

· 专题一:区块链技术及应用 ·

## 区块链技术的应用前景与挑战:基于信息保真的视角

高杰<sup>1\*</sup> 霍红<sup>2</sup> 张晓庆<sup>1</sup>

(1. 西安交通大学 管理学院,西安 710049;2. 国家自然科学基金委员会 管理科学部,北京 100085)

[摘要] 本文从发布保真、传播保真、更新保真三方面讨论了信息保真的概念,分析传统互联网技术在信息保真方面所面临的困境。结合比特币的发展,总结了区块链技术相对于传统互联网在数据写入机制、数据存储机制、历史数据维护机制三方面的特点,分析认为区块链可以实现传播保真和一定程度的发布保真,在比特币场景下区块链可以实现更新保真,但在一般使用场景下区块链难以实现更新保真。归纳了目前产业应用区块链技术的实践,结合对区块链技术特点的分析,识别了区块链技术产业应用所面临的机会与挑战。最后,提出区块链技术的发展与应用仍需解决的三大问题:提升区块链交易处理速度、物联网与区块链技术相结合以及区块链管理机制的设计。随着区块链技术以及相关配套技术的发展,区块链技术一定可以得到广泛的应用,并深刻影响和改变人们在互联网上的行为模式和企业之间的合作模式。

[关键词] 区块链;信息保真;比特币;机制设计

DOI:10.16262/j.cnki.1000-8217.20200313.017

### 1 互联网的困境与信息保真

在前互联网时代,由于物理空间的限制,人与人之间连接的成本较高,连接的强度较低。互联网的出现降低了节点间的连接成本,增强了节点间的连接频率与强度,缩短了节点间的“距离”,把世界变成了一个“小世界”。节点之间通过信息交流,深化了分工协作,促进了融合创新,提高了生产和创新的效率,创造出更高的价值。梅特卡夫定律(Metcalfe's Law)指出,一个网络的价值与该网络中活跃节点数量的平方成正比<sup>[1,2]</sup>。在梅特卡夫定律的支配下,互联网呈现出极强的规模经济性,每个网络都会努力扩张自己的规模,从而形成了自然垄断<sup>[3]</sup>。而网络扩张的赋能者,即平台提供商,往往处于垄断地位,并能获得巨大的超额利润。在互联网时代,涌现出了一大批成功的平台型商业模式,例如:脸书、微信、微博、抖音等社交网络平台,亚马逊、阿里巴巴、京东、拼多多、滴滴、爱彼迎、美团等电子商务平台。就社交网络平台而言,在空间维度上,用户越多,平台所提供的连接服务对单个用户的效用越大,吸引力



高杰 西安交通大学管理学院工业工程系教授。2001、2007年在西安交通大学获学士、博士学位。2004—2006年在早稻田大学留学,2012—2013在美国 Santa Clara 大学访问。研究领域包括供应链管理、共享经济、服务转型战略。主持国家自然科学基金项目3项,获陕西省科技进步二等奖3项。2012年被评为教育部新世纪优秀人才。曾为陕重汽、陕鼓动力、中国石化、Intel 成都公司等企业管理咨询,在国际期刊发表SCI论文20余篇,SCI被引700余次。

越强,即存在网络外部性(Network Externality)<sup>[4]</sup>;在时间维度上,用户一旦适应了某个社交平台,迁移到另一平台的成本就会较高,即用户黏性大。此外,平台所提供的连接服务,作为一种信息产品,前期的设计、开发等固定成本较高,后期的系统维护等边际成本非常低。因此,社交网络平台具有非常强的规模经济性,呈现出“大鱼吃小鱼”和“赢者通吃”的特点,竞争中的胜出者则可以凭用户数量优势和垄断地位通过广告、用户引流、数据分析等业务盈利。电商平台则分别针对卖家和买家两类用户提供两种具有互补性的信息服务,面临双边市场(Two-sided

收稿日期:2020-01-07;修回日期:2020-02-18

\* 通信作者,Email: gaoj@mail.xjtu.edu.cn

Market)<sup>[5]</sup>。虽然单个卖家或买家市场内部不存在网络外部性效应,但卖家与买家双侧间存在网络外部性。卖家越多,买家越愿意使用该平台购物;而买家越多,卖家也愿意通过该平台售卖产品,因此也容易形成自然垄断。电子商务平台一般通过服务费、佣金的形式获取收益<sup>[6]</sup>。

