区块链

领导干部读本

任仲文◎编

区块链将为新一代信息技术发展带来新机遇
引发新一轮技术创新和产业变革

人民日报出版社

区块链

领导干部读本

任仲文◎编

人民日报出版社

图书在版编目（CIP）数据

区块链——领导干部读本 / 任仲文编.—北京：
人民日报出版社，2018.4
ISBN 978-7-5115-5389-8

Ⅰ.①区… Ⅱ.①任… Ⅲ.①电子商务—支付方式—中国—
干部教育—学习参考资料 Ⅳ.①F713.361.3

中国版本图书馆CIP数据核字（2018）第060451号

书　　名：区块链——领导干部读本
编　　者：任仲文

出 版 人：董　伟
选题策划：鞠天相
责任编辑：蒋菊平　刘天骥
版式设计：九章文化

出版发行：人民日报出版社
社　　址：北京金台西路2号
邮政编码：100733
发行热线：（010）65369527　65369512　65369509
邮购热线：（010）65369530　65363527
编辑热线：（010）65369528
网　　址：www.peopledailypress.com
经　　销：新华书店
印　　刷：大厂回族自治县彩虹印刷有限公司

开　　本：710mm × 1000mm　1/16
字　　数：160千字
印　　张：13.5
印　　次：2018年7月第1版　2018年11月第5次印刷

书　　号：ISBN 978-7-5115-5389-8
定　　价：28.00元

序　言

当前，全球新一轮科技革命和产业变革持续深入，国际产业格局加速重塑，创新成为引领发展的第一动力。在这一轮变革中，信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的领域，是全球技术创新的竞争高地，是引领新一轮变革的主导力量。

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用，被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在2008年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一

代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。

尽管区块链技术还存在可扩展性、隐私和安全、开源项目不够成熟等问题，但是已有的应用充分证明了区块链的价值。未来一段时间内，随着区块链技术不断成熟，其应用将带来以下几个方面的价值：

一是推动新一代信息技术产业的发展。随着区块链技术应用的不断深入，将为云计算、大数据、物联网、人工智能等新一代信息技术的发展创造新的机遇。例如，随着万向、微众等重点企业不断推动 BaaS 平台的深入应用，必将带动云计算和大数据的发展。这样的机遇将有利于信息技术的升级换代，也将有助于推动信息产业的跨越式发展。

二是为经济社会转型升级提供技术支撑。随着区块链技术广泛应用于金融服务、供应链管理、文化娱乐、智能制造、社会公益以及教育就业等经济社会各领域，必将优化各行业的业务流程、降低运营成本、提升协同效率，进而为经济社会转型升级提供系统化的支撑。例如，随着区块链技术在版权交易和保护方面应用的不断成熟，将对文化娱乐行业的转型发展起到积极的推动作用。

三是培育新的创业创新机会。国内外已有的应用实践证明，区块链技术作为一种大规模协作的工具，能推动不同经济体内交易的广度和深度迈上一个新的台阶，并能有效降低交易成本。例如，万向将结合“创新聚能城”建设，构建区块链的创业创新平台，既为个人和中小企业创业创新提供平台支撑，又为将来应用区块链技术奠定了基础。可以预见的未来是：随着区块链技术的广泛运用，新的商业模式会大量涌现，为创业创新创造新的机遇。

四是为社会管理和治理水平的提升提供技术手段。随着区块链技术

在公共管理、社会保障、知识产权管理和保护、土地所有权管理等领域的应用不断成熟和深入，将有效提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，对社会管理和治理水平的提升具有重要的促进作用。例如，蚂蚁金服将区块链运用于公益捐款，为全社会提升公益活动的透明度和信任度树立了榜样，也为区块链技术用于提升社会管理和治理水平提供了实践参考。

随着新一轮产业革命的到来，云计算、大数据、物联网等新一代信息技术在智能制造、金融、能源、医疗健康等行业中的作用愈发重要。自“十二五”被确立为七大战略性新兴产业之一以来，我国新一代信息技术的发展迅速，逐步成为各行业深化信息技术应用的方向。从国内外发展趋势和区块链技术发展演进路径来看，区块链技术和应用的发展需要云计算、大数据、物联网等新一代信息技术作为基础设施支撑，同时区块链技术和应用发展对推动新一代信息技术产业发展具有重要的促进作用。

（根据工信部发布的《中国区块链技术和应用发展白皮书》整理）

目 录

CONTENTS

001 一、区块链是什么

任何产业能够得到长久发展，都需要推动社会进步，满足人们生产生活需求。无论区块链在当下是否真正为实体经济发展和改善人民生活提供了支持，但长远来看，以人为本，从大众的根本需求出发，为社会进步和经济发展提供高效率、低成本的解决方案，才是区块链行业发展壮大，迈向成熟的持久动力。

——人民网总裁 叶蓁蓁

053 二、区块链的价值

区块链是一种分布式数据库系统，特点是不易篡改、很难伪造、可追溯。区块链记录发生交易的所有信息，一旦数据进入区块链，即使是内部工作人员也很难在其中做任何更改而不被发现。这个特点决定了其与互联网应用密不可分。应用场景越大、越丰富，区块链技术和产业的发展就会越快。

——北京航空航天大学数字科技与区块链实验室主任　蔡维德

099 三、区块链发展进入新阶段

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。

——《中国区块链技术和应用发展白皮书》

135 四、区块链发展带来新挑战

区块链的治理规则总体由区块链参与者设定的规则组成，规则本身又分为两大层面：一是技术层面的治理规则，由软件、协议、程序、算法、配套设施等技术要素构成。二是技术外部的、监管法规层面的治理规则，由法规框架、条文、行业政策等组成。兼顾两者，才更有利于保护参与者乃至全社会的广泛利益。

——《中国区块链技术和应用发展白皮书》

179 五、区块链未来前景展望

整个人类的历史是分久必合、合久必分，区块链技术使得互联网时代也到了一个新的分久必合、合久必分的时代。我们正是面临着区块链和去中心化技术给这个时代带来的一场新的革命。

——丹华资本创始董事长　张首晟

一、区块链是什么

任何产业能够得到长久发展，都需要推动社会进步，满足人们生产生活需求。无论区块链在当下是否真正为实体经济发展和改善人民生活提供了支持，但长远来看，以人为本，从大众的根本需求出发，为社会进步和经济发展提供高效率、低成本的解决方案，才是区块链行业发展壮大，迈向成熟的持久动力。

——人民网总裁　叶蓁蓁

从互联网思维到区块链思维

“区块链”作为新兴技术，短时期内得到如此多的关注，在现代科技史上并不多见。我们希望在行业发展的关键节点，通过搭建产业、学术、资本、传媒等多方参与的高层次交流平台，促成思想激荡、百家争鸣，在技术研发、商业应用、政策扶持、资本助力等方面总结经验、谋划未来。

人民网已经创立 21 年，它始终保持着技术敏感，对于区块链技术及其应用也保持着密切关注。在此，就当下的“区块链热”与大家分享一些我们的看法。

首先，区块链行业作为当前最受关注的科技创新热点之一，聚集着大量人才、资本和社会资源。区块链正处在发展的关键节点。

第一，区块链行业将迎来重要的政策机遇期。2018 年 5 月 28 日，习近平总书记在中国科学院第十九次院士大会、中国工程院第十四次院士大会上发表了重要讲话，将区块链与人工智能、量子信息、移动通信、物联网等并列为新一代信息技术的代表。这表明中央对区块链技术的发展前景寄予厚望。目前，全国已有十余个省、自治区和直辖市，相继出台了支持和鼓励区块链产业发展的相关政策，雄安新区更是把区块链纳入重点产业，大力发展。总书记的讲话对各地方、各部门更加全面和深

刻认识区块链技术、积极出台有关政策，将起到巨大的推动作用。

第二，行业处于由乱到治的关键阶段。众所周知，区块链技术正处在发展初期，出现了一些“乱象”，给经济、金融和社会秩序带来了一些困扰。2017 年 9 月，中国人民银行、中央网信办、工业和信息化部等七部委联合发布《关于防范代币发行融资风险的公告》，明确指出首次代币发行（ICO）进行融资的活动涉嫌从事非法金融活动，严重扰乱了经济金融秩序。此后，在各级政府、社会舆论及众多业界有识之士的共同努力之下，区块链行业的负面效应逐步得到遏制，出现了一些积极变化，“专注技术落地，服务实体经济”正越来越成为业内人士的共识。如今，从大型企业到创业公司，从政府基金到天使投资，大批从业者和相关机构都在用实际行动致力于区块链技术落地，有的已经取得了初步成果，这些都是非常积极的信号。局面来之不易，我们应当倍加珍惜，共同强化区块链行业积极向好的发展态势。

其次，过去几年，许多传统行业运用“互联网思维”创造了新的商业模式。如今，区块链行业迎来重大机遇，要习惯运用“区块链思维”去照亮认识盲区、倒逼技术升级、开拓产业空间。

第一，“区块链思维”是什么？目前给“区块链思维”下定义是一件有困难的事情。我个人理解，区块链技术目前最大的意义在于它的运行机制：通过技术的精巧组合，完成资源的公平分配，从而确保社区的目标一致、成员的行为规范。这给我们看问题、想办法提供了一种全新的切入角度和思考路径。因此，关于“区块链思维”，我想至少可以提炼出三个关键点：一是技术架构的可靠性；二是分配过程的公平性；三是成员行为的规范性。

第二，用“区块链思维”做什么？区块链技术在很长一段时间内都

被理解为“比特币技术”，比特币成了区块链的代名词。但是如果将比特币架构直接照搬套用到其他区块链技术应用场景中，难免衣不合体。“区块链思维”可以帮助我们跳出比特币架构，从内涵层面认识整个技术体系。目前，区块链技术的 2.0、3.0 版本对“比特币架构”进行了优化，这些都是“区块链思维”的具体体现。

第三，“区块链思维”怎么用？我想需要区分区块链技术的内涵与外延，把内涵的刚性和外延的灵活性相结合。现阶段，区块链技术最显著的内涵在于使用分布式记账、非对称加密、点对点传输等技术组合，确保数据不可篡改、全程可追溯，从而解决社会交往中的信任构建难题。基于这一内涵，区块链技术要应用于各种具体场景，其外延要不断拓展，例如区块链与激励机制的结合，智能合约的发展，等等，最终都是为了通过区块链技术来确定真伪，让价值在互联网上直接流通，构建真正的价值互联网。想象是技术进步的重要驱动力。我们不妨以开放的心态，开发出区块链技术更丰富的应用，引领技术健康发展。

最后，关于区块链的种种讨论，虽然达成了一定的共识，但是还存在诸多分歧。我们在此呼吁业界同人继续深入交流、凝聚共识、去伪存真，用发展、科学、战略、冷静的眼光看待“区块链热”。

第一，用发展的眼光看区块链技术。回顾区块链技术近十年的发展历程，我们会发现它与早期的互联网技术有许多惊人相似的故事。比如都是从小众的学术圈走向中间的商业圈，再走向大众的社会圈；再比如早期都被赋予实现个人自由、平等的价值理想等。但从互联网技术的后续发展可以看出：实验室中的经典架构与现实社会结合后，将会发生改变；绝对自由是不存在的；商业的深度参与，使得早期的理想状态十分短暂；资本与技术反复博弈将会推动新技术应用螺旋式上升……总之，如

果用发展的眼光看技术，热点只是起点。

第二，用科学的眼光看区块链标签。当下区块链之所以备受热捧，一个重要的原因是被贴上了许多特别的标签，比如：去中心化、全程可追溯、不可篡改等。但这些标签是否都经得起历史和现实检验，还不宜过早下结论。以“去中心化”为例，从哲学上讲，矛盾总有主次；从现实来看，大到宇宙星系，小到一个原子，都有中心。区块链经典的技术架构虽然去掉了数据结构的中心，但其运行仍受中心化节点的约束。去中心化的标签能否在区块链上贴得牢，可能还需要进一步探讨。事实上，曾经有“去中心化”标签的互联网，只是颠覆了旧的中心，形成了新的寡头。

第三，用战略的眼光看区块链产业。任何产业能够得到长久发展，都需要推动社会进步，满足人们生产生活需求。无论区块链在当下是否真正为实体经济发展和改善人民生活提供了支持，但长远来看，以人为本，从大众的根本需求出发，为社会进步和经济发展提供高效率、低成本的解决方案，才是区块链行业发展壮大，迈向成熟的持久动力。要高度警惕任何想一夜暴富的投机想法，警惕任何想捞一票就走的骗子行为，建立健全行业持续健康发展的自律准则和监管机制。

第四，用冷静的眼光看区块链商机。“区块链热”骤然兴起的重要原因是很多人都认为区块链技术有广阔前景并害怕错过商机。但历史证明，商机并非都是先到先得、先到多得的游戏，新技术发展的各个阶段都会创造新的商业机会，不同阶段的商机适合不同类型的人和机构去把握。就像现在互联网产业蛋糕的最大拥有者，并非都是最早的从业者和探索者。俗话说“好饭不怕晚”！与其躁动焦虑、盲目跟风，不如静心分析社会需求，研究行业痛点，找准自己最能创造真实价值的领域、阶段，

或许最终会取得更大的收获。

作为党和国家在网络舆论生态中的“领航者”“排头兵”，人民网的发展始终以内容和技术双轮驱动。未来我们将继续发挥主流媒体优势，秉持实干兴业的心态积极布局区块链：一是体现主流媒体的担当，为业内提供真实、权威的新闻资讯，为监管机构提供决策数据和政策参考，促进区块链产业持续、健康发展；二是扎实推进技术研发，积极探索区块链技术与人民网主营业务结合的有效路径，探索区块链技术的实际应用和实用产品；三是务实搭建开放平台，连接行业资源，布局优质项目，探索产业发展，推动区块链技术的进步，促进区块链造福人民美好生活。

（本文根据人民网总裁叶蓁蓁最近演讲整理）

区块链的缘起和发展

从一个梦想说起。多年前，我还是一个“北漂”，那时候的我有一个梦想：建立一个互联网平台，每个人都可以把自己的想法发到上面，有相同想法的人可以参与、支持，让有梦想的人去圆梦。几经辗转，“梦”终究还是一个“梦”。直到接触了区块链，我发现这个“梦”至少有部分实现的可能。

什么是区块链？

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。

区块链（Blockchain）是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术。区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

大部分观点认为，区块链技术是中本聪发明，从比特币开始的。其

实不然，区块链技术早在上世纪七八十年代就有了。只不过中本聪创造性地把分布式存储和加密技术结合发明了比特币，而因为比特币的价格一路攀升才逐渐为人们所重视和熟知。

提起区块链不能不提币，但是比特币不等于区块链，只是区块链技术的应用之一；区块链也不等于各种币，各种币只是区块链经济生态和模型中的一部分。区块链技术的应用不一定非要有币，但是必须承认，因为有了比特币和各种币形成的财富效应，区块链技术才得以更快、更广泛的引起人们的关注、认识，也客观上推动了实际应用的发展。

区块链的形式、特点及现状

区块链目前主要分为：公有链、私有链、联盟链三种。三种各有侧重点、应用场景和实现的功能，以及基于此构成的不同的经济生态模式。

三种链的特点对比如下表：

	私有链	联盟链	公有链 1.0	公有链 2.0	公有链 3.0
参与者	个体或机构内部	联盟内部使用，具有准入机制，安全性更高	任何人可以自由使用	任何人可以自由使用	任何人可以自由使用
信任机制	自行背书	集体背书	POW	POW/POS	POS/DPOS 等
记账人	自定	参与者协商决定	所有参与者	所有参与者	所有参与者或多中心记账
激励机制	无	可选	需要	需要	需要

