区块链的边界*

郭迅华

guoxh@tsinghua.edu.cn

2018-08-27

那台陈旧的台式电脑开足马力运转了三天三夜，挖出了我最初的一点比特币。我被这无政府主义者的奇思妙想所激起的强烈好奇心得到了满足，同时也无法再忍受呼呼作响的电脑风扇带动机箱震动所发出的巨大噪音，于是我关闭了挖矿程序。那时的我完全没有意识到，生平最大的一次发财致富的机会，就这样与我擦肩而过了。

数年之后，比特币以波澜壮阔的涨跌吸引了全世界的目光。其身后的区块链技术随即走上前台，成为众所追捧的热点。许多人将区块链视为继互联网之后的新一轮革命，宣称其将冲击和重塑各行各业。在诸多的媒体文章中，区块链被描绘为一种快速、安全、跨平台、低成本的交易环境，干净而彻底地解决了交易中的信任问题，从而为各种经济活动提供了一个高度可信赖的“价值网络”，在此基础上给经济社会各个领域带来颠覆性的创新。

在我看来，区块链技术无疑具有其独特的魅力。然而，技术本身并不具有颠覆性，真正具有颠覆性的，是人们运用技术的方式。比特币所追求的不受任何个体控制的“对等”（peer-to-peer）货币系统，具有其颠覆性色彩。而区块链技术只是为对等货币系统这一颠覆性的理念，提供了可能的实现手段。除了货币之外的其他领域是否能够利用区块链技术实现颠覆性的创新，则取决于领域的具体特征，以及区块链的技术特性与这些特征之间的契合度。换言之，区块链并非是一种普遍性的革新方案，其影响力的范围，受限于其自身的技术性质和领域的具体需求。

*本文发表于《清华管理评论》2018 年第 11 期。

本质上说来，区块链的技术目标，是创造一种开放、对等的信息环境，使得参与者之间可以直接交易，无需依赖于中介平台。在传统的中心化信息环境中，交易需要通过中介平台来完成。例如支付交易需要银行或支付宝之类的支付中介，购物交易需要淘宝之类的买卖平台。之所以需要摆脱中介平台，是因为中介平台可能是不可靠的。交易者为了实现交易，必须信任中介平台。一旦中介平台出现问题（不论是技术故障、人为错误还是欺诈），交易者就会蒙受损失。这种由于中介平台的可靠性问题所带来的可能的损失，可以称作“信任风险”。在区块链环境中，由于中介平台不复存在，这种对于中介平台的信任风险，也就可以被消除。

但是，需要指出的是，区块链所消除的，仅仅是交易者对于中介平台的信任风险，而绝不是像许多人所认为的那样，可以大幅度地降低“信任成本”，甚至是完全解决交易中的信任问题。首先，区块链只能消除交易者对于中介平台的信任风险，而不能消除交易者相互之间的信任风险。其次，区块链通过在交易环境中去除中介平台来消除信任风险，即通过“去中介化”来实现“去信任化”。而以这种方式实现“去信任化”，必然需要付出额外的成本。在许多情形下，这种成本可能是十分巨大的。

从这种意义上说来，“去信任化”所需要付出的成本与信任风险之间的大小对比，决定了区块链应用的边界。在这样的边界条件下，至少在很长的一段时间内，区块链应用的范围是十分有限的。在社会经济各个领域实现这种开放、对等的信息环境，即便是一种未来的方向，也还需要漫长的历史进程。

区块链：不可篡改的账簿

区块链源于比特币。比特币的目标，在于建立一套开放、对等的货币系统。从信息技术的角度看来，货币存在于交易之中，货币系统的实质是交易的记录，也就是账簿。一个可靠的货币系统，必须确保其交易账簿是不可篡改的。在以往的一切体系中，交易账簿由特定的人或机构维护。账簿的维护者具有修改账簿的能力，以其自身的信用和外部的监管担保账簿不被篡改。在网络环境中，中介平台就是账簿的维护者。区块链技术为比特币提供了一个开放、对等的账簿，不依赖于特定的维护者。为了确保交易能够被准确

记录且账簿不可被篡改，区块链需要有大量的参与者，并且依赖于两个关键性的机制：对等分布式存储和基于投票的共识。

所谓对等（peer-to-peer）分布式存储机制，就是将整个交易账簿完整地保存在每一个参与者的计算机上。所有参与者所保存的交易账簿都是完全相同的。每一笔交易，不论其发生在哪两个交易者之间，都会被广播给所有的参与者，从而被记录在每一个参与者的账簿上。在这样的情形下，中心化的账簿维护者不复存在，每一个参与者都是账簿的维护者。这样的账簿是开放的，每一个参与者都可以随时查阅账簿的内容；这样的账簿也是对等的，每一个参与者都拥有与其他人完全相同的信息。

