就会在固定时期 $T$ 内进行伯特兰德竞争。

回想一下，卖方观察不到其他卖方的报价，而只能观察到自己客户的情况。然而，由于可以使用自己的私有信息推断该期是否出现了客户，因此这种有私人监督的重复博弈本质上是一种不完美情况下的公共监督博弈。这里的不完美性体现在，即使没有任何卖方偏离合谋均衡，惩罚依旧会被触发。

文献中关于动态重复博弈的一个标准结论是可持续的均衡主要取决于贴现因子 $\delta$ 的大小，无名氏定理（Folk Theorem）就是其中最有名的例子。因此，我们可以推导出贴现因子的下限，并将其表示为 $\delta_{(T,f)}$。而在它之上存在着一个均衡，该均衡对应着特定的 $T$ 和 $f(x, y)$。

**引理 2.2** 定义 $f(q_i) \equiv \mathbb{E}_{q_j}[f(q_i, q_j)]$ 为质量为 $q_i$ 的卖方吸引的买方比例，则一个有着参数 $\{T, f\}$ 的合谋策略需满足如下条件才是一个均衡：

$$(M_1 - M_2)\lambda\delta(1 - \delta^T) \geqslant M_3(1 - \lambda\delta - (1 - \lambda)\delta^{T+1}) \quad (7)$$

---

㊱ 当卖方报价比合谋时的报价更低时（即低于 $q_i$），我们的分析仍是稳健的。

其中 $M_1 \equiv \mathbb{E}[f(q_i)(q_i - \mu)]$，$M_2 \equiv \mathbb{E}[[q_i - q_j]^+]$，$M_3 \equiv \max_{q_i}\{(1 - f(q_i))(q_i - \mu)\}$。

这里，$M_1$ 为卖方在合谋阶段每一期的期望收益，$M_2$ 为卖方在惩罚阶段每一期的期望收益，$M_3$ 为卖方偏离均衡策略时获得的最大收益。当贴现因子足够小（卖方不够耐心的时候），偏离均衡获得的收益会高于其在未来受到惩罚时获得的收益。此时，不存在稳定的合谋均衡。

**命题 2.3** 当贴现因子 $\delta < \delta_o^{Traditional} \equiv \inf_f \delta_{(T,f)}^{Traditional} = \inf_f \frac{1}{\lambda} \frac{M_3}{M_1 + M_3 - M_2}$ 时，对于任何 $(T,f)$，都不存在合谋均衡。

在参数为 $(T,f)$ 的合谋均衡下，社会福利取决于 $f$，而消费者剩余由 $(T,f)$ 以及合谋价格共同决定。消费者剩余与惩罚的期数 $T$ 有关，这是因为当没有买方这一情况出现触发了惩罚阶段时（每一期该情况发生的概率为 $1-\lambda$），买方可以获得正的消费者剩余。

## 2.3 区块链世界

通过记录者验证信息，区块链技术可以帮助参与者达成有关商品交付状态的共识。正如在第 1.2 节中详细介绍的，这一验证过程通常涉及信息分发。

为了强调这一经济力量，我们首先研究在完美共识下的情况，即当 $K \to \infty$，$\tilde{z} = \tilde{\omega}$ 时，基于区块链技术如何形成共识。该情形刻画了许多现存的区块链，如比特币、Ripple 和 Symbiont 等，在这些区块链上，验证请求或交易信息被分发给足够多的参与者，其中包括重要的机构参与者（注意，这里并不是说区块链上的所有人都是记录者）。进一步地，本文将在第 3.2 节中分析，在非完美共识下，共识质量与信息分发之间的权衡。

**假设 2** 区块链通过关联无限的参与者（包括卖方和一组连续分布的买方），从而形成有效的分布式共识。更具体地，卖方通过观察其顾客出现的情况或通过在被联系过程中推断出顾客出现的总体情况，知道当前市场的总体状态，由此形成共识 $\tilde{z} = \tilde{\omega}$。

回忆一下，$\tilde{\omega}$ 是关于交付状态（成功与否）的信息。假设 2 意味着：（1）自我执行的智能合约完全依赖于参与者对货物状态的共识；（2）卖方可以观察到区块链上整体的经济活动。这一点与假设 1 形成了鲜明的对比。此外，我们还注意到，区块链系统可能具有更丰富的信息，通过使用这些信息，

模型结果可以得到进一步扩展。而本文的论述仅需要较弱的条件，即仅要求卖方可以观察到总体的经济活动。

本节的余下部分，我们将探讨区块链和智能合约如何提高市场进入和市场竞争，并展示该技术如何导致更多的合谋行为，在此之上，我们还会进一步讨论其中的政策含义。

### 2.3.1 智能合约与市场进入的增加

在区块链的世界中，进入者可以根据商品的交付状态报价，即 $\mathbb{P} = (p^s, p^f)$，其中 $p^s$ 和 $p^f$ 分别为商品交付成功和交付失败时的卖方报价。一个诚实型进入者 $C$ 可以通过提供 $(p^s,0)$ 的价格将自己与欺诈型对手相区别。欺诈型对手并不能从模仿该策略中获得收益，因为他知道最后的结果肯定会以交付失败、自己得到零利润而告终。所以，此时诚实型卖方肯定会进入市场。在竞争性均衡（不存在合谋）中，我们可以得到如下命题：

**命题 2.4** 在区块链世界的竞争性均衡中，诚实型卖方 $C$ 肯定会进入市场，他们首次进入市场的时期为 $\tau = min\{t \geqslant 0 \mid q_{c,t}\mathbb{I}_t \geqslant max\{q_{A,t}, q_{B,t}\}\}$ 或者更早。