续表

	私有链	联盟链	公有链 1.0	公有链 2.0	公有链 3.0
中心化程度	以中心化为主	多中心化	去中心化为主 + 多中心化	去中心化	多中心化
突出优势	透明和可追溯	效率 / 成本 / 安全性	信用的自建，挖矿记账，支持二次编程	在公链上编写 Dapp 应用更容易，具有平台化的特点	更快的交易速度，支持多种编程语言编写 Dapp，可以挖矿也可以不挖矿
典型应用场景	机构内不对外提供服务的区块链应用和研究	行业、组织、联盟等进行数据资源交互和交易的多中心化的共识机制	线上的交易记账	线上的基于公链的各种 Dapp	线上基于公链的各种 Dapp
典型代表	Overstock	R3 的银行联盟	比特币	以太坊	EOS 及其他新公链
承载能力	1000 ~ 10 万笔 / 秒	1000 ~ 10000 笔 / 秒	少于十笔 / 秒	几十笔 / 秒	百万笔 / 秒

区块链行业的现状，首先给人的印象是各种币的涨涨跌跌，刺激着圈内圈外人的神经。根据不完全统计，国内外目前已经开发出来的和待开发的“公链”达数千条之多，但是实际能落地应用的屈指可数，目前仅“以太坊”的系统完整性和生态建设相对较好，聚集全球最多的开发者群体，可以基于“以太坊”开发一些应用型的“DAPP”。然而由于交易速度等方面的限制，还是无法大规模的落地一些对交易速度、并发速度要求高的应用。因此，目前也只能进行一些相对浅层次的应用：卡牌类游戏、去中心化的阅读、社区等，距离大规模应用还有相当的距离。

当然，我们同时也必须看到，由于巨大的财富效应，不管是美国、

中国、日本、欧洲、新加坡，乃至更多的东南亚、地中海、加勒比海国家，尤其是美国的硅谷和中国北上广深杭，区块链行业吸引和聚集了顶尖的大量人才，技术很可能以超过我们预期的速度取得突破，而大规模的应用爆发很可能就在未来 6 到 18 个月就会发生。

区块链技术的缘起和应用

“代码即法律”“代码即信任”是区块链世界经常提及的两句话，也是区块链世界的核心和精髓，浓缩为两个字就是值得信任的“共识”。不可否认的是，区块链技术从一定程度上体现了技术人员，尤其是程序员对现实世界的不信任，希冀于通过代码来构建一个更加的公平、公正、公开的世界。比如中本聪创造比特币的时候就写明确说过，因为美元的不可信任，所以他要创造一个可信赖的永不增发的货币体系。

区块链技术，表面上解决的是技术性的问题，本质上解决的信任的问题，是基于代码的信任、不可篡改的信任、广而告之的信任，是在一个缺乏信任的环境下建立信任和传递信任的问题。

从客观上来说，区块链技术的发明，也确实有助于构建更加公平、公正、公开的社会。尤其是进入移动互联网时代，过去两年人类产生的数据量超过了人类有史以来总和的 9 成以上，人类的各种经济、社会行为，甚至包括人类本身，都以各种数据的形式被存储在了服务器上；尤其是随着 AI 技术的发展，人类的情感、触感等也将彻底的数据化、网络化。当一切都数据化、网络化以后，个体的人、组织、企业、机构、政府等数据的所有权、使用权、收益权如何进行分割、保护、实现，将会成为最重要的命题。如果在传统的中心化的网络上，我们每个个体、机构等

的数据名义上是自己的，实际上都是中心化的组织的，这也是移动互联网时代缔造了包括阿里、腾讯、谷歌、脸书等无数大公司的原因。个体的利益和权力，都被这些中心化的大公司以无偿或者极低的价格拿走了，成为了这些中心化公司的资产，并且利用这些资产进行了一系列的增值。而数据的提供者则只能被动的享受一些或免费或收费的服务，并且无法从中分享发展的收益。

如果 AI 是生产力，那么区块链虽然是技术，但是本质上体现的是生产关系。区块链，以一种技术的形式，重新构建了商业关系甚至是生产关系，区块链是人类有史以来对于商业关系和生产关系最伟大的发明。为人类社会突破以往的商业模式、商业逻辑和生产组织关系提供了全新的模式、平台和技术实现的路径及工具。通过数据上链的形式，个体的权益被保护，通过与授权与被授权的形式，个体可以参与到整体的发展中，甚至可以参与整体发展的决策过程，影响或推动整体的发展，并且从整体发展的收益中获取到自己原来被剥夺的应有的权益。

因此，凡是需要更加公平、公正、公开的企业、行业，都可以用到区块链技术，都可以用区块链技术进行改造和实现；凡是需要数据存储、保护、授权、交易的企业、行业，都可以用到区块链技术，都可以用区块链技术改造和实现；凡是需要社会化协作，尤其是跨境的、基于计算机网络可以完成的社会化分工和协作，都可以用到区块链技术，都可以用区块链技术改造和实现。

Coin 和 Token 的区别

“Coin”是币，“Token”是“代币”，也被翻译为“通证”，即“通

用的证明”的意思。绝大多数人，笼统地把两个都称为“币”，实际上这是两个完全不同的概念。

谈区块链，是不能避开“币”的问题的，否则就是“掩耳盗铃”。但是区块链不等于币，币更不等于区块链，不是所有的区块链都必须有币，但是有些区块链没有币也是不行的。所以有“有币区块链”和“无币区块链”之说。

本来意义上的区块链的“币”都是“公链”的“GAS”（燃料），因为链是需要节点和矿工的，矿工就是节点的建设者和运维者，矿工支持链的运转是需要进行投资和获取回报的，基于链的应用、交易等，是需要成本的，因此需要“GAS”，也就是“币”。基于公链原生的“币”，一般被称为“Coin”。

“Token”本质上是一种权益的证明，因此也分为“权益型代币”和“功能性代币”。“Token”一般出现在基于公链诞生的各种应用型的区块链项目上。“权益性代币”更加接近于证券，实际上就是发行该“Token”的项目或者公司的股权；而“功能性代币”是在使用该应用过程中为了打造更好的用户体验、进行生态建设和激励媒介。所以，“权益性代币”的定价和升值基础一般是项目本身发展的未来的价值；而“功能性代币”的定价和升值基础一般是项目中业务、服务的定价或者是未来使用该应用的用户的数量多少及项目的经济模型设计的通缩所造成的稀缺性。

需要不需要有币，本质上是区块链项目本身的定位和经济模型所决定的。比如公链项目一般都有币，而联盟链和私有链一般不需要有币。为什么这么讲？因为公链项目的参与人是不特定的，是完全公开的，所有人都可以参与的，每个人都可以去贡献也可以使用。但是公链的开发、维护、节点的建设和运行，都是需要有人参与和付出的，如果没有币，

那么他们的回报从哪里来？没有基于币的合理的经济模型，就没有人愿意参与到其中来了。而联盟链和私有链的投资和收益都是有固定的、特定的对象的，所以可以没有币。

举个例子：区块链公链可以近似地理解为网络开发语言，比如 C++、Java 之类的，是一种底层的支撑技术。但是和开发语言不同的是，公链除了技术本身的迭代进化之外，还需要节点去进行分布式记账、交易与维护。其一：如果用传统的法币模式，在技术产生效益之前，或者说产生的效益不够大的情况下，如何调动参与的各方的积极性？其二：如果用传统的法币模式，各参与方之间，如何进行实时、有效、快速、不受空间和时间限制的结算？答案很明显！

区块链的未来

可能有人会注意到一个问题，“Coin”也好、“Token”也好，纯粹的数字货币，除了交易中的价值，对人类本身是没有意义的，仅仅是一串字符或者说是代码而已。那么除了交易的价值，代码的意义是什么？谁真正需要代码？其实，代码本身只有对机器才有意义。代码是机器运行的基础，也是机器之间交流、沟通、结算、进行资源分配的工具。所以我认为，区块链本质上是为机器服务的。

我们说过，AI 是生产力，区块链是生产关系，而机器是生产工具；未来，AI+ 区块链 + 机器，将构成世界的主体。当 AI 进化到足够智能以后，由人类编写的区块链将有 AI 来进行，而机器之间，比人类之间更加容易达成“共识”，遵守“共识”。

如果我们人类不能很好的规划、掌控好技术的发展，未来的人类，

很可能是高度人工智能的机器统治下的“肉机”。而今天和未来所有的区块链从业人员，将成为机器的“带路党”。

区块链对创业和创新的贡献

提到区块链，还有一个不能不提的问题的是 ICO。ICO（是 Initial Coin Offering 缩写），首次币发行，源自股票市场的首次公开发行（IPO）概念，是区块链项目首次发行代币，募集比特币、以太坊等通用数字货币的行为。

ICO 是一种区块链行业术语，是一种为加密数字货币 / 区块链项目筹措资金的常用方式，早期参与者可以从中获得初始产生的加密数字货币作为回报。由于代币具有市场价值，可以兑换成法币，从而支持项目的开发成本。ICO 所发行的代币，可以基于不同的区块链。常见的是基于以太坊（ETH）和比特股（BTS）区块链发行，由区块链提供记账服务和价值共识，实现全球发行和流通。

ICO 参与者对于一个项目的成功非常重要，他们会在社区里为该区块链项目进行宣传，使它产生的代币在开始交易前就获得流动性。但 ICO 的参与者最看重的依然是由项目发展或代币发行后价格升值带来的潜在收益。

IPO（英文简称 Initial Public Offering）首次公开发行，指股份公司首次向社会公众公开招股的发行方式。与 ICO 相比，他们有共同点也有区别。

它们的共同点：都有募集资金的行为；都有潜在投资者为了潜在的巨大收益而冒险参与。它们的区别：ICO 的大部分支持者是项目爱好者或

不专业的投资者；ICO 有可能发行的不是股份，是通证；ICO 不募集法币，募集的是通用性较高的数字货币；IPO 的投资者一般不参与项目，而 ICO 的投资者是项目社区的重要组成部分，相当部分 ICO 的投资者本身就是项目开发者、合作者或者用户。

2017 年，全球 ICO 募集资金超过了 50 亿美元，2018 年预计将超过 100 亿美元。ICO 已经成为区块链行业创业最重要的资金来源，并且通过“币改”等方式正在逐渐成为初创企业或者发展中企业极其重要的募资方式。

当然，其中鱼龙混杂，难免泥沙俱下。在看到很多问题的同时，我们也必须同时看到，ICO 对于创业和创新的巨大的贡献和支持。尤其是在区块链发展还很早期的阶段，需要进行大量的投资而又没有产出的情况下，依赖传统的融资方式和融资手段是无法支撑这么多创业团队，无法吸引这么多优秀的人才进行先烈、先驱式的探索的。ICO 对于区块链技术和行业的整体发展，起到了无法替代的作用。

区块链被认为是下一代互联网，是互联网十倍、百倍的规模，而一项基础技术的发展，需要大量甚至是天量资金的投入。而基础技术，历来是我们国家最薄弱的环节。和互联网最息息相关的 IP 技术不是我们的，操作系统不是我们的，数据库技术不是我们的，很多底层的技术都不是我们的。互联网时代，中国的企业成功基本都是在应用层面的成功，而不是底层技术的成功。这一点，希望在区块链时代能够改变或者说避免。只有允许更多的尝试和失败，才有可能在区块链时代不落伍，甚至是领先世界。而这些靠行政规划，靠传统的 VC、PE 投资模式是很难实现的。

另外一方面，自从李克强总理提出“大众创业、万众创新”以来，全国上下，创业气氛浓厚，无数创业者响应号召投身创业大潮中。但是

我们同时也需要看到，现代创业成本越来越高，失败率越来越高。仅靠创业者自身的资金积累或者覆盖率、成功率极低的风投模式已经越来越难支撑。因此，创业和创新急需新的融资和发展的模式。而我们传统的资本市场和金融资源，基本上都是为大公司服务的，不是为创业公司服务的，很多融资的模式和结果，事实上已经背离了融资的初衷，更不必提为小微企业、创业企业服务了。所以，探索和建立真正服务小微企业、创业企业的投融资模式、渠道、平台，是极其重要的课题。ICO 尽管有各种问题，但是至少让我们看到了希望。规范以后的发展，必然会为创业和创新带来更大的支持。

社群与崛起的 90 后

区块链是基于“共识”的技术平台，因此可以天然聚集用户形成“社群”。大的社群有数十万人，小的社群也有几千人，而“社群”天然有领袖存在。区块链社群的领袖，由于掌握了大量的信息、资金资源，对社群的领导力和影响力更是其他类型的社群所无法比拟的。社群领袖的态度、动向，甚至好恶等都可以直接影响甚至决定一个项目、一个币种的走势乃至成败。号称中国“比特币首富”的李笑来就是其中最典型的代表。

但是，区块链上社群领袖中最需要关注的恰恰是另外一批人，一批 85 后和 90 后，尤其是 90 后。很多家境优越的 90 后较早的参与了数字货币投资，部分草根也因为早期参与数字货币的投资，随着 2017 年数字货币牛市的来临，已经积累了惊人的财富。这些人在积累了巨额的财富同时，大量投资新兴的区块链项目、媒体、基金，因为自媒体的发达和

区块链创业正处于风口，这些人从而在投资界和创业界、乃至全社会拥有了更大的影响力和话语权。

区块链的宗旨是构建更加公平、公正、公开的世界。区块链上有一个常用的词，叫作“映射”，即用户在一个链上拥有的资产或者权利，要同等的投射到其他的资产或者权利上。假以时日，区块链启蒙和培养出来的人群、社群领袖，在掌握了天量的财富、资源和媒体发声渠道以后，会有什么样的现实诉求，这是我们必须思考和面对的。

关于监管的一些思考和建议

作为一个行业的从业者，我们经常在思考和探讨如何才能更加有效地促进这个行业的长远和健康发展。从全球范围来看，基本上各国政府都欢迎区块链技术，并且愿意积极推进区块链技术在包括政府管理、政务公开、民生保障、金融体系等方面的应用。但是在对于数字货币和数字货币延伸出的交易所、ICO 等方面则态度差别很大。有欢迎的、有拒绝的，还有有限接受的。

基本的态势是：大国普遍比较谨慎（日本除外），小国普遍欢迎；资本和外汇自由流通的国家比较宽松，反之则相对严格。

而且我们看到，由于区块链天然的去中心化和全球化的特征，资金、人才等正在迅速地向政策宽松的地区和国家流动。

在区块链上，我们能看到一个非常有意思的现象：大国未必竞争得过小国，而很多小国正在用宽松的政策割大国的羊毛，时代变了。

作为目前全球区块链的两个中心之一，作为全球网民、币民，未来也是“链民”最多的国家，我们国家要高度重视这一趋势并且尽快出台

有效的措施。只有构建一个有序的市场，行业才能得到健康的发展，并为经济、社会的发展贡献力量。

根据行业的现状、发展的趋势，结合区块链行业公开、透明等技术特点，关于监管方面，我在此提出一些想法和建议，希望可以起到抛砖引玉的效果。

1. 鉴于区块链项目的自身公开、透明等特点，可以通过技术手段对项目进展、融资、支出等进行追踪。

2. 对以“Token”形式投资或者回报的机构进行管理和引导。

3. 堵不如疏，出台相应的法律法规，对散户投资进行明确的规定，制定相应的项目融资额度、投资人数量、单个投资人单笔、总量投资额度等方面的限制。

4. 提供或者说对进行募资的平台进行管理和指导，所有项目必须进行合格的 KYC。最好的投资人教育是“亏钱”，投资人会在投资过程中学会风险控制。

5. 用区块链技术对公开募资的项目进行定期专业化审计，并提供投资人投诉的畅通的通道且能进行及时有效的反应。

6. 严厉打击伪区块链项目和打着区块链旗号的传销行为。

7. 制定合理的税收政策：数字货币的最大特征之一是货币私人化，实际上货币私人化并不是大问题，最大的问题是通过数字货币税收的私人化。对于国家和政府而言，这才是最大的问题。因为数字货币最终要兑换成法币，所以实际上并没有增加法币的数量，只是在某些环节上替代了法币的流通。而如果不制定与数字货币相关的税收政策，通过数字货币流通创造的价值全部私人化，才是国家和政府最大的隐患和损失。