对等分布式存储的一个潜在问题，在于不同的参与者所保存的账簿可能出现不一致。一方面，网络传输的延迟和中断，可能会使得不同的参与者接收到不同的交易信息；另一方面，试图进行欺诈的攻击者可能有意地发送虚假的或是篡改过的信息。这些情况都会导致区块链网络中一部分参与者所保存的账簿内容与其他人不一致。为了消除这种不一致现象，区块链使用了基于投票的共识机制，通过参与者的投票来决定哪一份账簿内容应该被接受。投票中胜出的账簿被所有参与者所保存，失败的则被舍弃。比特币区块链采用了一种被称为“工作量证明”（proof-of-work，PoW）的方式来实现账簿共识。“工作量证明”本质上是一种基于计算能力的投票，参与者的计算机通过计算繁琐的数学题来证明自己的计算能力，获得最多计算能力支持的账簿在投票中胜出。

在拥有大量独立参与者的条件下，对等分布式存储和基于投票的共识机制保证了区块链账簿的不可篡改性，使得网络中的任何单独的参与者，都无法对账簿进行随意的修改。任何单独的参与者的账簿出现错误或是丢失，都不会影响整个体系的可靠性。换句话说，区块链账簿的不可篡改性依赖于三个要素：一是大量的独立参与者，二是对等存储，三是基于投票的共识。削弱其中的任何一个要素，区块链账簿体系的可靠性都会被弱化。

“去信任化”及其代价

作为一种账簿系统，区块链的核心特征，是不再有中心化的账簿维护者。账簿保存在所有的参与者手中，攻击者对区块链账簿的恶意修改，会在

投票机制中被否决。从而，交易的参与者不再面临对账簿维护者的信任风险，通过“去中介化”实现了“去信任化”。

但是，如果据此认为区块链大幅度地降低了交易成本，甚至是干净彻底地解决了交易中的信任问题，则是谬以千里了。区块链仅仅是消除了交易者对于中介平台的信任风险。其对于解决交易者之间的相互信任问题，则并没有实质性的作用。举例说来，一个基于区块链的二手车交易市场，能够摆脱对中心化的在线交易平台的依赖，从而，平台的可靠性问题不会再对交易造成风险。区块链可以确保卖家发布在市场上的信息是由卖家自己发布的，且没有被篡改过，同时也可以确保在该市场中所进行的交易被忠实地记录下来，并且不会再被更改。然而，区块链却无法确保卖家所发布的信息是真实准确的，无法核实卖家对车况的描述是否与实物相符。要实现交易，买家必须信任卖家。这种信任当然会存在风险，而这样的风险并不能被区块链所消除。也许有人会争辩说，如果一辆汽车从出厂开始的所有交易、使用和维修信息都被记录在区块链中，那么当这辆汽车被出售时，卖家就可以轻而易举地全面准确掌握车辆的真实状况了。然而，我们如何保证生产商、销售商、用户、维修厂全都主动、及时、准确的把每一个环节的信息提交给区块链呢？区块链能够忠实地记录参与者提交给它的信息，但并不能主动采集信息，更不能确保信息与实物相匹配。要确保卖家所发布信息的真实性和准确性，其关键性的挑战在于实时可靠的信息采集技术和严格的制度规范，这些都不是区块链所能够解决的问题。恰恰相反，与区块链相比，中心化的在线交易平台反而更具备主动采集并核实信息的能力和动力。从这种意义上说来，一个高度可靠的中介平台，能够有效地降低交易者之间的信任风险，这样的作用是区块链所难以具备的。

更值得注意的是，区块链以“去信任化”的方式来消除交易者对于中介平台的信任风险，其代价可能是巨大的。信任风险存在的原因，在于中介平台可能是不可靠的。区块链并不是通过提高中介平台的可靠性来降低信任风险，而是完全取消了中介平台。在区块链中，每个参与者都是账簿的维护者，且每个参与者都有可能试图篡改账簿。是大量独立参与者、对等分布式存储、基于投票的共识这三个关键要素，确保了那些篡改账簿的企图能够被有效地阻止。从这种意义上说来，区块链的一个基本假设是，每个参与者个体都是不可信任的。区块链实际上是一种“无信任”的环境。