在区块链世界的竞争性均衡中，预期未来消费者剩余和社会总福利在 $t = s$ 时分别为：

$$\prod_{buyer} = \mathbb{E}_s\left[\sum_{t=s+1}^{\infty}\delta^{t-s}\mathbb{I}_t(q^{(2)} - \mu)\right] = \frac{\delta\lambda}{1-\delta}\mathbb{E}[q^{(2)} - \mu] \tag{8}$$

$$\prod_{total} = \mathbb{E}_s\left[\sum_{t=s+1}^{\infty}\delta^{t-s}\mathbb{I}_t(q^{(1)} - \mu)\right] = \frac{\delta\lambda}{1-\delta}\mathbb{E}[q^{(1)} - \mu] \tag{9}$$

与（5）式和（6）式相比，消费者剩余（二阶统计量的线性函数）和社会福利（一阶统计量的线性函数）都有所上升。这表明，由智能合约导致的市场进入增加和市场竞争提升，会使整个经济变得更有效率。

### 2.3.2 许可链中合谋的增多

虽然区块链与智能合约可以鼓励市场进入与竞争，并以此改善消费者剩余和社会福利，但它们也可能导致更差的结果。在这些更差的结果中，动态均衡中的社会福利与消费者剩余水平都低于传统世界。为了说明区块链增加合谋的这一效果，我们首先关注只允许在位者而不允许进入者使用的许可链（此时没有市场进入），随后我们再讨论允许所有人参与的公有链。

#### 2.3.2.1 使用智能合约进行合谋

正如下文阐述的那样，在区块链和智能合约的技术下，卖方可以利用更丰

富的或然情况以及由此产生的补偿支付（side payment）来促成合谋。所有卖方都一致性地约定向买方报出一个他们可以要得到的最高价格 $q_i$，该价格可以有效地从买方那里榨取全部剩余。卖方还约定，每一期提供最高质量商品的卖方获得所有消费者。如果一个卖方没有为消费者提供最好质量的商品，智能合约就会自动地将该卖方获得的利润转移给其他卖方。[37] 通过对偏离均衡的行为施加这一自动惩罚，智能合约就可以在任何贴现因子水平下支持稳定的合谋。

上述利用智能合约达成的合谋非常容易被发现，也可以被反垄断法轻易禁止（见本文3.1.2节）。而一个更为相关和有趣的现象是，即使智能合约没有发生明显的补偿支付，区块链仍然可以导致更严重的合谋，而这正是我们接下来要讨论的内容。

2.3.2.2 许可链中的隐性合谋

在隐性合谋中，我们考虑与传统世界中相同的合谋阶段、惩罚阶段和配置函数 $f$。这里的关键在于，在传统世界中，卖方偏离均衡的行为以及没有消费者出现这两种情况均可以触发惩罚阶段，与此不同，在区块链世界中，由于被联系的参与者至少可以从是否有服务请求发出（获取该信息甚至不需要参与者安装物联网传感器）这一信息中推断出市场中消费者出现的情况，所以此时的惩罚阶段只能由卖方违背合谋策略这一行为触发，这使得卖方可以完美地监督合谋者偏离均衡的行为。[38]

换句话说，由于偏离均衡的行为可以在区块链生成分布式共识的过程中被准确识别出来，因此传统世界中不完美公共监督下的重复博弈现在变为完美的公共监督博弈。可持续的合谋均衡也变得更加容易实现（在均衡路径上不存在惩罚）。

**命题 2.5** 对于给定的 $(T,f)$，我们定义在许可链中可维持合谋的临界贴

---

[37] 为了让智能合约生效，分布式共识形成过程中还需要卖方的身份信息，只有这样，区块链系统才能识别出是否是最优的卖方在服务所有的消费者。更为一般的，在不同的合谋均衡中，即使在缺乏卖方身份信息/特征的情况下，系统还是可以对偏离合谋均衡的行为进行惩罚。

[38] 为了避免引发价格战，偏离合谋均衡的卖方很有可能想在线下进行货物交付，这牵涉我们关于在位者都是诚实型卖方的假设。然而，更一般化地，智能合约对所有交易者都是有益的，即使对在位者而言，线下窃取市场份额也较为低效。此外，在我们关于贸易金融的例子中，卖方在线上线下转换的灵活性也存在很多问题。

现因子为 $\delta_{(T,f)}^{\text{Blockchain2}}$，回想在命题 2.3 中定义的 $\delta_{(T,f)}^{Traditional}$ 以及 $\delta_0^{Traditional}$，我们有如下命题：

（1）对于任意的 $(T,f)$，$\delta_{(T,f)}^{Blockchain2} < \delta_{(T,f)}^{Traditional}$。

（2）当贴现因子 $\delta \in [\inf_f\{\delta_{(T,f)}^{Blockchain2}\}, \delta_0^{Traditional}]$ 时，合谋均衡只在区块链世界中存在。

在（2）中，合谋下的消费者剩余要低于在没有区块链的竞争性均衡中的消费者剩余。

## 2.4 区块链冲击

现在假设有一个允许 3 家公司（在位者 $A$ 和 $B$，以及新进入者 $C$）都使用的公有链，那么进入者进入带来的收益会超过合谋增多带来的成本吗？

### 2.4.1 公有链下的消费者剩余

回想在第 2.3.1 节中求解的竞争性均衡，为了描述经济中其他可能的合谋均衡，我们考虑如下合谋策略：

（1）合谋阶段：每一期，在卖方的类型实现以后，每个卖方根据商品交付的状态提出报价 $q_i$。令 $\hat{f}(q_i,q_j,q_k) \in (0,1)$ 表示产品质量为 $q_i$ 的卖方服务的消费者份额，此时其他两个卖方的产品质量分别为 $q_j$ 和 $q_k$。