传统互联网虽然能够经济、高效地传递信息,但由于存在技术和治理机制等方面的缺陷,并不能保证信息的真实性。信息保真包括三个方面,(1)发布保真:发布者所发布的信息与所描述的客体状态相符;(2)传播保真:信息在传播过程中不能被轻易篡改或模仿;(3)更新保真:信息能够随客体状态的动态变化而实时更新。只有在满足信息保真性的前提下,才能实现交互节点间的深度信任,也只有基于深度信任才能够实现节点间的深度互动,带来价值增值,例如:新交易机会的发现、新生产分工的形成以及新商业模式的诞生。本文尝试从信息保真的视角,探讨区块链对互联网的改进,以及区块链应用的前景和挑战。

传统互联网既能传递真实信息,也能散布谎言,社会上的不实信息与诈骗行为并没有随着互联网的普及而减少。首先,信息的发布方可以轻易发表与事实不符的信息。这一点在社交媒体上最为明显,“假新闻”在社交媒体上的泛滥影响了人们对事实的判断,扰乱了社会秩序<sup>[7]</sup>。其次,信息在传播过程中很容易被篡改和模仿。即便在发布保真的条件下,信息传播过程的扭曲也会干扰事实的传播,降低互动双方的信任。互联网上,网络数据维护方主动篡改或被黑客非法篡改的案件时有发生。最后,在互联网上流传的信息也可能由于无法及时更新、无法反映事物的变化而失去价值。例如,人们无法根据某人几年前留在社交媒体上的状态信息判断此人的职业、收入和家庭状况。即使这些信息在发布的时候和发布后的传播过程中都是准确的,如果这些信息没有随着其个体实际状态的动态变化而及时更新,它们将逐渐失去价值。

如果互联网无法实现信息的保真性,会导致虚假信息的泛滥以及信息提供者与接收者之间的信息不对称,并形成“柠檬市场”<sup>[8,9]</sup>。在“柠檬市场”上,高质量的产品和服务提供商无法将自己与低质量的竞争者区分开,从而无法获得差异化优势和质量溢价,并最终离开市场,这样市场上只会留下低质量的提供商。“柠檬市场”损害了互动双方的信任,阻碍了市场分工深化。因此,当前互联网上流行的商业

模式以社交、游戏和浅交易(电商)为主,这些商业模式主要依赖信息的即时有效性,而不强调信息的历史有效性和动态更新性。然而,这类商业模式伴随着互联网人群的饱和正在逐渐从蓝海走向红海。新的商业机会则蕴藏于互联网对各产业在创新、生产、交易、融资等环节的深度改造,这意味着互联网上个体之间的合作更加深化,并对信息交换、储存与更新环节提出了更高的经济性、时效性与保真性要求。

在需要信息保真的商业模式中,传统的互联网也会努力实现一定程度的信息保真。一般而言,负责维护重要信息的数据库的中心节点(平台企业),为了维护企业信誉及遵守法律法规,会建立一套信息认证与监管体系,实现信息的保真性。例如,在电商领域,阿里巴巴会负责维护商品信息、交易记录和用户账户余额的数据库,并且为这些服务收取一定的费用。但是,由单一机构维护的中心化数据存储系统正在面临深刻的信任危机。在数据维护方与用户利益不一致的情况下,数据维护方作为代理人有强烈的动机背弃委托人(用户)的利益,这就导致了道德风险问题。数据维护方本身可能会篡改数据获利,例如:在按点击量付费的网络广告中,广告商可能改大点击次数,而在按照播放次数向创作者付费的流媒体平台上,平台商可能改小播放次数。此外,数据维护方也可能由于对信息安全的投入不足,造成数据被第三方(例如:黑客)篡改或破坏,此类案件在大数据环境下屡见不鲜。

## 2 区块链对互联网信息保真能力的改进:以比特币为例

比特币是一套去中心化的数字货币发行与支付系统<sup>[10]</sup>。在发行方面,任何人都可以下载并运行开源的比特币软件,成为节点,通过相互竞争的方式获取创建区块的权利,并获得该区块中所包含的比特币。这个竞争的过程需要耗费大量的算力(反复运行散列算法),找一个最小的散列值,类似黄金的采掘过程,被称为挖矿。比特币生成算法会动态调整算法的复杂度,已经产生的比特币越多,参与挖矿的人数越多,算法就越复杂,挖矿的难度越高。比特币的发行机制保证了其稀缺性,不会发生通货膨胀,因此也被称为“数字黄金”。在存储与支付过程中,比特币利用区块链技术,实现了高度的信息保真,实现了各节点间的信任。区块链是将分布式数据存储、点对点传输、共识机制和加密算法等计算机技术结合起来,形成的一种去中心化的数据存储系统<sup>[11]</sup>。