8. 合法化和监管交易所：未来数字资产的流通将全部通过中心化和

去中心化的交易所进行，这已经不是通过行政命令可以解决的。区块链是全球化的、无国界的，但是人是国家化的，只要在合理的边际成本线内，交易所可以，也是愿意被进行合法化监管的。同时，由于区块链的全球性特征，需要我们的政府加强与全球主要经济体的沟通，达成对于数字货币、数字资产监管的全球的、广泛的共识，并且基于此共识进行相应的协作。

一个席卷全球的基于区块链的时代正在快速地到来，拥抱是毫无疑问的，但是如何拥抱，用什么样的心态和姿势去拥抱，是值得我们思考和探索的。

（薛靖中，杭州高度投资管理有限公司合伙人、杭州 AI&Block Center 创始人）

三问区块链

近段时间，有关比特币的新闻非常吸睛，区块链也跟着火了一把。资本市场上，各种区块链概念股的股价涨跌犹如过山车般惊心动魄。从反应敏锐的资本市场可以看出，区块链正站上风口，受到各方高度关注。

什么是区块链？

一种去中心化的分布式账本数据库，没有中心，数据存储的每个节点都会同步复制整个账本，信息透明难以篡改

近几年，越来越多的机构开始重视并参与区块链技术研发。从最初的比特币、以太坊，到各种类型的区块链创业公司、风险投资基金、金融机构，贴上“区块链”标签，立马就“金光闪闪”。不仅如此，很多人的微信朋友圈也被各种解读区块链的文章刷屏。

那么，到底什么是区块链？

工信部指导发布的《中国区块链技术和应用发展白皮书 2016》这样解释：广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、

利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

交通银行金融研究中心高级研究员何飞进行了通俗解释："简单地说，区块链就是一种去中心化的分布式账本数据库。"去中心化，即与传统中心化的方式不同，这里是没有中心，或者说人人都是中心；分布式账本数据库，意味着记载方式不只是将账本数据存储在每个节点，而且每个节点会同步共享复制整个账本的数据。同时，区块链还具有去中介化、信息透明等特点。

"区块链技术本质上是一种数据库技术，具体讲就是一种账本技术。账本记录一个或多个账户资产变动、交易情况，其实是一种结构最为简单的数据库，我们平常在小本本上记的流水账、银行发过来的对账单，都是典型的账本。"腾讯金融科技智库首席研究员王钧说，安全是区块链技术的一大特点，主要体现在两方面：一是分布式的存储架构，节点越多，数据存储的安全性越高；二是其防篡改和去中心化的巧妙设计，任何人都很难不按规则修改数据。

以网购交易为例，传统模式是买家购买商品，然后将钱打到第三方支付机构这个中介平台，等卖方发货、买方确认收货后，再由买方通知支付机构将钱打到卖方账户。由区块链技术支撑的交易模式则不同，买家和卖家可直接交易，无须通过任何中介平台。买卖双方交易后，系统通过广播的形式发布交易信息，所有收到信息的主机在确认信息无误后记录下这笔交易，相当于所有的主机都为这次交易做了数据备份。即使今后某台机器出现问题，也不会影响数据的记录，因为还有无数台机器作为备份。

提到区块链，很多人就把它与比特币联系在一起，不少人甚至把区块链等同为比特币。何飞说，比特币是区块链的一种呈现方式，但区块链并不等同于比特币。区块链是比特币的底层技术和基础架构，而比特币是区块链的成功应用，但并不意味着区块链只能应用到比特币上。

区块链有什么用？

能解决金融、公益、监管、打假等很多领域的痛点难点，但有不少适用条件

金融服务是区块链技术的第一个应用领域。运用区块链技术能解决支付、资产管理、证券等多个领域存在的痛点。

以支付领域为例，金融机构特别是跨境金融机构间的对账、清算、结算的成本较高，涉及很多手工流程，不仅导致用户端和金融机构后台业务端等产生高昂的费用，也使得小额支付业务难以开展。区块链技术的应用有助于降低金融机构间的对账成本及争议解决的成本，显著提高支付业务的处理效率。另外，区块链技术为支付领域带来的成本和效率优势，使金融机构能更好处理以往因成本过高而被视为不现实的小额跨境支付，有助于实现普惠金融。

比如，为解决金融机构间对账成本高的问题，2016 年 8 月，微众银行联合上海华瑞银行推出微粒贷机构间对账平台，这也是国内首个在生产环境中运行的银行业联盟链应用场景。微众银行区块链首席架构师张开翔认为，传统“批量文件对账”模式长久以来未能解决的成本高问题，正是区块链技术的用武之地。随后，洛阳银行、长沙银行也相继接入机

构间对账平台，通过区块链技术，优化微粒贷业务中的机构间对账流程，实现了准实时对账、提高运营效率、降低运营成本等目标。截至目前，平台稳定运行 1 年多，保持零故障，记录的真实交易笔数已达千万量级。

在公益领域，区块链技术也大有可为。蚂蚁金服涉及区块链的首个应用场景就是公益，帮助一群听障儿童获得一笔善款，然后运用区块链技术促进公益更加开放透明。蚂蚁金服技术实验室高级产品专家胡丹青说：“区块链公益平台就像是我们在互联网上构建了一个专门用于邮寄资金的邮局。用户捐的每一笔钱，我们都会打包成一个包裹，这个包裹通过区块链平台传递，每经过一个节点，我们都会盖上一个邮戳，最后送到受捐人手上。这样可以保证用户捐的每一笔钱都是透明、可追溯、难以篡改的。”

在商品打假方面，区块链技术可以大显身手。胡丹青介绍，蚂蚁金服将区块链技术用在了正品溯源上。目前，已有部分来自澳大利亚、新西兰的海淘商品比如奶粉，用支付宝扫一扫，就能知道是不是正品。“跟此前商家自录入商品信息不同的是，区块链是让多位‘记账师’公正、独立、不可抵赖地完成记账。”

对于金融监管，区块链技术也能发挥一技之长。2017 年金融区块链合作联盟（深圳）发布的《金融区块链底层平台 FISCO BCOS 白皮书》认为，区块链为金融监管机构提供了一致且易于审计的数据，通过对机构间区块链的数据分析，能够比传统审计流程更快更精确地监管金融业务。例如，在反洗钱场景中，每个账号的余额和交易记录都是可追踪的，任意一笔交易的任何一个环节都不会脱离监管视线，这将极大提高反洗钱的力度。

有业内人士认为，区块链 1.0 主要针对数字货币；区块链 2.0 针对智

能合约，可以应用在金融市场中；区块链 3.0 适用的场景将会更多，甚至会开创一个“区块链时代”。

何飞认为，区块链确实能解决很多领域的痛点难点，但区块链不是万能的，也有很多适用条件。

比如，区块链技术去中心化的特点适合多方参与的场景，如果只是单边或双边参与价值就不大。由于需要每个节点都去核对，区块链技术也不适用那些高频交易的活动。

再如，区块链强调的是公开透明，并不适合对数据隐私要求特别高的场景。

区块链会成新风口吗？

技术目前还不太成熟，要警惕概念炒作，特别要区分是技术创新还是集资创新，不能为了区块链而区块链

区块链概念这么火，未来会成为又一个“互联网 +”吗？

近年来，区块链的发展生态逐渐得到改善与丰富。业内人士认为，拥有国家政策扶持，得到广泛关注和资金支持，区块链技术能实现逐步稳定进步。区块链技术上行前景虽广阔，但对此也要保持一颗平常心。

“尽管眼下区块链大热，但我们仍然认为，它还处于一个非常早期的阶段。”胡丹青说，区块链概念目前存在虚热，不是热在拿技术解决现实问题，而是热在集资圈钱、炒作估值，尤其是热炒的绝大部分所谓 ICO（首次代币发行）都是集资工具创新，跟技术创新无关。

区块链技术确实能创造很大的价值，但一些风险也不容忽视。

“区块链技术还不太成熟，可应用场景比较有限，更应警惕资本市场炒作概念。”何飞说，区块链热潮的背后免不了会有一些搞噱头想投机的公司，他们并没有真正开展业务，只是企图到资本市场捞一笔就走，要谨防由此出现“劣币驱逐良币”，导致真正想开展业务的机构退出市场，影响区块链技术的应用。

胡丹青建议，对于目前的区块链热，监管部门应更主动地介入，区分是技术创新还是集资创新，鼓励政府组织、有公信力的专家、行业参与者共同帮助公众辨识，全面遏制区块链名义下的集资创新，让 ICO 实际控制人必须为集资行为承担责任。“判断是技术创新还是集资创新的依据其实很清楚，即是否以信任为始，是否通过解决信任问题创造了实际价值。”

今后更好地推广和使用区块链技术，还需继续完善基础设施、加强相关法律政策制定等。

王钧认为，共识算法等区块链的核心技术尚存在优化和完善的空间；另一方面，区块链的处理效率还难以达到现实中一些高频度应用环境的要求。目前主流的区块链技术平台均发源于国外，国内的区块链技术服务商要耐心地从底层开发做起，做到技术自主可控，争取引领全球区块链技术发展。拥有区块链应用场景的企业，要积极拥抱新事物，同时科学评估上链需求，不能为了区块链而区块链。

何飞认为，政府可以出台相关政策，指导有志于投身区块链技术研发应用的企业，同时明确一些区块链适合应用的场景及国家鼓励的领域等。

《中国区块链技术和应用发展白皮书 2016》建议各级政府主管部门借鉴发达国家和地区的先进做法，结合我国区块链技术和应用发展情况，

及时出台区块链技术和产业发展扶持政策，重点支持关键技术攻关、重大示范工程、“双创”平台建设、系统解决方案研发和公共服务平台建设等。同时，建议国内重点企业、科研、高校和用户单位加强联合，加快共识机制、可编程合约、分布式存储、数字签名等核心关键技术攻关。

（王　观）

来源：《人民日报》

区块链与比特币

如何理解比特币与比特币区块链？

比特币区块链并不是一个单一技术，而是由多种技术组成的一个集成体。这些技术之前都有，只不过比特币进行了非常机智的融合，形成了一个有机运行的体系。比特币区块链是一个完全封闭的体系，只允许比特币这种唯一的数字资产（价值），脱离了现实世界，能够给人们无限美好的遐想，但却实际上无法解决现实世界的实际问题。比特币区块链追求的是由全世界不同所有者的计算机加盟共同运行和维护，不附属于任何国家与法律的一个美好世界，一个理想的社会，形成了一个具有较强宗教信仰的组织。所以强调“去中心”（即去政府、去权力、去监管）和“去中介”，实现“人人自组织，人人可发币，人人自金融。”有人说：区块链的底层是数学逻辑，中层是哲学思维，顶层是宗教信仰。

实际上，正因为比特币体系过于追求完美，致力于摆脱现有世界运行体系，反而使其陷入脱离现实、自我封闭的“乌托邦”思维，越

是追求完美，就越陷入封闭，就越难以解决现实世界的实际问题，反而会使其失去实用价值，沦为一种“网络游戏”，更别说能够改变世界、颠覆法定货币体系。表面上，比特币区块链实现了去中心、去信任、去中介，可以点对点自由转让比特币资产等，似乎形成了充分民主法治、平等自由，不可造假篡改、没有税收和不当费用，没有贪污腐败等的美好社会，形成了所谓的“信任的互联网、价值的互联网、秩序的互联网”。但这种“美好的”比特币区块链体系，脱离现实世界根本无法独立存在，比特币如果不能与现实世界的法定货币兑换，就难以实现其价值。而要实现比特币区块链的“价值”，就必须与现实世界相连接，使比特币区块链体系成为以法定货币代表的社会财富转移的一个中介环节或过渡阶段。

在比特币必须与法定货币兑换，必须加入网络交易平台等辅助环节才能发挥功能的情况下，就使得比特币区块链区去中心、去中介等特性反而可能产生严重问题。放在现实世界的大环境看，其货币资产的转移如果通过比特币区块链体系运行，实际上是增加了中介环节，而不是去中介，而且由于比特币体系高度匿名，刻意规避监管，难以充分满足反洗钱、反恐怖输送等方面的要求，反而可能产生很多新的严重问题，很多有关比特币、区块链的说法都难以成立。

比特币的痛点

不知不觉中，过于追求完美的比特币区块链体系脱离了现实，走向了封闭，这恰是比特币区块链的根本问题所在。

1. 比特币区块链难以建设一个去中心、民主平等的社会

比特币圈无法实现其宣扬的“去中心”“平等民主”局面：底层代码维护的核心团队与参与挖矿和运行的主要力量能够发挥更大影响力。受计算机运算能力的影响，比特币的挖矿和获得，并不是像宣传的那样人人都有平等的机会，竞争的结果，使得挖矿获得比特币的机会越来越集中到少数算力强大的矿池或节点上。

2. 比特币区块链“去信任”“去中介”的点对点交易是有严格条件的

在比特币体系内部，交易双方无须提供身份信息并得到足够权威的印证，即可进行直接的交易形成所谓的“信任的互联网、价值的互联网、秩序的互联网”，但这都隐含了一个重要前提，就是所有的人都参与到同一个比特币区块链网络平台；平台上运行的只能是比特币，而不能是比特币以外的其他资产或价值；比特币从其产生的源头就得到网络系统严密的验证和记录，难以造假或篡改。因此，比特币需要在一个“干净”，基于比特币区块链网络平台的环境。

如果交易双方不足同一个网络平台上注册，不同平台的规则又不统一，这种点对点交易就难以实现。而现今数字货币鱼龙混杂，平台众多，使得比特币区块链难以实现广泛含义上的点对点交易。

3. 比特币区块链只是比特币产生和汇划的封闭系统，实际功能有限

现实世界的资产或价值很难推送到这一体系上运行。即使能够推送

上去，如果没有一套非常严密的线下印证体系，确保所推送资产的合法性、真实性、准确性，一旦有虚假的东西推送到比特币区块链体系上，其运行体系再严密都无法逃避“以讹传讹”的结果。如果严格局限于比特币区块链体系内，基于比特币产生的规则，它甚至连用比特币发放贷款或投资应该产生的利息或红利都解决不了，将严重影响金融的发展和功能发挥。要发挥比特币体系的功能，就必须将比特币兑换成法定货币，并将比特币体系作为现实世界资金汇划的一个过度环节或新的中介环节。而这就需要比特币体系与现实世界实现连接，从现实世界大环境看，其结果不是去中介，而是增加了中介。

4. 比特币网络交易平台并不是比特币体系内在组成部分，不是去中心的

随着比特币等网络数字币与法定货币兑换需求的扩大，出现了专门的网络数字货币交易平台，为数字货币兑换，特别是为那些不愿意参与挖矿，却愿意参与比特币等数字币炒作的人提供专业服务。但是，这种与法定货币的兑换或交易的专门平台，只是比特币区块链体系的外挂系统。这些交易系统并没有完全受到比特币区块链体系的约束和保护，也没有得到金融监管足够的有效监管，交易平台的运行及其存放的资产是存在风险隐患的。所以我们要明确一个概念，比特币区块链体系和比特币交易体系是两个不同的概念，而现在很多人却总弄混着两个概念，给了投机者收割韭菜的机会。