（2）惩罚阶段：当该期有买方出现，但其中一个卖方没有见到任何买方的时候，惩罚阶段就会被触发。换言之，只有在有些卖方偏离均衡策略的时候，惩罚阶段才会被触发。一旦触发惩罚阶段，所有卖方就会在 $T$ 期进行伯特兰德竞争。

**引理 2.6** 设定产品质量为 $q_i$ 的卖方得到的消费者份额为 $\hat{f}(q_i) \equiv E_{q_{-i}}[\hat{f}(q_i,q_{-i})]$。在区块链世界中，如果参数满足下式，则上述合谋策略就可以成为均衡：

$$\delta\lambda(1-\delta^T)(\hat{M}_1-\hat{M}_2) \geqslant (1-\delta)\hat{M}_3 \tag{10}$$

其中 $\hat{M}_1 \equiv \mathbb{E}[\hat{f}(q_i)(q_i-\mu)]$，$\hat{M}_2 \equiv \mathbb{E}[(q_i-max_{j\neq i}q_j)^+]$，$M_3 \equiv \max_{q_i}\{(1-\hat{f}(q_i))(q_i-\mu)\}$。

对上述各 $\hat{M}$ 的解释与引理 2.2 中类似，但需要注意的是，此时针对的是三个卖方，而不是两个卖方。（10）式的左边也稍有调整，这是因为在完美公共

监督的情况下，惩罚变得更加精准。

### 2.4.2 区块链冲击下的动态均衡

更一般地，就福利和消费者剩余而言，有区块链冲击的均衡结果集是传统世界均衡结果集的一个非平凡超集。我们使用 Blockchain3 表示有三个卖方的公有链。

**定理 2.7** 贴现因子的临界值 $\delta_a^{Blockchain3} \equiv \sup_{\hat{f}}\{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$ 定义良好且满足 $\delta_a^{Blockchain3} < 1$。对于所有的 $\delta > \delta_a^{Blockchain3}$，任何在传统世界中实现的消费者剩余和社会福利都可以在区块链世界中得以实现。此外，区块链世界还存在一些其他的均衡结果，相比于传统世界，这些结果下的消费者剩余和社会福利可能会更高或更低。

在定理 2.7 中，$\delta_a^{Blockchain3}$ 的下标 a 表示“all”，即所有，表明如果贴现因子高于 $\delta_a^{Blockchain3}$ 的话，那么所有的合谋均衡都可以维持。类似地，我们可以定义临界值 $\delta_0^{Blockchain3} \equiv \inf_{\hat{f}}\{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$，则此时只需满足一个更弱的条件，即 $\delta > \delta_0^{Blockchain3}$，比特币技术就有可能损害消费者福利。

值得说明的是，当所有卖方都参与合谋并且所有的服务都由有着最低质量 $q_i$ 的卖方提供的时候（该质量比仅存在在位者时的商品质量还要低），区块链技术可能会使社会总福利减少。

本文的结论在有更多在位者和进入者的时候也是稳健的，下面的引理阐述了在更一般化的情形下，消费者剩余为何在区块链世界中可能变得更低。

**引理 2.8** 对于 $m \geqslant n \geqslant 2$，如果 $\lambda < \frac{n-1}{n}$，则 $\delta_0^{Traditional,n} > \delta_0^{Blockchain,m}$，其中 $m$ 和 $n$ 分别代表在有区块链和没有区块链的情况下，参与合谋的卖方的数量。因此，对于所有的 $\delta \in [\delta_0^{Blockchain,m},1]$，此时传统世界中 $n$ 个卖方之间不存在合谋，而区块链技术会使消费者剩余变得更低（区块链世界中共有 $m$ 个卖方，这其中包括新进入的卖方）。

## 3. 讨论与拓展

在本节中，我们将从监管的角度提供一些讨论，并对前文的模型进行若干拓展。

### 3.1 减少区块链上合谋的措施

本文对区块链可能破坏市场竞争的担忧与市场上其他观察者的观点一致。

尤其当探讨 R3 这类许可链的时候，由于其链上成员都是大型金融机构，这一担忧变得更加严重。正如卡明斯卡（Kaminska，2015）指出的那样，“这种技术真正促进的是那些虽然互不信任但为了维护其所在市场的价值和稳定，仍需要合作并形成卡特尔的团体”。本文强调了一种区块链可以阻碍竞争的特定经济机制，并严谨地分析了合谋为何发生以及如何发生的情况。实际上，实证研究也发现，更大程度的信息共享可能会导致合谋发生（Bourveau et al.，2017）。下面我们将在本文的分析框架下讨论如何通过监管和市场措施抑制合谋。