它与传统的中心化数据库的差异可以归纳为以下几点:

(1) 数据写入机制不同。中心化数据库在写入之前通常不对数据的真实性进行验证,或者仅通过中心化节点进行验证。在区块链上,数据要经过多个验证节点的共同验证,经过某种共识算法对该项数据的真实性形成共识之后,才能写入区块链。在验证节点具备足够可信性和验证节点之间不会合谋取利的前提下,区块链的写入机制能实现信息的发布保真。由于各节点的验证和共识需要消耗相当的算力和时间,区块链为实现发布保真需要付出一定算力和时间代价。

(2) 数据存储方式不同。中心化数据库由单一的节点负责数据的存储和维护,而区块链上的数据存储是由多个节点各自维护一份拷贝,任何被认可的数据操作都会被实时同步至所有具备存储权限的节点上。任何单一节点的数据丢失、篡改都会被其他节点上的数据自动修正,只有当多数的节点同时发生了数据的一致性篡改,才能改变整个区块链系统中的数据。

(3) 数据存储格式与历史数据修改难度不同。在中心化数据库上,中心节点可以不经网络上其他节点的授权任意编辑和修改任一部分的历史数据。为了加大篡改数据的难度,区块链采用链式数据存储格式,相关的加密算法保证了无法局部地修改数据,任何历史数据的修改都必须同时修改该条数据以后的所有数据,这在分布式存储的情况下几乎是不可能完成的任务。因此,一项被验证为真实的数据被写入区块链系统之后将几乎不能被任何节点篡改,这实现了数据的传播保真。

在数字化货币系统中,信息需要即时反映客体状态的变化,信息更新的延迟可能会引起严重的经济纠纷,例如欺诈问题。每次信息更新都意味着信息的再次发布。因此,为了在通用场景下实现信息的更新保真,区块链上的各验证节点需要针对每次更新后的状态,消耗相当的时间与算力重新验证信息的真实性并形成共识。在信息更新频率较高或对实时性要求较高的情境中,区块链技术难以完美解决信息的更新保真问题。比特币是一个封闭系统,系统内数据(即账户上的比特币数量)不需要与系统外客体进行交互,不需要验证外部客体状态与区块链上数据的一致性,只需保证系统内交易的真实性就可以实现信息的更新保真。因此,在比特币这一特定应用场景下,区块链完美解决了货币信息的保

真问题。在比特币系统中,新成员和老成员享有相同的信息,不存在任何的信息不对称,并由此建立了去中心化的信任体系。

通过区块链技术,比特币实现了开放性动态系统中信息的高度保真,成为在商品交换、价值储存、记账等应用领域非常便捷的货币<sup>[12]</sup>。随着比特币应用范围的不断扩展,其价格也震荡升高,价格最高时曾达到20 000美金一枚,目前比特币的价格约为10 000美金一枚(截止到2020年2月18日)。一个去中心化的电子货币系统能够被大众所接受,且安全运行十多年的时间,充分体现了区块链技术的优越特性和广阔应用前景。

然而,目前承担价值储存、支付手段和记账单位的货币(例如:美元、欧元、日元、人民币、英镑)都是国家主权货币,其信用由国家信用背书。比特币作为一种电子黄金虽然无需国家信用背书也可保证其信用,但匿名性使得其成为洗钱、贩毒、军火等非法交易的选择。因此,比特币目前依然是一个被排除在主流支付系统之外的小众的加密货币体系<sup>[13]</sup>。此外,在比特币系统中,验证节点需要消耗大量算力和时间进行验证,才能将交易信息写入区块链,目前每秒只能处理7笔交易。相比之下,Visa支付系统每秒能够处理上万笔交易,缓慢的交易处理速度也限制了比特币作为主流货币的可能性。