5. 比特币区块链体系过于强调“去中心”，反而影响其效率、成本与监管

比特币区块链体系要实现“去中心”，就需要大量外部计算机接入

并共同运行。这样，加入的计算机节点越多，在比特币的挖矿与转让需要全网广播、验证、分布式处理等的难度就越大，其“挖矿”过程需要消耗越来越大量的能源，甚至会造成环境污染。法定货币外挂交易平台的处理程序繁杂、效率很慢、成本很高。更重要的是，如果加入比特币体系这样一个完全抵制或规避国家监管的中间环节，法定货币的流通就可能完全失控，被恐怖分子、毒品贩子、网络黑客、金融骗子等利用。

6. 过于追求去中心化、充分的民主自由，实际上就会脱离现实

在人类社会中必然存在个别利益与公共利益的矛盾和统一，只有在公共利益最大化的情况下才能使个别利益最大化得到根本保障。在当今世界仍然是以各个国家主权独立和自治为基础架构，国家之间相差悬殊的情况下，设想建立一个“去中心”、无政府的网络世界和超主权的世界货币，完全摆脱现实世界国家法律的约束，去建立一个去中心化，独立于国家概念的网络平台同样是不现实的。

7. 比特币难以成为真正的货币

比特币在设计上就是模仿黄金，总量限定，而且挖矿越来越难，产量分阶段逐步减少，以期消除人为过多投放的可能性，并为比特币升值创造巨大想象空间。但高度模仿黄金设计货币体系的思路，本身就是货币设计理念上的一种倒退，是不能成立的。黄金等贵金属曾经长时间作为货币，但正因为其强烈的自然属性，使其供应量难以与经济社会发展的实际水平，特别是可交换社会财富的规模相适应，容易造成日益严重的通货膨胀，或者是通货紧缩，币值剧烈波动使货币难以有效发挥价值

尺度的功能，最终必然被可以进行数量调控，能够保持货币总量与可交换社会财富规模基本吻合（社会物价综合指数相对稳定）的主权货币或法定货币所取代。黄金退出货币舞台是必然选择，不可能再退回去，重新成为货币。

同时，比特币尽管模仿黄金，但仍不可能成为真正的“数字黄金”。黄金作为一种受人追崇的自然物质（贵金属），其本身是具有真实使用价值和价值的。但比特币却纯粹是一串网络系统产生的加密数字或数码，并不是自然物质，一旦离开比特币体系，就没有任何价值。

8. 网络数字币 ICO 存在更多问题

随着区块链及比特币、以太币等网络“数字币”的升温和价格上涨，也催生了很多“区块链创业公司”及其相应的山寨币或分叉币。这些“区块链创业公司”由于概念新、时间短，经营业绩难以达到 IPO 的监管条件，于是，在一些参与“炒币”的资本运作者的推动下，出现了专门以网络数字币首次发行并募集热点网络数字币（主要是比特币、以太币，而非法定货币，从而规避非法集资风险）为主要特征的 ICO 集资方式。但这些 ICO 大多没有得到监管部门的有效监管，其实际运行存在很多暗箱操作、内部炒作，虚假宣传、恶意传销的成分。由此可见，ICO 的出现影响极大，看似为区块链创业提供了新的融资方式和渠道，实际上重点是用于炒作数字币，面向公众募集资金（而非私募），但严重缺乏必要的规则和监管，很容易产生非常严重的金融和社会问题，甚至将区块链的发展引入歧途。

区块链的发展应跳出“比特币区块链”范式

1. 唯有跳出“比特币区块链”的思维和范式，区块链发展才能实现自我“救赎”

必须清楚地看到，比特币只是区块链应用的一个成果，“比特币不等于区块链”。区块链是多种技术的集成，比特币只是区块链多种技术整合的一种形式，还可以有不同技术的多种组合形式。因此，区块链的发展必须跳出“比特币区块链”的思维和定式，不必过于追求理想化，转而脚踏实地、实事求是，注重运用相关技术解决现实世界的实际问题，并在实践中不断改进和完善，充分发挥区块链的积极作用。

2.“去中心”只是比特币区块链的特点，并不代表所有的区块链都必须是去中心的

去中心，并因此需要吸引大量外部计算机加入，形成计算机“公有链”共同运行，不一定是区块链的必要内容。区块链也可以在私有计算机群上中心化独立运行，或者吸引一定的合格参与者加盟，形成由加盟者计算机组群共同运行的半中心化“加盟链”运行体系。

3. 比特币等网络系统内生“币”，与区块链并不是密不可分的

如果不追求“去中心”，就不一定需要像比特币这样的激励机制，就可以转变区块链的运行重心：从聚焦于“挖矿”产生“数字加密货币”，以及这种“数字资产”的转让认证和记录上，而放弃对资产合法性、真

实性、准确性，以及交易双方身份的真实性、准确性的验证，形成完全脱离现实世界的网络封闭环境，转变为强化对资产合法性、真实性、准确性以及交易双方身份的真实性、准确性的验证，而不再需要开发和运行系统内生数字币（“虚拟资产”），进而将区块链融入到现实世界之中，真正解决现实世界的实际问题，并充分满足国家法律和监管要求，避免成为非法交易、恐怖输送等的工具。

总之，完全拘泥于“比特币区块链”范式，并无多大价值和发展空间，区块链的发展需跳出“比特币区块链”的思维和范式。

（本文是中国银行原副行长王永利在清华大学的演讲，略有改动）

区块链的特性

区块链的价值

我们人和人之间最核心的经济关系就是交易，但在没有区块链之前，我们所有的交易活动，怎么样保证交易双方真实可靠的完成一笔交易？两个人之间互相不信任。比如说我们在互联网上网购，一定要有支付宝。

2003 年淘宝出来以后，首先阿里巴巴觉得没有一个支付宝，不可能在互联网上把电商做下去，需要一个支付宝担任信任中介，确保交易完成。现在我们刷的银行卡，如果不是银行发的，商户是不敢收你的，银行是一个信用的中介。在区块链出来之前，任何的交易活动都需要有一个中介，没有一个中介，不可能两个人在缺乏第三方的情况下，两个陌生人达成一笔交易。

区块链干的事情就是信任的机器。倒过来说用一台机器人取代了一个信任中介的作用，用一套数学算法确保两个陌生人不借助于第三方的情况下，把一笔交易，不管是金融的交易或者是商品的交易能够完成。这就是区块链的最核心、最本质的东西，区块链是信任的机器。

区块链是去中心的。要把区块链中间的中介去掉了，在经济交易活动当中，所谓的去中心无非有这么几个意思：

1. 我们在完成一笔交易的时候，不再需要第三方，这个第三方就是一个中心。

2. 我们在开展经济活动的时候，需要有一个组织，我们有这么多的公司，可能大部分来自于各种各样的商业机构、商业组织，但是在区块链上所从事的所有经济活动，不再需要像公司的这种制度，不再需要这样一个组织。

3. 不再需要这样一个商业机构，我们很熟悉的这样一个组织形式来帮助我们完成经济交换活动，来完成各种形形色色的交易。

4. 除了不需要这个组织之外，任何的经济活动都有可能，或者说在数字世界里面的数字经济活动都不再有一个，它的激励机制不再是一个中心化的机构建立起来的。

我们每个人为中心化的机构服务，那么这个中心化的机构给我们工资，给我们奖励，给我们职务，来激励我更好地为这个事业服务，一定有一个中心化的机构来建立这样一个激励机制，但在区块链上面这个激励机制不是由中心化的机构来建立。

从三个层次了解区块链

第一个层次，区块链最底层的一个层次，实际上是分布式网络，区块链是架构在分布式网络技术之上的一个应用。

分布式网络对于区块链来讲，最主要的作用就是解决了点对点通讯的问题。

第二个层次，在分布式网络基础上，如果我们给它加一层东西，加一层密码学的账本体系，这个分布式网络就变成了分布式账本。

密码学的账本体系和我们现在所碰到的金融账本体系，比如说在银行的开户等等是非常不同的。最大的一个不同，银行的账户体系只能记录你的资金，但是密码学的账户体系能记的东西比这要多，不仅可以记你资金的状况，可以记信息，甚至可以记跟你身份有关系的所有数据都可以在这个账本体系上建立起来。

更重要的一个区别在于密码学账本体系，它的开户和金融账户体系开户完全不同的。如果你要去开立一个账户，一定要做 KYC，银行一定要辨别你是好人还是坏人，你的信用等级是多少，我能最大限度地为你提供多少金融服务，所以它需要很高的成本，因为你要去辨别谁是好人谁是坏人，辨别好人之后，你还要对他信用作分析。

密码学账户体系，没有这个 KYC 的过程，任何一个人不需要借助第三方，就可以在比特币的区块链上开无数个账户，没有人来辨别你是好人或坏人。但不管是银行账户体系还是区块链上的密码学上的账户体系，但所要达到的目的是一致的，这个目的就是要从事交易，基于这个账户完成。银行需要有一整套的人员、模型、机构、过程来辨别你金融服务的请求是不是应该得到允许，是不是可以让你完成。

区块链没有这些东西，它有的是一套数学算法，一套数学算法，建立了一套网络上的规则，这套规则依照它做，那么所有的坏人不可能在上面作恶，如果不依照这套算法做，那么你不可能实现你想要达到的目的。这样两套账户体系，就知道谁的成本高，谁的成本低。运行一套数学算法，一个人和一万个人同时运行它，边际成本不会增加，但如果银行来辨别一个人的金融服务的请求，你服务一个人和一万个人的边际成

本一定是增加的。

第三个层次公有区块链，或者叫比特币区块链。加了两个什么东西就变成了公有区块链或比特币区块链了呢？第一个发行数字货币的货币体系，这个数字货币的货币体系和我们现在的货币体系是完全不同的两个东西，数字货币不是我们现在的货币，更加不可能是法币，它是一个很特殊的东西。

两个之间最大的区别在哪里呢？我们现有的货币，即使完全电子化了，它再电子化，也只是存储了你的一串数字，你的微信、支付宝钱包里，你的银行账户里面，无非里面是一串数字。数字货币不是数字，是计算机程序。

如果你有两个比特币，那你有的不是数字，是一段代码，是一段计算机程序，它不是简单地从纸币变成了电子，从物理形态上，我们有铜、金银，后来变成了纸币便于携带，再后来为了更方便携带，于是变成了电子化，那只是物理形态上的变化。而到数字货币，是根本性质发生了变化，它变成了一段计算机程序，因为它是程序，所以我们可以赋予它智能合约。

从技术发展来看区块链

技术发展趋势，技术发展进程的角度谈区块链，现在行业里头分成区块链 1.0、区块链 2.0、区块链 3.0。

所谓区块链 1.0，最典型的代表就是 2009 年 1 月份上线的比特币区块链。区块链 1.0 最主要的，最核心的贡献就是建立了一套密码学的账本，提供了一套新的记账方法，和我们以前所熟悉的复式记账法不一样。

但它有一个缺欠，比特币区块链，它所有的规则是事先写好的，没有人可以在比特币区块链上修改任何规则，你只能用它，而不能在它的基础上再去发展，说我写一些新的代码，是不是能够用比特币区块链干一些别的东西？对不起，不允许的，不支持别的开发，这是区块链 1.0。

到 2015 年的 7 月份，有一个新的公有区块链，叫以太坊，正式上线。以太坊区块链和 1.0 区块链比较起来，最大的不同，就是别人在以太坊区块链的基础上做其他的应用开发。你可以用我作为底层做你的事情，这是它和 1.0 最大的不同。同时以太坊区块链有一个非常伟大的计划，它希望把以太坊区块链建成世界计算机，建立一个全球性的大规模的协作网络，所有人都在以太坊区块链上做计算、运用，这个计划到目前为止还是在进行中，没有能够完成。

同时因为它允许别人在以太坊区块链上做一些其他的应用开发，因此它提出了一个叫作智能合约，支持大家在上面编智能合约。智能合约不是合同，智能合约就是一套保证你的合同能够在不借助于第三方的情况下得到执行的计算机程序。合同是合同，合同需要律师，需要现实世界当中的法律，依据法律来签的，智能合约不是合同，是一个计算机程序，这个计算机程序能够保证你们俩合同签完之后，谁都不能反悔，只要条件达成，这个系统会自动扫描大家商量好的一个网站，来判定谁赢谁输，自动触发支付的条款，这是区块链的 2.0。

因为性能上不能支持大规模的商业应用，区块链技术往前发展，2018 年开始进入到区块链 3.0 的阶段。3.0 没有其他技术上大的突破，3.0 要解决的就是大规模商业应用，在技术上，在性能上要能够支持大规模的商业应用。

从商业角度来看区块链

从商业的角度，从经济的角度来介绍区块链跟我们现在的经济，现在的商业有什么关系，它有什么价值，能干什么。

有人说区块链经济才是真正的共享经济，为什么呢？因为它没有股东跟你分利润，任何一个人加入这个网络，就可以得到应该得到的那份价值，均分给所有的使用者，那才是真正的共享经济。

所谓的加密经济学，因为区块链技术等等很多新的东西，可能对我们很熟悉的基于工业经济的很多经济规则要进行重构。在工业社会，要让生产到达最高效率，我们需要流水线，我们需要大规模的生产，我们需要公司这种组织形式，没有这些生产组织形式，我们经济不可能达到一个最好的效率。可是在区块链的世界里面，在区块链的经济体里面，这些统统都不需要了，这就是加密经济学正在研究的问题。

比特币区块链就是一个分布式商业的最伟大的实验，所有的产权是开源的，所有的组织机构是非盈利的，没有股东，没有董事会，没有管理层，什么都没有，是一个八无公司，但是它运行了九年时间，每秒钟都在发生着交易、汇兑、支付，没有出现过坏账，系统没有出现过宕机。

任何中心化的系统，即使是金融机构的系统，每年一定会出现系统宕机，这是我仔细请教过 IBM 的，你们的技术能不能做到像比特币区块链一样的，不出现一秒钟的宕机？他说不可能的，为什么比特币区块链可以做到？分布式网络。由谁在管理它吗？没有人管理它，自己花钱买了服务器，跑到四川找一个电费便宜的地方，为比特币区块链工作，没有人组织他们，为什么来？因为有利益，有很高的利益，有一套激励机制。

所以分布式商业，不是取代我们现有的公司，也不是取代政府对市场的管制，在市场失灵的时候，政府的管制是必须的，只是说在这两者之外，会多一个东西，为什么会多一个东西？

多出来的自组织分布式商业在以前就有。为什么突然变成一个显学？因为我们的经济越来越数字化，在互联网上，在数字世界里面有很多东西原来的规则，原来的机制，原来的理论不够了。

所以未来，所谓的市场机制、政府管制和自组织治理这三者会相得益彰，它不是革命，也不颠覆，也不是谁取代谁，也不是政府没有了，政府还是政府，在这两者失灵的时候，政府的管制有独到的价值。

同时，企业也有企业的价值，但是在数字世界里，可能有一套新规则来治理我们越来越数字化的经济，这个里面很多地方更有效的是分布式商业，是自组织。

（肖风，中国南开大学经济学博士，万向控股有限公司副董事长、万向区块链股份公司董事长兼总经理、万向区块链实验室发起人）

区块链的核心：“共识”