#### 3.1.1 区块链竞争与企业竞争

虽然我们关注的是多个卖方在单一区块链上竞争的情况，但在实践中，也可能存在多个区块链以供卖方和买方选择。由于买方总是选择能够提供最优价格的区块链，因此区块链之间的竞争似乎不利于卖方在一个区块链上达成合谋行为。虽然区块链竞争也许可以缓解在特定区块链上的合谋行为，但从长远看，如果某个区块链由于网络效应占据支配地位，监管者仍然需要通过拆分区块链平台、防止合谋等方式进行干预。虽然这种“拆分大玩家”的方法对传统工业企业也适用，但这一点对于区块链尤其重要。这是因为，虽然合作是区块链生态系统中不可或缺的组成部分，但合作也可能会扰乱系统运作。对于一个即将被启用或想要增强竞争程度的新区块链平台而言，不同的机构用户和散户必须就如何使用这个平台进行协调与合作；而协调问题已经在比特币、以太坊等加密货币的市场先行者具有支配地位这一事实中得到了充分体现。[39]

当然，上述讨论也提出了其他问题：如为什么相比于在同一个区块链上的卖方而言，区块链之间的合谋更加困难？政府可以做些什么来促进协调，从而改善区块链平台的设计？这些都是非常有趣并且有待未来研究的问题。

#### 3.1.2 监管节点与设计

在传统世界中，观察和收集更多的市场信息通常有助于监管机构更好地发现合谋。类似地，在区块链中，尤其是在私有的许可链（通常没有自动将监管机构纳入商业生态系统）中，增加一个监管节点，可以帮助监管者更好地监督市场参与者的经济行为，减少参与者之间的合谋。然而，如果是这样的话，区块链世界和传统世界就不再有差别：因为无论在哪个世界中，有权调查

---

[39] 作者感谢 *Review of Financial Srudies*（RFS）主编 Itay Goldstein 为我们指出了这一点。

和惩罚公司的政府都可以达到相同的结果。如同在我们的模型中，通过监督买方（如果买方存在的话）是否购买了最高质量的商品，监管者就可以发现并阻止合谋行为。

然而，得益于区块链上的实时防篡改记录，我们相信区块链世界比传统世界具有更大的优势。因此，监管者不必担心报告错误和时间延迟，他们能够以相对较高的频率发现和遏制合谋与市场失灵。此外，回溯性审计也不再易于操纵，第1.3节中的Hyperledger Fabric案例体现了这一点。

监管者还可以参与区块链协议的设计，如政府可以保留全网广播的部分加密信息的访问权限，访问权限的设定不仅能够消除利用智能合约开展的合谋行为（见第2.3.2节的讨论），还可以基于对交易和定价行为的统计分析更好地发现合谋行为。[40]

#### 3.1.3 用途与共识生成的分离

在模型中，卖方可以利用区块链上的信息更精准地惩罚其他卖方偏离均衡的行为。同时，他们之所以可以观察到区块链上的信息，是由于他们在帮助生成分布式共识的过程中，信息被分发并记录在区块链上。从这个角度看，一个较为明显的解决方案是将那些帮助生成分布式共识的参与者与分布式共识的使用者分离开来。如在我们的模型中，如果卖方只能使用区块链技术与买方签订智能合约，而不能参与信息的记录行为，则他们就不能再使用加总的市场信息进行合谋。

正如本文第1.2节中关于贸易金融的例子中谈到的，将卖方从信息记录的活动中排除有很大的难度。这是因为那些被排除的参与者很可能是最有资格验证记录的人（例如，他们可能是来自同一行业、有着丰富经验的其他卖方）。现在大多数公有链还没有将这两个群体分离，部分区块链，如Symbiont，倾向于将记录者和终端用户分离，然而该方案还有待进一步探讨。

在区块链从业者之间，关于用途与共识生成相分离的讨论还比较新颖，然而，它反映了在去中心化（一个有弹性的体系需要更广泛的参与者）和中心

---

[40] 当区块链上存储和处理的信息量很大的时候，监管层也有其他方面的担心。在区块链在贸易金融的应用中，大部分数据都为私人数据，从而他们需要遵从监管［如遵从“通用数据保护条例”（GDPR），该条例从2018年5月25日起生效，并且适用于所有在欧盟国家的区块链平台］。在该情况下，区块链应该被设计为一个私有链或许可链，由一个或多个制定使用条款的实体进行运营，这些实体作为控制者，负责在遵循法律的条件下对个人数据进行编译。

化（只有少部分有经验的参与者才能提供高质量的输入信息）之间的另一权衡，该权衡构成了未来关于区块链应用政策讨论的重要方向。㊶

### 3.2 不完美共识

在第 2 节中，我们假设有无数的区块链参与都作为记录者参与共识的生成（$K \to \infty$），此时即为完美共识的情况。如果假设只有有限的区块链参与者可以作为记录者，即 $|K| = K < \infty$，此时就是不完美共识。假设在不完美共识下，正确记录商品交付状态的概率为 $\psi$，其中 $\psi = \sum_{k \in \mathbb{K}^*} \omega_k \leqslant 1$，且 $\mathbb{K}^* = \{k \in \mathbb{K}: b_k\, \omega_k < h_k\}$［具体见式（3）］。

$\psi$ 本质上以简化形式刻画了在不完美共识下的共识质量，许多其他协议具有与此相一致的特征。㊷ 简单地说，一次成功（失败）的交付可能被记为交付成功的概率为 $\psi$（$1-\psi$）。在不完美共识下，诚实型进入者能否在区块链的帮助下通过智能合约 $(p^s, p^f)$ 进入市场，并将自己与欺诈型进入者区别开呢？

现在我们允许进入者可以承担初始损失，假设进入者承担初始损失的能力为 $L$，它帮助诚实型进入者将自己与欺诈型进入者区分开来，该假设放松了第 2 节脚注㉜中“排除激进型定价策略”的假定。在分离均衡下，诚实型卖方在阶段性博弈中求解如下最大化问题：

$$\max_{(p^s, p^f)} \psi\, p^s + (1-\psi)\, p^f$$

$$s.t.\ \psi\, p^s + (1-\psi)\, p^f \geqslant \mu,\ -p^f \leqslant L, \text{以及} (1-\psi)\, p^s + \psi\, p^f < 0$$