在这种“无信任”的环境中，每个人都可能是坏人。要阻止坏人干坏事，只能依靠群体机制（对等分布式存储和基于投票的共识），并且这个群体要足够大。在“无信任”环境这种“最差情况”基础上建立群体机制，必然是需要付出成本的。这种成本可以被称作“去信任化成本”。在讨论区块链是否能降低交易成本时，“去信任化成本”不应该被忽视。在当前的区块链体系中，“去信任化成本”包括多个方面。

首先，对等分布式存储需要耗费大量的存储空间和网络流量。以比特币为例，到 2018 年初，一份完整的比特币账簿所占用的存储空间已经超过了 150GB，且以每年数十 GB 的速度增长。全球数百万比特币用户的每一台计算机上，都需要保存这一巨大账簿的完整拷贝。此等规模的账簿仅仅是承载了比特币每年 3000 万笔左右的交易量。对于一个交易支付系统而言，这样的交易量其实是微不足道的。相比之下，支付宝在 2017 年双 11 一天的交易量，就达到了 14.8 亿笔[1]。如果比特币交易量快速增加，那么其账簿体量很快就会超出普通用户计算机的存储能力。为了解决这一问题，新的比特币客户端软件允许用户只保存账簿的摘要信息，而不保存完整的账簿。然而，如果大量参与者都不保存完整的账簿，那么对等存储分布式机制就会被大幅削弱，区块链体系的可靠性，也就会被严重地降低。

其次，基于投票的共识机制需要耗费大量时间和计算资源，并制约交易确认的速度。仍以比特币为例，每一笔交易都需要被打包到区块当中，每一个区块都需要经过“工作量证明”（PoW）投票才能得到确认，因而区块生成的速度严重限制了交易确认的速度，使得整个比特币网络只能支持每秒 3-7 笔的交易确认速度，这与支付宝每秒数千笔的交易速度相比，存在着天壤之别。尽管后来的技术改进（如以太坊等）可以通过提升区块的规模上限、加快区块的生成速度等手段提升交易确认速度，但只要仍采用 PoW 这类基于计算能力的投票机制，那么为了保证该机制的有效性，必然需要足够的时间来完成投票过程。另一方面，PoW 投票机制耗费了巨大的计算资源。据估计，在当前的规模下，比特币网络的 PoW 运算每年大约需要消耗 730 亿度电，占全球总耗电量的 0.33%，相当于 670 万个美国普通家庭的用电总量，超过数十个国家全国的用电总量[2]。为了克服这些问题，新

[1] http://tech.sina.com.cn/roll/2017-11-12/doc-ifynsait7423134.shtml

[2] Digiconomist, “Bitcoin Energy Consumption Index,” https://digiconomist.net/

的区块链设计引入了“股权证明”（Proof-of-Stake，PoS）和“授权股权证明”（Delegated Proof-of-Stake，DPoS）等机制来取代 PoW。然而，放弃了基于计算机能力的 PoW 投票机制，参与投票的用户计算机就不再具有对等性，拥有更多股权的少量用户在投票中能够具备更强的话语权，从而严重削弱区块链的去中心化属性，降低区块链体系的可靠性。

第三，无中心的结构使得区块链系统难以修改升级。区块链的账簿通过对等存储和投票机制来维护，因而对账簿规则的任何修改，也只能通过投票机制来实现。仍以比特币为例。在运行了一段时间、影响力急剧扩大之后，比特币最初设计形式中的两个缺陷迅速暴露出来。第一个缺陷是区块大小上限设置过低（1MB），且区块生成速度设定过慢（每 10 分钟一个区块），这导致了比特币的交易确认速度缓慢（每秒 3.3-7 笔）。区块大小上限和区块生成速度其实只是账簿结构中的两个参数，在最初的比特币软件实现过程中被人为地设定，所有的参与者计算机都采用了这两个参数值。只要能够调整这两个参数，交易确认的速度就能得到提升。然而，由于区块链系统的无中心结构，这两个参数难以被改变。在少量的参与者计算机中修改这两个参数，只能导致这些修改后的计算机所生成的账簿区块在投票中被否决。只有在超过 50% 的参与者计算机中修改了这两个参数，新的参数值才能够在投票中胜出。这种软件更新的过程被称为“分叉”（fork），其实现往往是极为艰难的。比特币最初设计形式中的第二个重要缺陷，是对比特币的总量设置了一个上限（大约 2100 万）。这一上限设置导致了比特币具有通缩属性。通缩属性使得人们对比特币产生升值预期，从而倾向于持有而非使用比特币。这一致命的缺陷决定了比特币不可能成为一种真正的流通货币（在我看来，比特币已成为一种收藏品和投资品，其作为一种流通货币的实践已经失败）。与区块大小、区块生成速度相似，总量上限同样只是比特币系统中人为设置的一个参数。但这一参数无法通过软件的修改升级来进行调整。改变或取消总量上限的唯一途径，是放弃比特币，重新设计并推广新的网络货币系统。这样的问题绝不仅在比特币中存在。从一般意义上说来，只要是具备大规模用户群体和完整的投票共识机制的区块链系统，都会面临部署后难以修改调整、难以升级的困境。

第四，“无信任”的环境取消了中介平台，导致一些原本可以由中介平

bitcoin-energy-consumption.