区块链最近半年成了妇孺皆知的事情，如果你对 20 年前的互联网有所记忆的话，我会说，区块链比 20 年前互联网的崛起要猛烈一千倍、一万倍。

上至总统、央行行长、银团、财团以及各大银行，下到每一个企业家、创客，甚至每一个年轻人，以及关心互联网的人，都绕不开区块链这个词。

区块链的核心是“共识”，尽管这个词听起来非常干硬，但是其内涵的思想，值得研究。

为什么要把“共识”带一个引号呢？这就说明，在这个共识的行业中，还有大量的噪音和语焉不详的事情。

共识正在孕育生成的过程当中，千万不要用寻找答案的心态来看待区块链，要一个猛子扎下去参与其中。

四个字解释什么是区块链

现在，区块链讲得很专业的人很多，但是讲得很通透的人不多。昨天在中科院参加一个区块链的论坛，我认为论坛上的白硕老师是在国内

把区块链讲得最通透的。

三年前，白硕老师就在用 4 个字解释了什么是区块链？就是“记账 + 认账”这四个字。

我们当今所有的经济活动，都对应着一个账户体系，不管是个人银行账户，还是企业的财务账簿。

账户体系几乎是我们所有经济活动、生产活动、日常生活的一个必要的数据记录体系，它反映了经济活动最基本的单元，比如买卖、交易、缔约、履约，这些事情。

传统的账户是什么特点呢？传统的账户是由专业的会计师来处理，使用的是经典的复式记账法。

那么我们说区块链是一个记账体系，是什么意思呢？这就意味着用数字化的方式来记账，把账簿划分成一个又一个的碎片，每一个碎片叫一个区块。

就好比我们账簿划分成科目，划分成分类账、总账等一本一本的账目，每一个区块链记录着账目交易的往来。

这有什么新鲜之处吗？

第一，这个账簿不是存储在你家的柜子里，而是存在一个“不知道什么地方”的地方，叫分布式存储。

第二，这个账簿是谁来记的？不是会计师，而是参与到区块链的整个社群中，所有的人一起来记。

第三，这个账簿里包含哪些内容呢？过去的账簿可能只包括你的进货、销货，只跟你有关，但今天区块链的账目，包含了凡是在区块链这个社群上参与的所有人的所有账户。

所以它是一个 P2P 的分布式网络，这就是记账的部分。

那么区块链的账簿既然记了账，我们怎么认这个账？比如区块链的真实性、可信、不可篡改、不可抵赖，它会建立起相互信任的机制，也叫共识机制。

区块链的革命性在哪里呢？它打破了过去账户只是私人和私人之间私密这样的一个狭隘观念。

我们可以建立起一个共同的账户，凡是参与到区块链这个联盟或者社群的所有人，都有权利享受该账户的基本信息。

我们需要思考的是：为什么要这么做？这么做对整个社会的商业逻辑、社会结构的影响在哪里？（至于说里面很多的技术构造、技术原理，可以暂时不明白，但一定要知道这件事情已经巨大无比。）

区块链发展到今天，已经有了 10 年的铺垫。

2008 年有一个神秘人物中本聪，发明了比特币，2009 年，他发出了一块比特币，从此一发不可收拾，今天比特币的价格，大约是 5 万人民币一个。这是 10 年的故事。

在 5 年前，一个年轻人发布了以太网的智能合约，后来成功募集了 1.62 亿美元，同时也促成了人们由比特币的概念向区块链概念全面认知的转变。

比特币是一种具象的数字货币，它的着力点是货币，但它的底层技术是区块链技术。在 5 年前，区块链和比特币这两个概念相对分离，后来这种底层的支撑技术，越来越被大家看好，原来它可以干更多的事情。

3 年前，世界范围内成立了大量的区块链联盟，包括各种银行、国际组织成立了联盟，包括基金会等 160 家机构联合成立了超级账本，这就意味着一个新的时代的开启。

稍微总结一下，至少你要掌握三个基本概念是：

第一，区块链和比特币不是一回事情。

第二，区块链是一个基层的技术。有人把它描绘成下一代互联网的技术设施，是一种基础设施或一种基本的协议，比如支付的协议，结算、清算的协议，交易的协议，甚至社交的协议，都在区块链上。

第三，最近的半年到一年中，发了那么多的区块链代币，出现了火爆的 ICO，这是怎么回事呢？

区块链的世界分成了两个部分，第一个叫币圈，第二个叫链圈。问题就在这里，大量的人在炒币或在发个人货币。而另外一拨人在做基础设施，研究它的加密算法、交易算法、隐私保护算法等等，夯实它的基础设施的基础。

币和链是什么关系呢？迄今为止，我还没有看到统一的共识，我个人的观点是：一体两面，什么意思呢？币是区块链应用的表征，而链是区块链的基础设施。

这个世界正在发生什么深刻变化？

今天不管是哪一个行业的人都需要瞪大眼睛，看看这个世界到底在发生什么深刻的改变？

那么世界到底发生了什么深刻的改变呢？我讲三本书。

第一本书：1980 年代的《合作的进化》。

密歇根大学的罗伯特·阿柯塞罗做了两个实验，非常残酷地告诉我们一个结果：人的现实生活中，最终的结果往往是彼此背叛，才是双方各自最优的选择。

但他有点不服气，再研究一下，我们到底能不能在自私的个体之间相互博弈，达成合作呢？

合作是人们埋藏在心底几千年来多么“伤感”的一个话题，大家真的希望合作，每个人都特别希望这个世界与人为善，都特别希望能够和谐相处，有利共享，有难同当。

但是这个世界依然弱肉强食，得到的最佳策略，依然是“一报还一报”。

第二本书：是诺瓦克出的一本书，叫《超级合作者》。

人真的是自私而生存的吗？难道合作就不是人的天性吗？所以他研究物种的群体行为，研究物种和物种的彼此之间互惠行为。

用日常生活的事例“挠痒痒”来讲，我给你挠挠背，你也给我挠挠背。很多生物学家、动物学家研究物种的时候，发现挠痒痒和互相梳毛，是上百万年生物演化过程中，遗存下来非常重要的新社会行为。

第三本书：是纽约大学詹姆斯·卡斯的《有限和无限的游戏》。

詹姆斯·卡斯同样关注人的合作与竞争问题，他分析了几千年来，人类社会演进过程中的各种博弈，并把它分成两类：

第一类就叫有限游戏，我们知道“game”这个既是游戏的意思，又是博弈论的名词。

他发现人类史上，几乎所有的“game”都是有限游戏，说白了就是有输赢，这件事情用我们的网络用语，我把它叫“作”，我们作了几千年。

不管你奋斗的目标是什么，不管你对价值观的判断怎么样，也不管你世界观的组合怎么样，你会发现，最终的结果非常令人遗憾：

几乎没有一个人能逃脱一报还一报的策略，自私的假设，以及零和

博弈的有限范畴。这是一个多么令人伤感的话题。

第二类则是无限游戏，就是让游戏一直继续下去。

两年前的 AlphaGo 把李世石打败，很多家长纠结要不要孩子学围棋。现在机器人都这么发达了，孩子学围棋还有意义吗？

聂卫平说："AlphaGo 让我重新认识了围棋，不仅仅停留在过去的规则上面，要学会玩无限游戏。"

在这种情景下，我们需要反思的是：迄今为止，我们所建立的合作原则，大致来讲，逃不出过去轴心文明的思想范畴。

而区块链的伟大意义就在这里，在没有区块链之前，不管我们用互联网做多少创新，我们发现它的思想底座并没有超越。

轴心时代是德国的哲学家雅斯贝尔斯的术语。轴心时代遗留给我们关于这个世界最好的解释系统是什么？就是己所不欲，勿施于人。

雅斯贝尔斯说，历史按纵向发展成四个部分：传说和神话中的"普罗米修斯的时代"、古代文明产生的时代、轴心时代以及科学和技术的时代，他认为轴心时代是最重要的。

在轴心时代里，各个文明都出现了伟大的精神导师——古希腊有苏格拉底、柏拉图，中国有孔子、老子等，他们提出的思想原则塑造了不同的文化传统，也一直影响着人类的生活。

所以我们今天的商业规则、社会伦理，以及政治法则，并没有超越己所不欲，勿施于人的法则，用博弈论的话就是"一报还一报"的策略。

换句话说，今天人类对价值判断、对伦理道德、对社会的认知，依然没有超越 2500 年前的先哲。

区块链的伟大意义也就在这里，区块链要在这个意义上，让世界重新启动。要重新理解合作，重新把合作建立在一个坚实的技术驱动之上。

这是一个非常伟大的创新，需要非常伟大的勇气。

因为我们过去一报还一报的合作，带来的社会代价非常之大。用我的话说，文明的演进史就是两件事情的构成：

第一件事情就是不停地吵架，因为我们彼此要说服对方。某些先哲总认为自己 Hold 住了世界的真理，不是这样吗？哪一个先哲不是言之凿凿地说，自己找到了真理，然后就开始说服大众。

第二件事就是不停地打架。彼此说不服，怎么办？打架啊！这种说法简单了点，粗糙了点，但我个人认为，从症状来说，似乎也靠谱。

“共同认可”还远远不够

三千年文明就是吵架和打架的历史，但背后掩盖了一件事——共识，什么共识？我们非常容易达成这样的共识：我们以为共识就是大家共同认可，对，但不够。

举例来说，从小骑单车、长大开车的人，我想你在父母的叮咛，教练、老师的指导，以及社会的塑造下，都知道一个基本的规则：第一，不要撞别人，第二，不要被别人撞。请问这是不是我们共有的知识，应该是吧！

那有这样的共有知识，这个世界就不发生冲撞事件吗？当然不是！请问，什么地方出了差错？

当我们不撞别人，又不被别人撞的时候，这只是达到了书本上的共有知识，但还不能保证不撞。

你还要必须知道别人是不是准备履行这样一个共有知识。也就是你必须知道别人知道什么，反过来，别人也要知道你知道什么，是不是这

样的。

开车在路上，当你要转弯、并线的时候，遵守规则的人都知道打灯，但会不会有一部分人不打灯就并线？

如果对方看到你要并线，给你留出一部分空间，让你并进来。这就是我知道你知道什么，所以让你也知道我知道什么。

所以共有知识，一定是我知道你知道什么的同时，你也应该知道我知道什么，是不是这样的？

这样就能保证这个世界和谐吗？不！因为还有第三层级：我要知道你知道我知道什么，你也要知道我知道你知道什么，是不是这样的？

所以当我们打灯的时候，一些新手司机就害怕后面那个车是不是踩刹车？通过这样的分析，我们知道，还有第四、第五层级。

所以，不要把我们的合作，建立在这样一个脆弱不堪的基础之上。这意味着什么？意味着我们可能需要重新构建这个社会的基础。

互联网的一次升维旅程

维纳写过一本书《神奇的单马车》讲道：以往我们追求每一个马车要经久耐用，但他从另外一个角度思考，什么是一个好的马车？他提了一个问题：

一辆好的马车，是怎么坏掉的？坏掉的时候，是车轴先断裂，还是车头先坍塌？还是车座先倒下？

所以他说，一个真正好的马车设计，是这个马车坏掉的时候，所有的地方都同时坏掉。

这又是一个乌托邦的情怀，但这个情怀的背后，展示了对一个好设

计的一种信念：

好的设计，并不是说每一个环节都要设计得棒棒的，而是所有设计的匹配要刚刚好，我把它叫作恰当设计。

我们今天的社会，虽然从工业文明向信息文明演进，但是我们依然沾染着大量的工业文明的遗迹，这个遗迹就是追求更高、更快、更强，更有力。

它应该是单马车描绘的这样刚刚好的社会，但非常遗憾，对这个社会刚刚好的期待，在过去三千年里面有太多的圣人先哲提出来，但就是无法实现，原因何在呢？

原因就在于底层技术不支持，在于我们过去的生产方式是落后的生产方式，组织方式是落后的组织方式。

我们过去是一种先生产、消费，后付费的方式。传统的记账方式下，今天发生的交易记进去，进入账户之后，聪明的企业家一般不关心再现金的流动、固定资产的周转、应收账款回笼的速度，因为这是一种串联的方式。

但是在“刚刚好”的社会里，边生产边消费的情形下，需要告别一种思维方式：就是我们过去的确定性思维方式。确定性思维方式是轴心文明以来，我们养成的一种基本思想框架，我把它叫作“定数崇拜”。

普利高津有一本书《确定性的终结》讲到确定性世界的终结，确定性世界的代价有：高昂的交易成本、履约成本、多次重复博弈。

老话说“日久见人心”，但是大家要付出多少昂贵的成本？对一个人来说，要付出几乎一生的成长代价，所以后悔药吃不得的原因就在这里。

可是，我们对这个事情太熟悉，以至于熟视无睹，我们不觉得这件事情可能发生变化。

但区块链来了，区块链就是真正改变信任的机制，区块链打的是这样一个巨大无比的赌：陌生人在互联网上能不能一次就达成信任？

互联网上成千上万的人在网络上连接，互相接触、互相交往，如果还像过去工业时代那样，就叫火车站模式。什么叫火车站模式？

火车站模式就是：比如我今天卖给你茶叶蛋，可能一辈子再也不会见到你，于是就产生了各种欺骗，各种尔虞我诈。但是在互联网，恰好陌生人的交往是常态。

这种情况下，如何保证陌生人一次就建立信任？这不是要通过道德说教，而是通过漫长的塑造才有可能达成。

今天区块链让我们已经极其接近这个社会底层的构造，陌生人的一次信任，我把它叫乌托邦。在这种情形下，区块链正在让这个乌托邦建立在非常坚实的基础之上。

更重要的一点：区块链把财富的生产和财富的分配平衡地放在了一个巨大的账本之中。这个巨大的账本对所有参与区块链的人，是公开透明的，同时又是加密保护隐私的。所以财富的生产和分配，同时进行，这是它的伟大意义。

所以，区块链让这个社会不再追求更高、更快、更强，而是追求刚刚好，就是达到某种程度上，会说“够了”，它是一个有“够”的社会。在这种情形下，人的创造力才能得到无穷的释放，才能进入到艺术的、创新的、创造的那种氛围当中。

所以区块链让我们每一个人达成自己的甜蜜三角，这个甜蜜三角就是指所能、所愿和所为之间的良好匹配。

每一个现实中的人都有种种遗憾，往往是所愿非所为，所能非所愿，或者所做非所能这样的一种剥离带来的。

说白了就是，由于种种历史原因，使他今天所做的不是他喜欢的，或者今天能干的，恰恰是他不喜欢的事情，这是对人、对生命的巨大浪费。

而区块链让我们坦然地放下自己，让我们尽快地进入到生命和生命共生演化的巨大网络之中，坦然地接受生命能量的相互支撑流动，坦然地用自己的生命意愿去接触所有的生命意愿。

不是为了追求价格的尔虞我诈，也不是为了追求财富的单边增长，而是追求共同的快感，共同的快乐。

区块链就是将每一个人内心深处的甜蜜三角用坚实的算法逻辑技术支撑、连接起来。

这难道不是一个伟大的社会吗？这难道不是一个伟大的画面吗？所以有人说，区块链开启了互联网的一次升维的旅程。

不要把互联网理解为就是一个网站，或者你手机上的一个流量，互联网已经进入到了价值网络，这个价值网络，是每一个人都可能参与其中，每一个人都可能恰当地表达自己，每一个人都可以恰当地在价值交流、互换、流动的过程中，享受到价值创造的当下快乐的这样一种氛围。

听上去是有很多的乌托邦色彩，但是技术在扎扎实实地进步，算法、隐私保护、人工智能在扎扎实实为这个社会底座拧上更多的螺丝，安上更多支撑的桩柱。

所以今天在这样一个论坛上跟大家分享区块链只有一个理由，就是每个人都不能与这样巨大的时代变革无关。

（本文是财讯传媒首席战略官段永朝于 2018 年 3 月 29 日在第二十三届中国服装论坛上所作演讲，略有改动）

二、区块链的价值

区块链是一种分布式数据库系统，特点是不易篡改、很难伪造、可追溯。区块链记录发生交易的所有信息，一旦数据进入区块链，即使是内部工作人员也很难在其中做任何更改而不被发现。这个特点决定了其与互联网应用密不可分。应用场景越大、越丰富，区块链技术和产业的发展就会越快。

——北京航空航天大学数字科技与区块链实验室主任　蔡维德

为什么要用区块链?