三个不等式分别为诚实型卖方的参与约束、进入者有限的损失承担能力，以及欺诈型卖方不会模仿诚实型卖方的约束。如在最后一个不等式中，欺诈型卖方有 $1-\psi$ 的概率被记录为成功交付商品，此时他获得的收益为 $p^s$；同时，他有 $\psi$ 的概率被记录为交付商品失败，此时他获得的收益为 $p^f$。当参数满足 $\psi \geqslant \dfrac{\mu + L}{\mu + 2L}$ 的条件时，上述最大化问题有解，即欺诈型卖方不会模仿诚实型卖方，

---

㊶ 根据 Chapman et al.(2017)，在记录者而非使用者之间充分地去中心化，仍然可能保留区块链在弹性和有效共识方面的优点。

㊷ 考虑一个在真实状态 $\tilde{\omega}$ 下有噪音，但不存在虚假报告（即虚报信息的收益 b 非常小）的信息环境。假设所有的记录者信息对称并且他们能够以 $\theta > 1/2$ 的概率观察到真实的货物交付状态。在一致同意的规则下，$\psi = \theta^K$。类似的，在多数同意的规则下，$\psi = \sum_{k=\left[\frac{K}{2}\right]}^{K} \binom{K}{k} \theta^K (1-\theta)^{K-k}$。

而诚实型卖方选择进入市场并获得正的利润。由此，我们得到如下命题：

**命题 3.1** 当共识的质量足够高，即 $\psi \geqslant \frac{\mu + L}{\mu + 2L}$ 时，使用智能合约有助于诚实型进入者进入市场。

当卖方的生产成本 $\mu = 0$ 时，只要共识的质量能够比现实世界稍微具有一些信息含量（即 $\psi > \frac{1}{2}$），智能合约就有助于诚实型进入者进入市场。

本文在模型中假设有一组连续到达的消费者，这意味着有一组需要被连续验证的交易。如果每一次验证都以独立抽样的方式选取记录者，那么即使在不完美共识的情况下，由于大数定律的成立，也可以保证关于消费者到达的总体情况被显现出来。因此，不完美共识并不影响合谋均衡的实现。总的来说，不完美共识只是略微削弱了市场进入与市场竞争。换句话说，达成完美共识只带来了微弱的福利改善。

正如我们在前文中所说的，减少合谋的关键在于分离卖方和记录者，并减少对卖方的联系程度。为了模型化这一过程，我们假设，对于每一次货物交付，卖方被联系参与信息核查的概率为 $\hat{\zeta}$，则消费者在该期出现但卖方对此毫不知情的条件概率为 $1 - \zeta \equiv (1 - \hat{\zeta})^n$，其中 $n$ 表示交易的次数。值得注意的是，在合谋阶段，卖方违背合谋被发现的概率为 $\zeta$ 而非 1，这就使得惩罚阶段被更少地触发，从而合谋均衡变得更加难以维持。即便如此，如果交易数量很大，违约被发现的概率趋近于 1，均衡也会接近于完美公共监督下的均衡，除非卖方被严格限制充当记录者（$\hat{\zeta} = 0$）。

### 3.3 信息不对称与服务质量的私有信息

在之前的分析中，我们都假设卖方的服务质量为公共信息，在本节中，我们允许卖方的服务质量为私有信息。私有信息下的合谋通常比较复杂（Athey and Bagwell，2001；Miller，2011），因此，我们在本节中仅关注竞争性均衡（以及在合谋惩罚阶段的竞争性阶段博弈）。我们将分析智能合约如何帮助缓解市场进入后配置的无效率，并推导出均衡市场状态下对应的智能合约。

特别地，我们发现，依赖交付状态成功与否设定的智能合约可以将诚实型卖方和欺诈型卖方区分开来。更为一般化地，区块链可以提供关于服务质量 $q$ 的共识。通过假设区块链的分布式共识可以帮助我们在有噪音的信息环境中订

立合同，我们对此进行了建模分析。值得说明的是，当卖方的服务质量为公开信息的时候，该设定并不重要。但是当卖方的服务质量为私有信息的时候，它能够帮助缓解信息不对称。

具体地，我们假设当服务的质量为 $q$ 的时候，商品质量为残次的概率为 $1-q$（买方得到 0 单位的效用），商品质量令人满意的概率为 $q$（买方得到 1 单位的效用）。区块链提供了关于商品质量的信息，该信息可以被用于智能合约。这里“商品残次”或“令人满意”是所有人都潜在同意的事情（而非对商品质量的主观感受）。

在这一拓展的智能合约下，我们现在有三种状态：成功交付并且顾客满意（$s$），成功交付但商品残次（$sd$），交付失败（$f$），对应状态下的卖方报价为 $(p^s, p^{sd}, p^f)$。

### 3.3.1 传统世界中的配置无效率

在没有智能合约的情况下，进入者总会声称他是诚实型卖方，提供高质量的商品（空口白话）。相似地，在位者卖方也不能将他们彼此区分开来。根据之前的逻辑，由于柠檬问题，进入者不会进入市场，并且提供不同商品质量的在位者无法彼此区分。在此情况下，我们有如下引理：