台提供的交易服务无法得到实现。在上文所讨论的二手车交易市场的例子中，如果存在中介平台，则该中介平台可以负责对卖家所发布的车辆信息进行评估和核实。在取消了中介平台的区块链市场中，买家只能自行考察车辆状况。对于大多数缺乏足够专业知识的买家而言，这一方式无疑是高成本的。这种服务的缺失，实质上增加了买家和卖家之间的信任风险，增加了交易成本。

由此可见，“去信任化成本”可能是十分巨大的。在讨论区块链是否能降低交易成本时，“无信任成本”是不容忽视的。

边界：信任风险 vs. 去信任化成本

信任能够降低交易成本，同时也带来风险。如果信任所产生的收益（交易成本的降低）高于其所带来的风险，人们就会选择信任。我们选择信任银行、信任支付宝、信任微信钱包，因为信任这些机构可以帮助我们更快捷地实现支付交易、大幅度地降低交易成本。尽管这种信任存在着风险（银行可能会出错，支付宝可能会停机，微信钱包可能会被篡改），但因为风险低于收益，所以我们仍然会选择信任。今天，当一名快递员把包裹交到顾客手中时，他很可能不会要求顾客签字确认，而是随即转身离开。快递员选择信任顾客，因为这种信任能够为他节约时间，降低成本。尽管这种信任存在风险（顾客可能会赖账），但因为风险低于收益，所以他仍然会选择信任。以这样的形式，信任创造价值。

从这种意义上说来，区块链放弃了信任的价值，建立在不信任中介平台的基础上。区块链中的交易不依赖于对中介平台的信任，从而消除了信任风险，但也相应不可避免地带来交易成本的上升。

当“去信任化成本”小于“信任风险”时，区块链应用具有业务价值；反之，在“信任风险”小于“去信任化成本”的情境中，区块链并不适合。“去信任化成本”与“信任风险”之间的大小对比，决定了区块链应用价值的边界。

技术的发展可能会降低区块链的“去信任化成本”，例如缩小账簿数据存储量，提高交易确认速度，减少计算资源的耗费，提高区块链网络体系的可调整性等。但同时，技术的发展同样也可能以多种不同的形式降低中心

化体系的信任风险，例如提高中介平台的数据透明性等。从而，“去信任化成本”与“信任风险”之间的力量对比会随着时间的发展而动态地变化。但在可以预见的未来，区块链的适用场合始终是有限的。在那些“信任风险”显著低于“去信任化成本”的领域中，刻意地追求区块链的应用，恐怕不是一种明智的选择。

对于银行、电商平台等中介机构而言，区块链无助于强化其地位和作用。区块链是对现有交易体系的否定，而非发展。只要能够控制和降低信任风险，中心化体系的效率优势，是区块链所难以企及的。

结束语

区块链所追求的开放、对等的信息环境，的确与现有的中心化体系有着本质的不同。但区块链并不总是能有效地降低总交易成本。只有在信任风险高于去信任化成本的情境下，区块链才能有真正的用武之地。

近年来的区块链热潮，既有业务应用的积极探索，也不乏建立在似是而非的概念标签上的资本游戏。概念炒作和资本游戏在不远的将来即会退潮，业务应用仍需漫长的探索。推动区块链业务应用实质性发展的动力，主要将来自于产业及社会信息环境的建设者和管理者，而不会是中心化的交易机构，也不会是追逐商业利益的创业企业。

许多人将区块链与 TCP/IP 网络相类比。在我看来，区块链所致力于创造的新型信息环境组织形态，其作用和影响，更类似于上世纪八九十年代兴起的开源软件运动。开源软件经过三十余年的发展，重新定义了软件的价值，重塑了软件行业的生产形式，其思想理念辐射渗透诸多领域，催生了大量改变世界的创新。区块链或许也具有同样深厚的潜在影响力，但很可能需要经过同样漫长的演化渗透，才能够真正地开花结果。