金融和科技的结合称为 Fintech。而 Fintech 的核心就是区块链。为什么？因为区块链技术从诞生之日就自带金融属性。而其他的 Fintech 技术，例如大数据、云计算、人工智能，与金融只是结合。金融并不是这些技术的原生属性。

区块链这个词很新，我们基本把它当作一个后互联网的新技术来看待。从大数据到区块链，金融业的未来已来。2015 年有一个叫 R3CEV 的区块链创业公司成立，这个创业公司在短短的三个月时间内，就联合 42 家主要的银行和金融机构参与，它的目标就是要建立银行的联盟，而区块链则被认为是下一代更加安全有效的连接工具。

据不完全统计，全世界 90% 央行都在积极探索数字货币和区块链技术，包括中国央行。除了央行外，还有一个重要的推手——十三五规划。十三五规划是国家级的战略规划，区块链这样一个新兴的技术在短短一年之内就写入了国家战略规划。区块链是一个相对来说比较复杂的计算机技术，融合了计算机网络、数据库、操作系统、密码群、分布置系统等技术，综合了很多计算机的监控和数据。

我们把区块链定义为是价值互联网，现在讲互联网更多是在讲信息

互联网，未来要创造一种价值互联网，方便人们很方便地在价值互联网上形成资金、资产的转移。现在的网上银行、手机银行、支付宝、微信等是否已经实现了价值转移？它确实是一种价值转移，但问题在于它们都是以相对中心化的方法实现价值转移的，很难用去中心化方法，这恰恰就是区块链最大的价值。区块链是一个纯的技术，技术会更加中立，它是一种通过技术手段来确保创造信用的方法。这是为什么很多国家、央行想积极探索研究区块链，用区块链发行数字货币背后的原因。也有人会把区块链定义成分布的、加密的技术。

区块链到底是什么样子的？区块链由数据块组成，数据块又分为区块体和区块头。区块体里面打包了一堆的交易，每一个区块的交易数不可能完全一致。区块头由一系列摘要性技术构成，其中一个很重要的技术是本区块的摘要 Hash，摘要 Hash 跟下面的数据具有一一对应的关系，因此，当下面的交易数中间任何一个数据发生改变的时候，它的摘要 Hash 就会发生改变。正是由于摘要 Hash 的存在，前一个数据块和后一个数据块之间就形成关联，在整个区块链之间想要更改任何一个数据，就会形成一种连锁反应，从而确保更改数据是非常困难的。事实上在很多区块链节点中间会包含一千个甚至一万个节点，这些节点之间是相互备份的过程。

现在的互联网都是信息互联网，而我们把区块链称为价值互联网，因为在互联网没发明之前，大家通过电视、报纸、传统媒体来传递信息，传递信息是一种相对自由的，相对中心化的方式，大家看到的信息都是差不多的，而由于互联网的出现，原来信息传递的方式完全改变。互联网的长项恰恰也是它的弱项，因为信息的传播不需要任何代价，篡改数据非常容易。当进入价值互联网时，区块链可能会形成这样一个底层的

技术：一方面它保证了像互联网一样在全球范围内高速度传播，另一方面又杜绝了拷贝、粘贴问题，所以区块链会成为价值互联网的基础。

如果我们把基于互联网的和基于区块链的金融服务来做一个对比，会发现上面两层基本是一样的，提供的都是对中端用户的金融服务。但是基于互联网提供金融服务，一定是有牌照的金融机构或者值得信赖的金融机构，只有通过这种信用机构本身的信用为其服务进行征信，才敢用阿里巴巴的支付工具。但是区块链不需要任何一方、组织机构提供这种信用，因为它自身通过技术确保了其信用。

再回到互联网时代，大家会问为什么要上网？在线下生活好好的为什么要上网？什么东西可以上网？现在，如果听过区块链就一定会问这几个问题，为什么要用区块链？什么东西可以用区块链？以及我们如何随地使用区块链？

区块链显然可以应用在金融上，一个很重要的应用是以区块链为基础的票据系统。中国一年票据交易量是 120 万亿，GDP 是 70 万亿左右，通常是 GDP 的 1.5 倍。因此，票据数量非常多，尤其对于小微企业来讲金额比较小；服务成本非常高；结算票多、融资票少；客户非常分散。同时还有一个很重要的痛点是流动性差，因为很多票是中小银行签发的，中小银行相对于大银行来说，信用度相对低。为了解决这个问题，我们创造了一个系统，这个系统以区块链为基础连接中小银行，构建银行联盟内的信用生态环境，用高效快捷的互联网方式为中小微企业提供票据融资服务。

其次，我们用区块链进行收益权登记。第一，通过区块链不可篡改性、唯一性，可以设立一个唯一的数字凭证，这个通过数据的算法确保它是唯一的。第二，由于技术上的可能性，它完全可以实现跨地域、多

中心化的信任。第三，通过区块链手段来有效的规避一些金融资产第三方善意取得的风险。第四，增强信息披露，满足监管要求。

此外，可以提供区块链基础服务。因为现在整个区块链技术还处于相对早期的阶段，让任何一个想要基于区块链进行创新的企业都来搭建这样一个平台就会变得非常复杂，我们希望借由 FbaaS 的平台，给很多想要基于区块链进行金融创新、行业创新、应用创新的这些企业提供服务。

区块链有很多用处，但从基础角度来说还存在一些到目前为止没有解决得很好的问题，称为区块链的三难问题。第一，去中心化。区块链系统本身是一个去中心化的，去中心化就是希望参与到网络空间的参与者或者系统构建者，不光是用户，而是构建这个系统的人节点尽可能分散，这是去中心化的特征；第二，它的性能，性能通常的衡量标准是每秒钟所完成的交易数；第三，安全，区块链是一种相对很安全的系统，这个安全怎么定义？就是以节点为单位，抵御更多地攻击者。去中心化，性能和安全构成一个三角形，这三角形其实是互为制约的。比如要提升它的性能，一种最简单的方法是尽可能中心化，第二种是放弃一定的安全性，不要太复杂，不要太多验证，不要每一步都做加密解密。去中心化和安全性之间也有一定问题，一般来说我们认为越去中心化它相对来说越安全。但是反过来说，如果把它作为一个纯中心化的系统，保护单个节点安全性其实相对来说变得容易。所以这个叫作区块链三难问题，三个方面都需要做出一定的平衡。

最后做一个简单的小结和总结，区块链是基于货币的创新，至于比特币价格是怎样的不做判断，因为这涉及政策、治理的层面，不知道它未来会怎样。但是从技术创新源头来看它就是要做一种加密的数字货币，

包括央行的数字货币也很有可能用区块链来做。第二是智能合约，收益权、票据、Parity 钱包等都存在大量的智能合约。我们希望未来各种应用能够基于区块链来做，从而上升到一种治理阶段，就像现在治理互联网一样，现在我们讲互联网 +，未来我们也会看到区块链 +。

（本文是中国区块链研究联盟高级研究员曹锋于 2017 年 12 月 2 日在由中国人民大学国际货币研究所和人民日报社《环球人物》杂志联合主办的“金融科技二十讲”公开课第十二讲中的主题演讲，略有改动）

区块链技术的时空位置

你为什么会出卖隐私？

今天我们来聊区块链这个话题，这是一个非常热门的话题，两个多月前，一群人晚上不睡觉还在吵这件事。

当然在今天很多人想来，区块链等于比特币，我可以通过虚拟货币挣钱。这是很多人想的。其实区块链之所以热，是因为它的能力远远比比特币要大得多，它有可能解决我们过去很多解决不了的事情。什么事情呢？我们从最近炒得比较热的一件事讲起，中国和美国都在发酵。这件事就是说 Facebook 卖掉了 5000 万人的隐私数据，挣了一笔钱。美国国会就说了，扎克伯格不像话，来国会听证，询问询问。

这一下子 Facebook 的市值就掉了 700 多个亿，很厉害。当然后来慢慢又涨回来一点。自打有了互联网，你的隐私就在减少，这是没办法的事。但是为什么这件事这么厉害？实际上每一个人一开始的时候不在乎，而且体会到了方便性。今天某种程度上你就是受害者了，倒不完全说你的隐私被卖掉了。

为什么出卖隐私，或者你的隐私被出卖了？从用户来讲也挺无辜的，两个原因，第一个原因，你无形中卖掉了你的隐私，这是一个你不知道的情况下。为什么这么说呢？我在硅谷的时候，我们做过一些真实的研究，找用户来回答一些问卷，做一些问卷调查。

他一方面用你的数据挣到钱了；第二方面，他还把你的数据给卖了；第三，他反过来给你做价格歧视，你没办法，为什么呢？你也不可能把你的数据存在你的计算机上，将来你在网上的行为就不可用了。这是第一。第二，就算不存在 Facebook 上、不存在百度，你存在第三方也一样，只要那家数据是有一个拥有者的，你现在就有问题。再一个，虽说大数据，用户很多很生气在哪呢？说是我个人数据，你们这些公司拿来挣了钱了，属于我。你就算给了我，腾讯把微信上的数据都给了你，你也看不懂。

所以这些问题大家说能不能我将来有去中心化的东西，放在互联网上一个不知道什么地方，腾讯也好、Facebook 也好、百度也好，你想用我的数据，咱们能不能商量商量。

为什么区块链有可能做到这件事？我把数据放到网上，没有我的授权同意，没有跟我之间的智能合约，这事你就干不了。因为它在数学上有一个很漂亮的地方，你不需要拥有这个数据就能验证这个数据里的各种形式。

过去像百度这种公司，如果做一些大数据统计，他没有你的数据就做不了。比如说今天听了得到直播的人，实际上有多少是买了得到产品的，这个事比如我们放到百度上，真实的数据你得交给他，才能用他的工具做统计。

以后不是这样的，我打个比方，过去是什么呢？你要有权利印这张

钞票，修改这张钞票，你才知道这钞票是真是假。以后只要给你一个验钞机，你能验证钞票是真是假就完了，钞票上你改动不了的。这钞票是放在你家的，你不需要把钞票给它。

区块链到底有什么作用？

区块链到底是什么东西？或者说它有什么用？我们讲两个真实的应用场景。区块这个东西实际上是个记录，你可以理解成你在笔记本上账本上写下一个记录。当任何一个东西产生的时候，实体也好、虚拟的也好，它就同时产生一个记录，你要把它理解成你自己就好了。

你生下来的时候身上就有一个特定的 DNA，这个是不能改的，哪怕你兄弟的 DNA 跟你都不一样，你这一辈子带着。这就是你唯一一个标识，这就是区块，你将来比如做这么一瓶水，做出来以后它就对应着这么一个区块，有一个自己的 DNA。

什么是链呢？就是说它将来所有的行踪、所有中间的交易、整个在生命周期各个过程的一个描述。比如我们说比特币从张三给李四，这个交易过程就要写上一笔，某年月日这个比特币是什么，对应一个随机的号码，从张三到李四手里，还要交到所有的矿机那，通知全世界它的所有权发生转换了。

说到这里，你就想到它有一个很好的用处，就是能够跟踪。比如说这瓶水将来从什么地方来，最后卖到我手里。这件事很重要，现在我们讲食品安全、药品安全，中间流通渠道要把住，中间谁要把箱子拿开，换两瓶假的进去，你是没法检测的，因为流程没法跟踪。以现有的技术跟踪它，实在是太困难了。

区块链将来有这么一个好处，这个药品安全还是很重要的，阿里巴巴的高管们跟我讲，中国路边小药房里头没用的药、过期的药，根本就是安慰剂淀粉的药非常非常多，这个比例说出来吓死你。这不是哪家药房能解决的问题，因为现在的技术根本解决不了，区块链是一个可能的解决方案。

一个简单的方法，这瓶药生产出来的时候，既然有一个区块，我就产生一个对应的区块链给它。它有一个对应的随机码，这个事一旦产生了，在全世界就不能更改了。

它下了生产线，比如说要装箱，先装瓶，这一瓶药就有一个区块链。装箱，区块链还有一个好处，几个区块链可以合并成一个新的，这个箱子本身有一个。我装一个 RFID 码，走出车间，进入仓库的时候，它就过一道门，又有一个记录。

这个门到仓库以后，谁如果把它打开了，换了一瓶药，这个区块就不对了，因为每瓶药上自己有一个区块。然后进入到货车，小货车送到大货车，然后到顺丰快递，通过飞机运到一个新的城市，放到一个集装箱里，最后形成一个大的商品往下传。

甚至他可以验证这瓶药不仅是哪个厂生产的，用了哪种原材料，这个源头是可以溯的。有了这个方法就可以从根本上解决问题。

你就会问，你描述的这个场景是否能成功？检测一瓶药或者一瓶水，由于成本问题，可能做起来有待一些时日。

大个头的比较贵的商品有可能能成，几年前我们投资一家美国的公司，开始是做区块链来跟踪智能合约，后来又做跟踪商品。大家可能听说了，美国对伊朗是禁运的，你要是把一些重要的设备卖给伊朗的话，这是很麻烦的。

但是美国政府就问波音，说我怎么证明你的飞机没有卖到伊朗去，或者里头一些重要的配件发动机没有卖到伊朗去？所以，波音、IBM 这些大公司就用这家小公司的技术，让美国政府能够跟踪到这台发动机到底卖到了什么地方去，它的使用情况是什么样的。

所以说现在因为只是一个成本问题，贵的商品已经做到了，以后你买的一瓶药，这个都可以完全跟踪得很清楚。所以这是区块链真正有用的用处，所以很多公司在开发区块链一些底层技术，也是看到了这些商业前景。

再有一个，区块链本身是一个智能的合约，刚才讲，制造一个实物的时候，它可以有这样一个好的性质。虚拟的东西也是，比如今天我们经常发现有两个问题，在做生意打交道的时候。

以后的智能合约是什么呢？一旦我们俩签了这个合同以后，这笔钱我付给你的某一笔钱，你扣除利润以后，货款可能要给下家，或者上游给你供货的公司。这个是要自动的和银行一起说好了的，所以这笔钱我给了你以后，你是不能随意拿去挪用的。比如说你真把钱还给某家视频公司的话，钱就没了，不一定给供应商，还不知道他给了谁了。

知道某一笔钱你划到某一个特定的账号，就是你跟上一家公司签的合同的时候，才能走得通。

你说我这个商业机密不就泄露了吗？我从哪家供的货，你这个玩意要是将来给我短路怎么办？这还恰恰就是区块链的好处。因为你可以验证这个合同的真假，你看不到合同的内容。

他问银行贷款时说我要贷一千万，因为我要把货比如说卖给北京大学，这件事可以验证，但是我不知道他这个货其实跟他合同详细的细节是怎么签的，也不知道他的货是从哪来的。比如说我们安装一个太阳能

板发电，清洁能源，也不知道是从哪家买来的。

然后银行可以监控这个钱是否按规定来流了，所以这是区块链智能合约的好处。刚才说的第二个例子也是实现了的。

区块链在时空中处于什么位置？

你怎么理解区块链的作用？这件事值得不值得关注？实际上很多事情只有放到一个很大的场景下，你才知道它的作用。

所谓大场景，常常这么划分：时间场景和空间场景。先讲空间场景，它在我们整个未来技术或者 IT 中的地位。我几年前写了一本书叫《智能时代》，这本书卖得很好，为什么呢？是我运气好，赶上当时 AlphaGo 赢了李世石。