**引理 3.2** 在传统世界中，卖方提出相同的报价 $p_i = \mu$，每个买方（随机地）选择其中一个卖方。在每个时期，买方的期望剩余和社会福利均为 $\mathbb{E}[q_c] - \mu$。

### 3.3.2 在区块链世界中的智能合约均衡

智能合约扩大了卖方的报价空间。一个诚实型进入者可以通过提供 $p^f = 0$ 的报价从而把自己与欺诈型进入者区分开来（欺诈型进入者在该报价下没有模仿动机）。同时，如何选定 $p^f$ 对于在位者并不重要，因为在位者总是会交付货物，即 $p^f$ 发生的概率为 0。我们进一步假设 $p^{sd} \leqslant p^s$，即当顾客收到残次的商品时，他们支付给卖方的价格会更低一些。这一假设是在证券设计文献中常用的标准单调性假设。[43] 商品质量为 $q_i = q$ 的卖方 $i$ 赚得的利润为 $S_q(\mathbb{P}) = qp^s + (1-q)p^f - k$，而每个买方获得的效用为 $B_q(\mathbb{P}) = q(1-p^s) + (1-q)(-p^{sd})$，其中 $1-p^s$ 是消费者从买到满意的商品中获得的净效用（即买到满意商

---

[43] 可参阅 Innes（1990），Hart and Moore（1995），以及 DeMarzo and Duffie（1999）。在买方向卖方询价并且选择最优报价的市场机制下，我们的设定在非正式第一价格拍卖（first-price auction）中有一个自然的重新解释（参见 DeMarzo et al.，2005；Cong，2017）。

品获得的1单位效用减去此时的商品报价 $p^s$ )。

卖方会提供很多不同的智能合约，但是在均衡状态下，只有一类智能合约会存在，如下命题进一步刻画了这类智能合约的特征（回忆 $\Phi$ 是关于 $q$ 的累积分布函数)。

**命题 3.3** 对于每个阶段博弈，存在一个基本唯一的竞争性均衡，在该均衡下，卖方提供的智能合约为 $\mathbb{P}^* = (p, p-1, 0)$。商品质量为 $q_i = q$ 的卖方提供的智能合约为 $(p_q, p_q - 1, 0)$，其中，

$$p_q = 1 - q + \mu + \int_{\underline{q}}^{q} \left[\frac{\Phi(q')}{\Phi(q)}\right]^2 dq' \tag{11}$$

这里，$p_q$ 随 $q$ 递减，买方都选择商品质量最高的卖方。

值得注意的是，高质量的卖方通常倾向于提供更高的产品保证。即使高质量的卖方报一个更低的价格，卖方的期望收益还是会随着他提供的商品质量的提高而变大，这是由于该卖方得到的顾客满意度更高。

在均衡合同 $(p_q, p_q - 1, 0)$ 下，不管最终的消费者是否满意，卖方获得的收益都为 $1 - p_q$。这一竞争性均衡的本质为现金拍卖，该拍卖中有一个商品质量为 $q_i = q$ 的投标者，他对自己的服务有一个 $q - \mu$ 的私人评价，并且报价为 $p_q$。在均衡中，买方选择质量最高的卖方，该卖方在买方到来的每一期获得第二高的评价 $\mathbb{E}[q^{(2)} - \mu]$（收入等价定理)。此时的经济结果与商品质量 $q$ 为公开信息时候的情形完全一样［见式（8）和式（9)］。此时我们有如下推论：

**推论 5.4** 在竞争性均衡中，智能合约可完全解决信息不对称问题，而且社会福利和消费者剩余与卖方质量信息的公开与否相互独立。

也就是说，对智能合约的形式施加限制可能会增加消费者剩余，其方式类似于证券设计对发行者收益的影响。对于关注消费者剩余的监管者来说，应该同时考虑合谋与智能合约的形式，这也是有待未来研究的一个话题。

## 4. 结论

本文发现，区块链等去中心化账本技术有着分布式共识、防篡改、自动执行等特征，该技术扩大了合同订立的空间，促进了智能合约的出现。然而，在达成分布式共识的过程中，该技术还会改变区块链的信息环境，通过促使合谋导致社会福利发生损失。

本文分析了区块链这一根本冲突如何重塑了产业组织和竞争格局，通过加

强市场进入与竞争，区块链可以提高社会福利和消费者剩余，但是该技术同样可能导致更多的合谋行为。总体而言，区块链和智能合约技术下对应的市场均衡有着更为丰富的经济现象。此外，我们还讨论了可以进一步提高消费者剩余的监管和市场措施，如区分共识的信息提供者和共识的使用者等。

本文在简化模型的框架下刻画了区块链的重要特征，分析了在共识生成与信息分发之间的重要权衡。如何订立稳健的共识协议、如何在特定区块链上设计合适的激励机制从而维持共识等问题，虽然超出了本文的讨论范围，但都是未来研究中非常有趣的话题，关于这一话题的探讨需要计算机科学家和经济学家的共同努力。

（中国政法大学　黄健栓　译　中央财经大学助理教授　朱菲菲　译校）

因篇幅所限，本文省略了附录部分，特向作者和读者致歉，需要者可向《比较》编辑室索取：bijiao@ citicpub. com。——编者注

## 参考文献


Abadi，J. ，and M. Brunnermeier. 2018. Blockchain Economics. Working Paper.

Allison，I. 2017. Maersk and IBM Want 10 Million Shipping Containers on the Global Supply Blockchain by Year－End. *International Business Times*，March 8. https：//www. ibtimes. co. uk/maersk－ibm－aim－get－10－millionshipping－containers－onto－global－supply－blockchain－by－year－end－1609778.