### 3 区块链在其他领域应用的机会与挑战

随着区块链技术在加密数字货币领域的成功应用,很多机构尝试将区块链技术应用到其他领域,深度赋能分布式合作,例如:数字版权<sup>[14, 15]</sup>、资产交易<sup>[16, 17]</sup>、食品安全<sup>[18]</sup>、供应链金融<sup>[19-21]</sup>和奢侈品供应链管理等领域<sup>[22, 23]</sup>。表1列出了区块链在以上领域的典型应用案例。区块链技术在这些领域的应用存在机会,也面临困难与挑战,分析总结如下:

表1 区块链技术在不同领域的典型应用案例

应用领域	案例	主要参与方
数字版权	EdgeTech Project	Sony Music Entertainment (Japan)
资产交易	资产证券化联盟链	京东
食品安全	Food Trust	IBM, Nestle, Carrefour, Unilever
供应链金融	金融壹账通	平安集团
奢侈品供应链管理	Tracr	De Beers



第一,成功落地的区块链项目必须能够实现中心化数据存储技术难以实现的信息保真能力。如前所述,传统互联网和中心化数据库也可以在一定程度上实现信息的高度保真,例如支付宝、银联、Visa等支付系统。利用区块链技术来实现传统互联网已经较好实现的功能,并不能够给用户带来足够多的额外效用。相反,可能因为当前区块链技术存在的数据处理速度缓慢等问题导致失败。因此,评估一个区块链项目落地的可能性首先需要明确:该领域信息的高度保真能否通过中心化系统实现?此外,区块链技术虽然在信息发布与传播保真方面有优势,但它并不能解决传统互联网与中心化数据库的其他不足。例如,当前很多机构希望利用区块链技术实现音乐、影视和文字创作等方面的数字版权保护。如果版权保护的难点在于中心化节点缺乏足够的公信力,区块链技术可能存在应用机会。如果版权保护的难点不在于信息的保真性,而在于侵权的鉴定、版权保护的收益分配等问题,区块链技术可能也力所不逮,难以应用成功。

综合前面分析,区块链技术可能在以下条件拥有比较优势:(1)单一节点由于信息不足、能力不足或者公信力不足,无法实现信息的发布保真,需要引入去中心化的机制来验证信息的真伪;(2)在高度利益相关的情境下,单一节点有动机篡改数据库中的信息牟利,无法实现信息的传播保真,需要引入去中心化的数据存储机制确保信息不被篡改;(3)高度保真的信息带来的额外收益远大于实现成本。在产业互联网领域,信息的高度保真能够减少企业之间的信息不对称,降低企业间的交易成本,提高企业之间的合作深度与效率,从而促进新的商业模式的诞生。因此,区块链技术,尤其是私有链或联盟链技术在共享经济(尤其是联盟式的共享制造)、供应链管理等领域具有较好的应用前景,京东、马士基、沃尔玛等企业都有成功应用的案例<sup>[18-20]</sup>。

第二,需要考虑信息高度保真的实现难度和成本。与中心化的数据存储系统相比,区块链技术通过多个节点的多重验证、共识机制、重复存储实现其信息保真性,需花费更高的信息验证与存储成本。此外,信息的多重验证也降低了处理速度,妨碍了用户的使用流畅度和体验,制约了区块链技术的广泛应用。因此,区块链技术只能应用在对信息处理量和处理速度要求不高的场景中。在有些应用场景中,信息需要实时反映客体的状态,例如,食品生产过程需要实时更新追踪信息以保证产品质量;在加

密数字资产领域,实物资产转化成能够拆分交易的数字资产,提升资产的流动性,信息的不及时更新会给用户带来欺诈的危险。在这些应用场景中,链下客体的物理属性可能不适于多节点间的重复信息验证,从而限制信息的更新保真。物联网技术的发展能够在某种程度上解决链下信息数字化与实时更新的问题,因此区块链技术的普及应用需要物联网技术的赋能及共识机制的创新。对于音乐、视频、图像等信息化产品,交易凭证、支付凭证、代币等金融信息相对容易实现信息保真,可能会率先应用区块链技术。

第三,区块链系统的安全与隐私保护问题<sup>[11]</sup>。区块链系统中高度保真的信息具有较高的价值,必然会成为被攻击的对象。个人信息一旦泄露,不仅会侵害用户隐私,还可能造成经济上的损失和生活上的不便;企业信息的泄露则侵害企业的商业秘密,影响企业的正常运作。公开性和隐私性是区块链系统难以完全调和的两面。为了保证规则的公开和透明,区块链系统的代码往往是开源的,代码的公开透明意味着系统的漏洞更容易被攻击者发现。由加密数字货币系统的漏洞所造成的用户财产损失案例不胜枚举。仅2019年1至8月份,由于区块链系统安全漏洞造成的损失已经高达33亿美元<sup>[24]</sup>。