实际上从 2016 年开始，我们基本上已经可以证明说它是一个标志，进入一个智能时代，所以人工智能是很重要的。现在还有一些人在踏踏实实做一些事情，但是不是太被关注，为什么呢？他们没有做所谓 2C 的事情，好多还是在做 2B 的事情，比如说 IOT 万物互联，我刚才讲区块链的很多用途前提是有 IOT 在这儿，有万物互联在这儿才有用。否则的话，刚才讲跟踪这个过程就不行了。

IOT 和人工智能加在一起，这个社会就变得很智能化。IOT 的设备哪都是，比如说现在我们刷脸的机器，这其实就是一种 IOT。它把你和整个互联网联系起来了，你在机场，像首都机场都可以通过这种方式，你进关进得很快。还有一个就是区块链，这三个技术我觉得把它给合在一起。我写了一个公式，人工智能 +IOT+ 区块链等于超级智能，未来社会是一个互联的。

它们三个是什么关系呢？超级智能就是说整个城市是一个机器人，人工智能是它的大脑，IOT 是它的感观，眼耳鼻舌身等等，区块链是它的神经系统，我们这些数据是通过区块链的方式在整个社会来传递的。

以后它可能未必是一个像腾讯这样的网络，或阿里巴巴的网络传输。所以这是第二个地位，就是它在时间点上的作用。我们今天的互联网经过了三代，第一代是 PC 和 PC 的联网，你如果当时不在 PC 机上面，你其实没有被联到网络上去的。很简单，你必须要登录以后才知道是你。所以，这是第一代，机器和机器联网，这个规模有多大呢？一年卖掉了几亿台 PC 机。

第一代互联网的时候，最牛的公司是谁？是微软和英特尔，剩下的公司基本上都是打酱油的。用什么？你用英特尔的芯片，Windows 的操作系统。

第二代就是手机互联网，只要手机放在身边，你就随时被挂在网上了。现在你自己的习惯已经改了，两三分钟就要看一下微信。大家说加一下微信号吧，不是说把这两个手机连起来，而是把这两个人连起来。

第三代大的玩家也变了，最收益的是谁呢？一个是谷歌、安卓，再一个就是像高通、三星这些公司，或者说它背后实际上生产处理器的公司就是一家，英国的 ARM。

第四代出现了，前三代都有一个问题，巨头控制着，你越来越不自由了。第四代能不能换一个玩法？你有传感器也好，你有操作系统也好，最好数据这件事我能不能掌握，传输的时候也不要都是通过你一家网络、一家服务器来做，我能不能分散一下？

所以你要把区块链在时间的节点上来看，它处在这样一个位置，就是说从第三代以后可能进入到第四代，所以这是它的重要性所在。

区块链＝生产关系？

很多人问，现在的技术每过一段时间就有一个技术很热，它们是什么关系？是不是后面一个会取代前一个，比如说区块链出来了，人工智能怎么办？

我说这两个风马牛不相及，不过你的问题还是很好的，首先这是一个好问题，因为确实很多人很犯糊涂，你问出来很好。第二，这是一个傻问题，因为它们风马牛不相及。怎么理解呢？人工智能是这么一件事，它是一个生产力。有些时候，我们人的智力水平到这个程度了，你要想再让生产水平提高，就需要新的技术，人工智能就是这个新的技术。

区块链是生产关系，怎么理解这件事？我们说生产关系主要有三个要素，第一，生产的钱和材料，生产的工具这些原材料，这些生产要素从哪来？归谁？

第一代的生产关系，我们先抛开马克思这一套不说，实际上归地主也好、资本家也好、企业主也好，随你怎么叫。

他们提供生产资料以后，你就替他干活。互联网过去是什么呢？过去大公司，为什么你要把数据存在 Facebook 上，你为什么存在百度？

因为你没有生产资料，它不归你。你不存在他们那你存在哪？对于这些公司来讲也一样，你为什么要去那上班？

你不到那上班没人给你工资，生产资料在人家那。既然在人家那，人家说了就算数，这是第一个阶段。

第二代是以硅谷为代表的科技公司的新玩法，现在中国的创业公司都在学。就是说我给你一些股权，每个人都谁小老板了，虽然你才万分

之一的股票，你老板 80% 的股票，没关系，反正你有股权。

再有一个就是发期权，期权是往前看，今天股票一百块钱，五年后还是一百，你一分钱赚不到，五年后五百，你从期权中赚四百，这是市场给你的奖励，投资人给你的奖励。这样一来，个人和企业利益都一致了。

今天你去看一看北京、深圳买房子的人，不是说在一个国有企业做到中层的这些人，40 岁熬到中层的人，不是的。一个小年轻，不小心当年加入腾讯了，或者加入阿里巴巴了，给了期权，那时候可能腾讯的股票才二三十块钱，现在值好几百、上千，拆分以后相当于上千，他不小心赚了一个差钱，他是受益的，他去腾讯去得早，所以发了这么一笔大财，在北京买了好多套房。这样就解决了员工内的生产关系，这是第二代生产关系。

当然，有一个很大的问题，比如今天咱们说中国有好几家独角兽，滴滴是一家。滴滴怎么起来的？你说风险投资给它投的，没有司机愿意接单，没有人去打车，起不来的。

其实前一千个愿意接单的司机和前一万个愿意打车的人，其实对滴滴的起步贡献很大。当时，这种公司多了去了，凭什么它起来了？就是因为有前面这些人在支持它。

但是滴滴起来以后，它的员工可能也分到期权，也挣到钱了，你要是前一千个人，不管是出租车司机也好，还是乘客也好，你是一分钱分不着的。

当然你说我白打了几次车，这点小头跟近一千亿的市值是比不了的，你是半分钱没有的，虽然你是前面的贡献者。因为什么呢？没法记录你的贡献，你凭什么一千个一定比一万个多，这贡献没法算，而且你打了

多少次车，该给你多少奖励，也没法算，因为没法跟踪你表现。

区块链出来以后，这个问题就解决了。就是说每一个人的贡献，每个人的行为，你打一次车就是一个智能合约，这个事是可以跟踪的。

尤其像游戏公司，同样五款类似游戏，凭什么 A 起来了，B 没有起来？这里面有很大的随意性的，早期前面付费的用户贡献很大的。

因为他有一个马太效应，越是玩的人多，越是挣钱很快。所以区块链解决了很大的一个问题，这是从收入来讲的生产关系。从生产工具来讲，它也解决了这样一个问题。我刚才讲了，区块链的数据不一定存在腾讯或者百度，你可以存在一个矿机上，你可以存在互联网的任何一个角落。

每个人和将来的潜在的老板也好，或者什么人也好，客户和提供服务的人也好，你每一次交易是个智能合约，咱们说好了。为什么很多人拿它去发币呢？就是这个币事实上记录你们的交易行为以及每个人相互的贡献，我们将来就是这么一个简单的合作关系。我做得好，拿的币多，我将来发的财就多，很多人是炒这样一个概念。

现在我提醒大家，99% 的币是骗钱的，不要上当。但是它从技术上来讲，提供这样一个可能性。那些大头不再控制生产资料了，分配制度变了，控制生产资料这一条变了，人和人的关系也变了。老板管下属的情况，或者说店大欺客，现在说给你来价格歧视，这些问题慢慢能得到解决。

区块链是个生产关系，重新定义了人和人之间的关系，相比来讲，它未必是把效率提高多少，这一点和人工智能不一样。所以，这是区块链和生产关系的意义。

你接下来说，我又不是搞技术的，我也未必会参与到这里头来。举

两个例子，理论上来讲，将来假设这个区块链平台做得特别特别好了，你也不需要写什么程序代码，你就可以用它的开源软件建一个以你为中心的区块链，这样一个应用的场景，你可以自己发你的币。

举个例子，我在大学研究生时，我们班上有一个女生学霸，她记笔记特清晰，我们这些平时翘课的人，到了期末考试的时候，就得借她的笔记，她也是活雷锋，就借给我们，她什么都没拿着。将来她可以这样说，说我的笔记好，哪怕你们不翘课，你们笔记也没记过我。

我做个区块链的应用，回头你们通过付给我币，你就拿到了我的笔记。她的区块链好到什么程度？好到一个清华的大教授最后自己写教科书就得让这个学生把笔记寄回来，因为他的教案都没有这个女生的笔记好。

有了区块链她就可以做分享，然后她还可以搞一个大社群，比如说清华的学生们，都把笔记贡献出来。还可以搞一个更大的范围，先不说这个事合法不合法，咱们抄题群体，抄作业群体，你别看抄作业这件事，抄作业是大学最增进感情的一件事。你作业被抄了你也没好处，但是有了区块链就有好处了。

比如说个人融资，你想出一本书，很多时候出版社说先拿五万块钱押在这儿，资助出版、编辑费用等等。这书也许最后卖得不错，教授以前也没办法，只好自己掏腰包。有了区块链以后，教授可以发个币，我筹五千块，一本书有时候畅销，前一千个读者说好话很重要，这一千个开始买了他这币的人可有动力把这本书做成畅销书出来。这些人也有贡献，他们也不是白帮忙的。所以每个人在平台足够健全时，你就可以利用它来做一些事情。

区块链＝公众号？

我还有一个等式，区块链 = 公众号。将来以太坊是一个技术平台，你把它理解成腾讯的微信，然后在这个技术平台上，你可以发布你自己的内容或者发布你自己的应用。

现在你通过一个什么方式呢？公众号的方式，或者小应用、新程序的方式来发布，将来你就通过区块链的方式来发布。你想要我这个，咱们商量好了智能合约，我加了密，你给我一个币。

实际上你就通过这个，以前是做公众号，你现在是做一个区块链。以前大家白读，你现在可以收一个币，也许你的币不值钱，你的内容就不值钱。

也许你的币值钱，你的内容将来就值钱。公众号给你打赏了，区块链的价值、币的价值上去了，你就可以从中受益。

所以你理解，将来做一件事，区块链等于公众号，大部分公众号不值钱，没有三五百个人读，但是有些公众号三五百万人在读。不是说搞区块链一定发财，你做一些事没用，白费工夫，但是做对了一件事，你可以通过这种方式来挣钱。

三代区块链分别是？

我为什么要讲三代区块链技术？我会在《吴军的谷歌方法论》里讲 50 个重要的发明，为什么讲发明的逻辑呢？因为很多人创业，我们说有好主意但是他做不成，其实你没搞懂发明真正背后的逻辑，我会给你找

一些成功案例。

失败的教训来一万次你也未必最后能成功，为什么？失败的路有一万条，成功的路只有一条，只有走到成功的路上你才能成功，试错试一万次也没用。所有发明都有一个共同的特点，我在《吴军的谷歌方法论》里头总结叫第三眼美女。什么意思呢？很多技术你至少要经过三次大的迭代才能成功。

举个例子，我们玩 PC 机的时候都知道，最早的做视窗的操作系统的不是微软，不是苹果，是施乐公司做的一个操作系统，做得很漂亮，鼠标什么的都是他们发明的，你听都没听说过。

为什么呢？除了一些对技术特别敏感的人喜欢玩这个，那个东西不实用，有很多问题没解决。这一点很重要，第一代技术一定有很多问题没解决。

到第二代是谁呢？乔布斯最早搞了一个 lisa，卖得也不好，长期基本上 5% 的市场份额，为什么？原因很简单，太贵。所以，第二代技术有时候好，但是用起来成本太高。有些时候第二代技术不一定好。

那么就要第三代技术了，第三代技术是什么？微软的 Windows，满大街都是。包括手机也好，我们今天用的安卓手机，第三代智能手机。区块链也是，今天即将进入第三代，要讲第三代就要先说第一代是什么。

第一代就是比特币，比特币实际上是一种加密货币，叫不叫货币再说，假设叫货币。实际上是每一个货币对应一个随机数，这个随机数只有你知道，别人不知道。

大家可以验证这个随机数的真伪，刚才我讲了，大家可以有验钞机，不能有印钞机，一旦拿了钞票，钞票就是你的。

你的一次交易把这个随机数给了别人，就产生一个新的随机数，旧

的就要作废掉。这是第一代的，通过这个方式大家认可这个算法，你就可以通过它来买卖一些东西。

比特币这件事证明了基于一个随机算法的区块链是可行的，但是刚才我讲什么呢？它一定有很多技术问题，比如效率低下、成本高。今天罗胖给我一个邮件说用户挑战我，说成本不高，交割时间不长。我待会再说这个。

什么叫成本高与不高？理论上来讲，区块链的交易成本可以很低，比如说一两分钱一次交易。但实际上这是理论上来讲，今天比特币这一代的技术做不到。比如你去买一杯咖啡，星巴克咖啡在美国 2.5 美元，你如果用比特币付款，因为每天的矿机挖矿都要挖掉大概上千万的钱，你算到每天有多少个币，有多少个交割。

我刚才说了两个问题还没有解决，一个是交割时间，QPS，每秒钟能够吞吐的量太小。现在其实大家在上面交易量是非常低的，频率非常低，所以这也是每天价钱上下浮动很大的一个原因。要做到什么时候才能真正比较好地应用呢？

基本上信用卡刷的频率是很高的，哪怕不到信用卡，差不多在纳斯达克上买股票的这样一个频率才行，所以这是第三代解决问题。

第一代和第二代还有一个不安全的地方，这个币的号给到你，你没有保存好，真丢了以后就找不回来了。这事很讨厌，理论上来讲，币是唯一的，我人也是唯一的，这个币交给了我，我除了背下来，或者把这个存在某个地方，随机码的钥匙。

我能不能跟人真的对应上？能验证我人的身份这件事对应上？所以，第一代第二代都没解决这个问题，第三代要解决这个问题。所以你这个用起来才方便。

还有一个问题，第一代、第二代，我跟他们好多做币的人去聊，也给他们做技术的投资。我说你们交易币最大的风险在哪？

你们想不到最大的风险在哪，不是钥匙忘掉了，有发生这种事，我一个朋友钥匙忘了，知道这是他的币，但是这个币永远找不回来。

这还不是最大的风险，最大的风险是跑路，这个交易平台，张三、李四、王五天天跑路的时有发生。跑路完了以后，有些比特币还有，你在平台上的一些钱，或者说钱包、资产就没了。所以，这是一个现在很大的问题。

第三代的时候，真正能希望说我能够绕过这些交易平台，完全做到点对点的这样一些交易，现在第三代技术就在解决这样一个问题。

（吴军，硅谷创投第一个掌门人、风险投资人、计算机科学家）

来源：得到 APP

价值互联网时代的区块链技术应用

工业化异化的人性回归

历史车轮滚滚向前，人类大踏步进入了数字革命时代，也迎来了云计算、大数据、区块链等技术浪潮。而在利益的驱动和工业化巨浪的裹挟下，人类如同工业流水线上的产品，被磨灭个性，走向趋同。

但凡有旧事物消亡之时，也一定有新事物在野蛮生长。随着工业 4.0 时代大幕初启，被工业化异化的人性正日益回归。

在认知层面，人类不再满足于趋同；在技术层面，智能制造还原了柔性制造和个性定制的可能，技术的裂变发展也为人性回归奠定了基础。

最近大家都在谈论区块链，但是都讲得很“肤浅”，因为如果仅仅局限于描述技术本身，区块链依然只是一个使用工具。而所有创业者，都应当从更高的哲学观和文化的视角看待科技演变。

思维和认知观比掌握知识更为重要，跳出技术去看待新兴技术，并且秉持着以人为本的初心，回归人性本源，人们终会意识到，所有的技术最终都将为人服务。

当然，区块链也不例外。

区块链是一台信任的机器

我们已经从信息互联网时代走向价值互联网时代，互联网也正在成为各行各业的基础设施。

因为信息互联网，人类社会已经发生了翻天覆地的变化，社会福利因此大幅增加；而因为价值互联网，人类社会也必将迎来一场更完美的革命。

而今天人们提及的价值互联网，其实也就是以区块链应用为主要代表之一的互联网新形态。信任，正是价值互联网中最重要的“价值”所在，重点体现在如何降低信用成本，打造可信机制。如何在万物互联的世界去打造一个可信机制，已是亟待破解的课题。区块链技术正是这样一个在泛在“去信任”的环境中去构造一种新信任机制和交易规则。

区块链（BLOCKCHAIN）是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次比特币网络交易的信息，用于验证其信息的有效性和生成下一个区块。作为比特币的一个重要概念和底层技术，区块链在本质上是一个去中心化的数据库。

区块链具备以下核心：

1. 是一个就近可寻找的存储节点；

2. 有密钥的加密的存储数据就近全部存放；

3. 任何数据生成必须满足前两者的要求；

4. 必须要在一个共同的互联网满足 tcp/ip 协议；

5. 在任何节点任何时候都可以持有密钥打开就近的各存储器上对应

欲取的数据；

6. 如何避免首次存储数据准确不出错；

7. 如何保证密钥不被复制成为非法合法用户任意使用；

8. 如何保证账本上的数据不被修改，因为能够存储就有可能被修改；

9. 公共互联网遇恶意病毒侵袭，全部数据被篡改失去原有真实性不能够恢复发生的损失，谁是纠正主体、谁是赔偿主体、风险救济如何实现；

10. 信任机制是不是牢不可破的，是否经得起极限考验 .....