Athey，S. ，and K. Bagwell. 2001. Optimal Collusion with Private Information. *RAND Journal of Economics* 32：428－65.

Aune，R. T. ，M. O'Hara，and O. Slama. 2017. Footprints on the Blockchain：Trading and Information Leakage in Distributed Ledgers. *Journal of Trading* 12：5－13.

Baron，D. P. ，and R. B. Myerson. 1982. Regulating a Monopolist with Unknown Costs. *Econometrica* 50：911－30.

Bartoletti，M. ，and L. Pompianu. 2017. An Empirical Analysis of Smart Contracts：Platforms，Applications，and Design Patterns. In *Financial Cryptography and Data Security*，eds. M. Brenner，K. Rohloff，J. Bonneau，A. Miller，P. Y. Ryan，V. Teague，A. Bracciali，M. Sala，F. Pintore，and M. Jakobsson，494－509. Cham，UK：Springer International Publishing.

Bessembinder，H. ，and W. Maxwell. 2008. Markets Transparency and the Corporate Bond Market. *Journal of Economic Perspectives* 22：217－34.

Biais，B. ，C. Bisière，M. Bouvard，and C. Casamatta. 2019. The Blockchain Folk Theorem. *Review of Financial Studies*，32：1662－715.

BlockchainNews. 2017. UPS－Backed Blockchain Consortium Seeks to Disrupt the Freight and

Logistics Industry. CCN, November 17. https://www.ccn.com/bita-looking-disrupt-freight-logistics-industry/.

Bloomfield, R., and M. O'Hara. 1999. Market Transparency: Who Wins and Who Loses? *Review of Financial Studies* 12: 5-35.

Böhme, R., N. Christin, B. Edelman, and T. Moore. 2015. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives* 29: 213-38.

Bourveau, T., G. She, and A. Zaldokas. 2017. Naughty Firms, Noisy Disclosure. Working Paper.

Buterin, V. 2014. Ethereum: A Next-generation Smart Contract and Decentralized Application Platform. White Paper.

Cao, S., L. W. Cong, and B. Yang. 2018. Auditing and Blockchains: Pricing, Misstatements, and Regulation. Working Paper.

Cao, S., L. W. Cong, M. Han, Q. Hou, and B. Yang. 2019. Blockchain Architecture for Auditing Automation and Trust-building in Public Markets. *IEEE Computer*. Accepted.

Chapman, J., R. Garratt, S. Hendry, A. McCormack, and W. McMahon. 2017. Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet? Working Paper.

Chen, L., L. W. Cong, and Y. Xiao 2019. A Brief Introduction to Blockchain Economics. Information to Facilitate Efficient Decision Making: Big Data, Blockchain and Relevance, edited by Kashi Balachandran, World Scientific Publishers, Forthcoming.

Chiu, J., and T. Koeppl. 2019. Blockchain-based Settlement for Asset Trading. *Review of Financial Studies* 32: 1716-53.

Cong, L. W. 2017. Auctions of Real Options. Working Paper.

Cong, L. W., Z. He, and J. Li. 2020. Decentralized Mining in Centralized pools. Forthcoming, *Review of Financial Studies*.

Cong, L. W., Y. Li, and N. Wang. 2018b. Tokenomics: Dynamic Adoption and Valuation. Working Paper.

Cong, L. W., Y. Li, and N. Wang. 2018c. Token-based Platform Finance. Working Paper.

Cong, L. W., B. Li, and T. Zhang. 2019. Alternative Data in FinTech and Business Intelligence. *Handbook of FinTech and Blockchain*, edited by Maurizio Pompella and Roman Matousek, Palgrave MacMillan. Book chapter under review.

de Vilaca Burgos, A., J. D. de Oliveira Filho, M. V. C. Suares, and R. S. de Almeida. 2017. Distributed Ledger Technical Research in Central Bank of Brazil. Working Paper.

DeMarzo, P., and D. Duffie. 1999. A Liquidity-Based Model of Security Design. *Econometrica* 67: 65-99.

DeMarzo, P., I. Kremer, and A. Skrzypacz. 2005. Bidding with Securities: Auctions and Security Design. *American Economic Review* 95: 936-59.

Easley, D., M. O'Hara, and S. Basu. 2017. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. Working Paper.

The Economist. 2015. The Trust Machine. October 31, https://www.economist.com/leaders/2015/10/31/the-trust-machine.

The Economist. 2017. A Yen for Plastic. November 4.

Eyal, I., and E. G. Sirer. 2014. Majority is not Enough: Bitcoin Mining is Vulnerable. In International Conference on Financial Cryptography and Data Security, 436 – 54. New York: Springer.

Fudenberg, D., and E. Maskin. 1986. The Folk Theorem in Repeated Games with Discounting or with Incomplete Information. *Econometrica* 54: 533 – 54.

Fung, B. 2014. Marc Andreessen: In 20 years, Well Talk about Bitcoin Like We Talk about the Internet Today. *Washington Post*, May 21.

Gillis, M., and A. Trusca. 2017. 'Not There Yet': Bank of Canada Experiments with Blockchain Wholesale Payment System. *CyberLex*, June 19.

Goldstein, M. A., E. S. Hotchkiss, and E. R. Sirri. 2006. Transparency and Liquidity: A Controlled Experiment on Corporate Bonds. *Review of Financial Studies* 20: 235 – 73.