#### 4 未来发展需要解决的问题

区块链技术的发展尚处在早期探索阶段,其广泛应用和落地依然需要克服诸多技术和理论上的难题。

首先,需要解决区块链系统的交易处理速度问题。缓慢的交易处理速度是影响用户使用体验和限制区块链应用的重要因素。交易的处理速度和信息的高度保真是一个两难困境,要实现更高的交易处理速度就需要减少验证节点,而这则将影响信息的保真性。因此需要针对具体的应用场景,在确保足够数量的验证节点和信息保真性的前提下,结合行业特点设计个性化的分布式信息存储模式和共识机制,提高信息的处理速度,这将是未来区块链领域值得研究的问题。

其次,物联网技术与区块链技术的结合问题。在产业互联网上,合作和交易往往涉及链下客体状态信息的实时更新与传递。当链上信息与链下客体的状态进行交互时,信息的发布保真和更新保真是一个重要问题。利用物联网技术可以减少数据传输中的人工干预,从而能够提升链下信息上链的准确

性和效率。

最后,区块链管理机制的设计问题。开放性与多主体交互是区块链系统的重要特点,但是也带来了管理的复杂性。一个产业级区块链系统中的主体之间可能拥有非常复杂的关系,有些主体之间是上下游的合作伙伴关系,而另一些主体之间却可能是竞争关系<sup>[25]</sup>。拥有信息的节点企业可以凭借其私人的信息优势获取额外利益,例如:市场需求、库存水平、现金流、企业资信等。分布式的记账系统实现了区块链各节点间的信息共享,剥夺了独占信息节点的优势地位。如何设计合理的收益分享机制,协调区块链上各主体间的利益关系,建立各主体之间的信任和信息共享模式,防止信息的过度泄露也是区块链研究的重要课题。此外,区块链基础设施的开发应该由谁来主导?此类基础设施建设的投入成本分担问题也是重要的区块链管理机制设计问题。例如:IBM一直在与马士基合作,尝试建立全球化的物流信息区块链系统,实现供应链信息共享和合作<sup>[19, 20]</sup>。然而,其他物流企业可能认为马士基才是这个系统最大的受益者,他们的加入将会增强马士基的竞争力而对他们的业务并无实质性帮助,因此限制了其他物流企业应用马士基所主导的物流区块链技术的积极性。

## 5 结 语

本文从信息保真的角度讨论了区块链技术对传统互联网的改进以及区块链技术的发展方向。区块链技术从机制设计上对传统互联网做了巨大的改进——从传统的中心化数据库转变为去中心化的分布式数据库,从基于单一节点的信息验证到基于多节点的信息验证。这些改进使得信息保真不再依赖单一中心节点的公信力,提升了信息保真性。当前,区块链技术的发展依然处在初级阶段,依然存在一些难以克服的技术缺陷,阻碍了该技术在不同领域的应用。但是,随着这项技术以及相关配套技术的成熟,区块链技术一定可以得到广泛的应用,深刻影响人们在互联网上的行为模式和企业之间的合作模式。