Green, E. J., and R. H. Porter. 1984. Noncooperative Collusion under Imperfect Price Information. *Econometrica* 56: 87 – 100.

Haber, S., and W. S. Stornetta. 1990. How to Time-stamp a Digital Document. In Conference on the Theory and Application of Cryptography, 437 – 55. New York: Springer.

Hackett, R. 2017. Maersk and Microsoft Tested a Blockchain for Shipping Insurance. *Fortune Finance*, Sept 5. http://fortune.com/2017/09/05/maersk-blockchain-insurance/.

Hart, O. 1995. Firms, *Contracts, and Financial Structure*. London: Clarendon Press.

Hart, O., and J. Moore. 1988. Incomplete Contracts and Renegotiation. *Econometrica* 56: 755 – 85.

Hart, O., and J. Moore. 1995. Debt and Seniority: An Analysis of the Role of Hard Claims in Constraining Management. *American Economic Review* 85: 567 – 85.

Harvey, C. R. 2016. Cryptofinance. Working Paper.

Haswell, H. 2018. Maersk and IBM Introduce TradeLens Blockchain Shipping Solution. IBM News Room, August 9. https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution.

Higgins, S. 2017a. IBM Unveils Blockchain Platform for Oil Trade Finance. Coindesk, March 28. http://www.coindesk.com/ibm-blockchain-platform-oil-trade-finance/.

Higgins, S. 2017b. Walmart, JD.com Back Blockchain Food Tracking Effort in China. CoinDesk, December 14. https://www.coindesk.com/walmart-jd-com-back-blockchain-food-tracking-effort-china.

Huberman, G., J. D. Leshno, and C. C. Moallemi. 2017. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. Working Paper.

Innes, R. D. 1990. Limited Liability and Incentive Contracting with Ex – ante Action Choices. *Journal of Economic Theory* 52: 45 – 67.

Jeffries, A. 2018. Blockchain is Meaningless. Verge, March 7. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

Kaminska, I. 2015. Exposing the 'If We Call It a Blockchain, Perhaps It Won't Be Deemed a Cartel?' Tactic. *Financial Times*, May 11. https://hackernoon.com/ten-years-in-nobody-has-come-upwith-a-use-case-for-blockchain-ee98c180100.

Khapko, M., and M. Zoican. 2018. How Fast Should Trades Settle. Working Paper.

Krishna, V. 2009. *Auction Theory*. Hoboken, NJ: Academic Press.

Kroll, J. A., I. C. Davey, and E. W. Felten. 2013. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In Proceedings of WEIS, Vol. 2013.

Lauslahti, K., J. Mattila, T. Seppälä, et al. 2016. Smart Contracts – How will Blockchain Technology Affect Contractual Practices? Technical Report, The Research Institute of the Finnish Economy.

Malinova, K., and A. Park. 2018. Market Design for Trading with Blockchain Technology. Working Paper.

Miller, D. A. 2011. Robust Collusion with Private Information. *Review of Economic Studies* 79: 778 – 811.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Working Paper.

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies*. Princeton, NJ: Princeton University Press.

Narayanan, A., and J. Clark. 2017. Bitcoin's Academic Pedigree. Communications of the ACM 60: 36 – 45.

Nayak, K., S. Kumar, A. Miller, and E. Shi. 2016. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. In Security and Privacy (EuroS&P), 2016 IEEE European Symposium, 305 – 20. Piscataway, NJ: IEEE.

Palmer, D. 2018. R3 Pilots Blockchain Trade Finance Platform with Global Banks. Coindesk, February 21. https://www.coindesk.com/r3-pilots-blockchain-trade-finance-platform-with-global-banks/.

Porter, R. H. 1983. Optimal Cartel Trigger Price Strategies. *Journal of Economic Theory* 29: 313 – 38.

Shin, L. 2017. Why Nasdaq is Even More Optimistic about Blockchain Than It Was 3 Years Ago. Forbes, Feb 21.

Stinchcombe, K. 2017. Ten Years in, Nobody Has Come up with a Use for blockchain. Hackernoon, December 22. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100.

Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks. First Monday 2.

Szabo, N. 1998. Secure Property Titles with Owner Authority. Online at http://szabo.best.vwh.net/securetitle.html.

Tapscott, D., and A. Tapscott. 2016. *Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin.

Taylor, C. 2016. Ornua Involved in Groundbreaking Blockchain Transaction. Irish Times, September 7. https://www.irishtimes.com/business/technology/ornua-involved-in-groundbreaking-blockchain-transaction-1.2782748.

Terekhova, M. 2017. Credit Suisse – led Blockchain Solution Makes Progress. Business Insider, August 23. https://www.businessinsider.com/credit-suisse-led-blockchain-solution-makes-progress-2017-8.

Tinn, K. 2018. Blockchain and the Future of Optimal Financing Contracts. Working Paper.

Tirole, J. 1988. *The Theory of Industrial Organization*. Cambridge: MIT Press.

Tirole, J. 1999. Incomplete Contracts: Where Do We Stand? *Econometrica* 67: 741 – 81.

Turing, A. M. 1937. On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society 2: 230 – 65.

Weiss, M., and E. Corsi. 2017. Bitfury: Blockchain for Government. HBS Case Study January 12: 818 – 031.

Yermack, D. 2017. Corporate Governance and Blockchains. *Review of Finance* 21: 7 – 31.

Zurrer, R. 2017. Keepers—Workers that Maintain Blockchain Networks. Medium, August 5. https: //medium. com/rzurrer/keepers – workers – that – maintain – blockchain – networks – a40182615b66.