## 参 考 文 献

- [1] Metcalfe B. Metcalfe's law after 40 years of ethernet. *Computer*, 2013, 46: 26—31.
- [2] Alabi K. Digital blockchain networks appear to be following Metcalfe's law. *Electronic Commerce Research and Applications*, 2017, 24: 23—29.
- [3] Catalini C, Tucker CE. Antitrust and costless verification: an optimistic and a pessimistic view of the implications of blockchain technology. *SSRN Electronic Journal*, 2018.
- [4] Katz M, Shapiro C. Network externalities, competition, and compatibility. *American Economic Review*, 1985, 75 (3): 424—440.
- [5] Rochet JC, Tirole J. Platform competition in two-sided markets. *Journal of the European Economic Association*, 2003, 1(4): 990—1029.
- [6] Armstrong M, Wright J. Two-sided markets, competitive bottlenecks and exclusive contracts. *Economic Theory*, 2007, 32: 353—380.
- [7] Grinberg N, Joseph K, Friedland L, et al. Political science: fake news on Twitter during the 2016 U. S. presidential election. *Science*, 2019, 363(6425): 374—378.
- [8] Gallet CA. Competition in the US lemon market. *Applied Economics Letters*, 2002, 9(3): 147—149.
- [9] Li Z, Ji Y, Tong L. Research on the 'Lemon' problem for Chinese online shopping market. *Advanced Science Letters*, 2013, 19(4): 1122—1125.
- [10] Kim S, Sarin A. Distributed ledger and blockchain technology: framework and use cases. *SSRN Electronic Journal*, 2019.
- [11] 贾丽平. 比特币的理论、实践与影响. *国际金融研究*, 2013, (12): 14—25.
- [12] Babich V, Hilary G. Distributed ledgers and operations: what operations management researchers should know about blockchain technology. *Manufacturing & Service Operations Management*, in press, 2019.
- [13] Hinzen FJ, John K, Saleh, F. Bitcoin's fatal flaw: the limited adoption problem. *SSRN Electronic Journal*, 2019.
- [14] Ding Y, Pu H, Liang Y, et al. Blockchain technology in the registration and protection of digital copyright. *Advances in Intelligent Systems and Computing*, 2020, 1017: 608—616.
- [15] Savelyev AI. Copyright in the blockchain era: promises and challenges. *SSRN Electronic Journal*, 2017.
- [16] Chiu J, Koepl TV. Blockchain-based settlement for asset trading. *Review of Financial Studies*, 2019, 32 (5): 1716—1753.
- [17] Smith J, Vora M, Benedetti HE, et al. Tokenized securities and commercial real estate. *SSRN Electronic Journal*, 2019.
- [18] Aitken, R. IBM & Walmart launching blockchain food safety alliance in China with fortune 500's JD.com. *Forbes*, <https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/>, 2017.
- [19] Groenfeldt, T. IBM And Maersk apply blockchain to container shipping. *Forbes*, <https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/>, 2017.

- [20] IBM Corporation. Maersk and IBM introduce tradeLens blockchain shipping solution. IBM Newsroom <https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution>, 2018.
- [21] Chod J, Trichakis N, Tsoukalas G, Aspegren H, Weber M. On the financing benefits of supply chain transparency and blockchain adoption. *Management Science*, in press, 2020.
- [22] Choi TM. Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains. *Transportation Research Part E: Logistics and Transportation Review*, 2019, 128: 17–29.
- [23] Mathew RM, Suguna R, Shyamala Devi M. Exploration of blockchain for edifying safety and security in IoT based diamond international trade. *International Journal of Innovative Technology and Exploring Engineering*, 2019, 8: 3224–3228.
- [24] 链安, 2019 前 8 个月区块链安全漏洞已造成 33 亿美元损失, 区块律动, <https://www.theblockbeats.com/news/3414>, 2019.
- [25] Ferreira D, Li J, Nikolowa R. Corporate capture of blockchain governance. *SSRN Electronic Journal*, 2019.

## Opportunities and Challenges of Blockchain Technology : the Perspective of Information Fidelity

Gao Jie<sup>1</sup>    Huo Hong<sup>2</sup>    Zhang Xiaoqing<sup>1</sup>

(1. *The School of Management, Xi'an Jiaotong University, Xi'an 710049;*

2. *Department of Management Sciences, National Natural Foundation of China, Beijing 100085*)

**Abstract** This paper analyzed the difficulties of traditional internet in ensuring information fidelity from three perspectives: publication fidelity, transmission fidelity and updating fidelity. Setting Bitcoin as an example, we analyzed the advantage of the blockchain technology over traditional internet in data recording, data storage and data maintenance. Compared with traditional internet, the blockchain technology was advantageous in realizing transmission fidelity and publication fidelity, while its advantage in updating fidelity highly depends on the usage context. We then summarized the use cases of the blockchain technology and identified the opportunities and challenges of its application. Three issues should be resolved before the large scale application: improvement of the transaction processing speed, the coherence of the blockchain with other technologies (e.g. internet of things) and the development of blockchain management protocols. Overall speaking, we thought that the blockchain will eventually co-evolve with other technologies, reach wide adoption and fundamentally affect the interaction behavior of individuals and organizations.

**Keywords** blockchain; information fidelity; bitcoin; mechanism design

(责任编辑 齐昆鹏)