区块链的进化方式是：区块链 1.0——数字货币区块链；2.0——数字资产与智能合约区块链；3.0——DAO、DAC（区块链自洽组织、区块链自洽公司）发展为区块链大社会（科学，医疗，教育 .....）。

区块链经济发展重点

区块链技术在经历了从概念到实践的坎坷之路后，应用落地的时机逐渐成熟，“区块链 +”的模式将在行业内带来新的商机，尤其是在金融服务、公共服务、信息安全、慈善、智能制造、社交应用、能源、物联网应用、医疗健康、政务管理、法律应用、农业应用方面重点发展，并将衍生出更广域的经济生态。

区块链应用案例：

1. 区块链金融服务产业应用

金融服务是中心化程度最高的产业之一，金融市场中交易双方的信息不对称导致无法建立有效的信用机制，产业链条中存在大量中心化的信用中介和信息中介，减缓了系统运转效率，增加了资金往来成本。

而区块链技术公开、不可篡改的属性，以及去中心化的信任机制，具备改变金融基础架构的潜力，各类金融资产均可以被整合进区块链账本中，成为链上的数字资产，在区块链上进行存储、转移、交易。

在银行、跨境支付、资产数字化、智能证券、保险等领域中有着广泛的应用潜力。

以银行为例，凭借去中心化的特点，区块链技术可以为银行创建一个分布式的公开可查询网络，其中的所有交易数据是透明和共享的，从而削减无效的银行中介，节省运营成本。

2. 区块链供应链管理应用

供应链是一种由物流、信息流、资金流所共同组成的，并将行业内的供应商、分销商、零售商、用户串联在一起的复杂结构。而区块链技术作为一种大规模的协作工具，天然地适用于供应链管理。

以美国加州的创业公司 Skuchain 为例：

在红酒供应链工作流程中，通过区块链技术提高了供应链透明度：

（1）红酒厂家首先将红酒产品分给经销商，并带有 Skuchain 设计的二维码；

（2）经销商把其中一部分红酒转让给下一个经销商时，会附带产品二维码；

（3）当有人试图复制二维码，系统将会发现，并可以跟踪到复制者，并对侵犯商品权、造假者进行惩罚。

3. 区块链智能制造应用

以物联网为例，区块链技术利用 P2P 组网技术和混合通信协议，处

理异构设备间的通信，将显著降低中心化数据中心的建设和维护成本，同时可以将计算和存储需求分散到组成物联网网络的各个设备中，有效阻止网络中的任何单一节点的失败。

另外，区块链中分布式账本的防篡改性，能有效防止发生工业物联网中任何单节点设备被恶意攻击和控制后带来的信息泄露和操控风险。

未来，人们还可以通过整合、借势、学习、变革等手段，充分把握智慧经济环境下的“智慧认知”和智慧技术为产业转型升级带来的发展契机。

（张旭光，浙江省科技创新创业促进会会长、浙江创建科技股份有限公司董事长、浙江省首届十大科技实业家）

区块链的应用呈现

我是 Jeoff，我在蚂蚁金服的花名叫“姐夫”，大家要找我，串亲戚没问题的。我在蚂蚁负责创新技术和创新业务，当然，区块链是很重要的一部分。如果看看 2017 年或 2018 年业界最热的东西可能就是区块链，热到什么程度呢？有时候我妈妈会问我区块链是什么东西，70 多岁，还谈比特币，说过山车一样上上下下。

这个事情我们技术实验室的同学也感受到热潮，我们有个同学叫希批，他到网上发相亲广告，没有人理他。最近他想了想，改了一下，他是区块链工程师，马上就收到 200 多份简历，很多姑娘专门给他发微信问他，“你是不是做比特币的，你们工资是不是比特币发的？你们做不做 ICO？”热度空前到这个程度。

今天，和大家分享一下，从蚂蚁作为一家科技公司，看看区块链这个视角，它与人们的生活发生的关系。

区块链是什么？

想象一下，2017 年有很多的关键词，说到比特币马上想到 ICO、智能合约，有些像虚拟货币、加密猫关联到一块儿。我们认为它会回到人间，泡沫过去之后，我们相信区块链会围绕技术的本质，阐述更多有社会价值的东西，通过沉淀技术，对我们的生活产生一些影响的东西。

另外，区块链非常高大上，要讲这个技术，它非常复杂。可能今天给你讲两个小时也搞不清楚密码学是怎么设计的，非常高大上。

但就像移动支付一样，它已经慢慢在改变你生活的一部分，在蚂蚁公司我们做的事情里已经慢慢进入你的生活，只是说你用的时候可能不知道，背后已经用到了区块链的技术。这是另外一个回到人间，它不是妖，也不是神，回到人间的平台上，确实慢慢与你我他都有关系，发生生活的变化。

区块链到底是什么样的东西？

互联网之前，我们有很多点对点的通信，任何资金的交易是双方要交互的，很多是通过单独管子相互对接。互联网产生之后进入了很多层，互联网有很多协议，最上面的是应用层，慢慢它就把下面共享的部分统一掉，上面无非是我建立逻辑就可以了，做应用，产生很多大的公司——Google、Facebook、阿里巴巴、百度、腾讯等这样的公司。

今后在统一的平台上，互联网平台上空前提高了通讯效率和数据交互效率，上面产生了很多新的应用，电商、搜索引擎，都建立在统一的

标准上，才可以有今天的互联网经济。

下一步很多人都预测到区块链带来更大的影响，因为它在互联网的基础上又近了两层，这涉及区块链是什么的问题——

共享账本。

今天房屋里有 100 人，我们讨论一个事情，一定要根据一个协议做事情，所以要签个合同。签合同的时候大家要讨论半天，某种程度上要达成一个共识，最后共识还不一定相信你，我们要写下来，一条条写在纸上。每个人要去看看，这个合同是不是你想代表你自己的一些利益，最后你要签上名，每个人都背书了，这样合同就生效了。

在区块链系统里差不多，某个机器，数据一致情况下用协议保证每个数据是一致的，校对完之后每个人签上名（电子签名）。有一天 100 个人里有一个人发生纠纷了，我们把它拿出来看看，大部分人同意，有一部分人不同意，我们就同意大部分人同意的那一版，这样统一各方来保证一致性，这叫共享账本。这 100 个人是一致的，签了名的，不能修改的。

另一个重要的一层就是共享合约。计算机就是数据在上面跑，数据一致之后接下来就是逻辑一致，保证结论是一致的。保证各方数据一致以后，就可以在上面加一些程序。保证数据的一致性、逻辑的一致性都会带来很大的自动化。

最后，区块链、AI 技术本质都是带来效率的提高，就是自动化，计算机最终的目的是不断地提高自动化的效率，这样就能提高社会的效率，带来很巨大的经济价值。

整个区块链发展趋势，一方面是公有链发展跟币相关，比特币、以太币，昨天晚上涨 20%，然后又跌了 30% 等等，它确实在上上下下。技

术层面上讲它造成很多的问题。光做一笔比特币的交易消耗的电能在高峰时超过 20 美元，买杯咖啡 5 美元的话，产生 5 美元的价值体现不了消耗的电能，40 万台的机器要达成共识，每天机器都在那儿算，过程中会消耗很多的电能。

这个角度来看，这么多机器加起来消耗的电能到高峰时每笔交易 20 美元，平时在 3 美元左右。如果真用比特币的交易，用比特币做比较简单的事情，比如买杯咖啡或茶，消耗的电能加起来可能比交易价值还要高。

很多公司在做的是联盟链，各大机构 PoC 非常多，都在摸索，在传统商业模式里如何引进区块链，可以做供应链，可以做认证。

在各个行业里，大家都在寻找自己的价值点，为什么区块链和很多的技术有区别？区块链改变的是生产关系，因为数据是生产资料，因为你需要数据，在数字经济里数据是生产资料，生产资料进来以后还需要生产关系，在各行各业里都有生产关系，这决定了区块链技术更加广泛和底层技术，它要改变生产关系、供应链的关系，各个机构之间紧密的关系。

蚂蚁金服区块链以联盟链为主，在商业和金融做了很多应用场景，而且全部是自主产权。

区块链的关键技术

下面我讲一下涉及的基本技术。

区块链有很多层次，最下面的是核心技术，上面是区块链系统，更上面的是区块链应用。从底层角度看，非常核心的技术点基本归结在几

个点上：

一是共识算法、性能；

二是隐私保护与安全，里面涉及非常深的技术，比如零知识证明。

三是区块链系统架构，还涉及很多跨链互联，因为在区块链里有很多平台，平台之间怎么互联网，就像局域网和局域网怎么互联。

四是核心技术上层是区块链系统。

区块链在全球布局，我们要支撑天猫这样的全球商品溯源，我们的机器要布到全世界，那么你会遇到很多的问题和挑战：

区块链技术中有共识，假如 100 个点要达成共识，并不是机器百分之百达成共识，比如我有 3 个机器在澳大利亚，澳大利亚到国内的网络速度比国内的慢，国内机器的共识就会慢慢把那边机器抛出去，就是这个小圈子跟不上时代了。

这会涉及很多共识机制设计的问题，以及高可靠性区块链平台、核心基础设施，还要有运维能力，简单在区块链系统上做个应用容易些，要做金融级，安全、可靠的系统是非常难的。同时要有很高的安全和隐私保护。

把所有的技术整合在一块儿提供一个平台，这个平台才能跑应用。蚂蚁金服在这些年里围绕核心技术做了很多的努力，在这个基础上，蚂蚁金服作为一家科技公司方面的投入，我们非常希望通过几年努力，在这些领域里我们来定义什么是区块链，因为我们有场景，有应用。

以上关于我们的底层技术，底层技术怎么整合到系统。

区块链如何改变经济模式和社会生活？

下面我讲讲区块链和我们生活的关系，有人觉得区块链是非常高大上的东西，但很难了解到核心的技术点。我们基本认为，区块链可以在三个流里会产生大的作用：第一，信息流。区块链很大的作用是信息的共享，就像我们经常要开会一样，各个公司经常要开会，开会干什么？依次分享数据，达成决策的共识，各方把数据、信息带进来，进行数据、信息分享，然后拍拍板然后去执行。信息流的分享会带来很大的经济效益，我们做的事情是关注信息共享，保证它透明，保证它可信，保证它执行。第二，物流。有了信息流之后还是信息层面的东西，和信息相关的有物流，物流怎么保证它的流动性可信以及基础设施。第三，资产的资金流。信息流、物流、资金流要融合在一起。我们在金融方面做了很多新的应用，因为它还在开发之中。蚂蚁金服落地的区块链应用场景：公益、溯源、金融……

下面用应用来呈现，区块链技术到底和我有什么关系？

公益

我们做了一个公益项目。在支付宝平台上有很多好心人士捐款，数额比较小——5 元、10 元，但人多，就会形成很大的资金流，最后通过平台和中间公益机构分配到贵州乡村小学，小学的学生需要书包，辽宁某个地方的老兵老了无助，很多地方的人需要帮助。

这时候我们建立一个平台，要解决一个问题——成千上万的人来的钱怎么汇集到一个基金的账号，怎么保证它最后到达受捐人的身上，包

括资金的全透明？我们是全程跟踪，每一笔捐款是怎么上来的，这个钱走到哪个基金，基金的钱怎么分配到最后受捐人的身上，每一笔数据全程透明，而且和我们的资金流对上，保证可以查到捐款是从基金人账号到支付宝账号或者从支付宝账号到基金的账号，全程跟踪。

这样空前提高了透明性，从捐款人，比如你我他每个人捐的 20 元，凑在一起变成 60 元，过程中我们可以看到这 60 元到了某个乡村某个小妹妹的书包。那个书包是 60 元，它全程透明告诉你这个钱确实用到了受捐人的身上。

通过我们一年的努力，现在有 38 家公益机构，有 355 个公益项目，有几亿资金通过这样的网络慢慢落到受捐人的身上。

这本身是资金流的专业金融问题，通过区块链技术，钱从哪里来，钱到哪里去，全程透明告诉你这个过程。这对将来的公益事业，很多需要接受帮助的人，这是很好的技术和应用。让每笔善款有迹可循，这和我们很多人的生活是密切相关的，非常清楚我的钱用到哪里去了。

溯源

如何保证进口的牛奶是真的牛奶，而且是高质量的牛奶，并且食品安全？我们和支付宝合作，通过澳大利亚海外机构，从海外的货舱，到国内的货舱，再到天猫的商家，你基本可以看到每一罐牛奶生产时经过了多少步到了你的手里，而且有时间戳——你知道什么时候生产的，到你手上，基本上不可算改。

等到消费者拿到商品时可以拿出你的手机扫一扫，根据上面二维码，它可以非常清楚地告诉你，从哪里来，经过多少步，在每一步上停留多长时间，这可以很高程度上体现食品的安全和新鲜度的保障。

金融

我们做了一个互助性保险的组织——每笔资金从哪里来，放在哪里，最后钱花在哪里，花在谁的身上，会员都可以非常详细地看到我的钱到哪里去了，监管、审计机构能非常清楚地看到这个钱运营时有没有什么猫腻。

所谓信息共享的例子里，马上可以延伸到的很多的场景例子。

数据共享和交易

住房领域里我们也做了很多的应用。

关于住房，首先我们必须要有一条可信的数据链——你住在哪里，和你的权益有关系，小孩能不能去那个学校上学；数据从哪里来，机构必须从可信的数据，在不可篡改基础上共享，并保证你的权益。数据共享以后，保证一致性以后，在上面可以开发很多的应用。

比如医疗领域的病例档案数据共享，免去病人重复检查的烦琐，提高医疗效率。

很多场景可以用到这个应用。它的本质上三个流信息流、物流、资金流。

区块链技术未来的方向

有些东西做简单比较容易，到巨大金融级的应用系统还是需要非常强大的技术和工程能力，因为大家都知道，金融级的系统基本不允许有任何的错误。

我们也认为，区块链技术肯定会和很多别的创新技术组合：

一方面是和物联网技术，刚才说物流，物理世界发生的事情要延伸到数字世界，我要映射到它在数字世界的资产，物理世界发生的很多事情要和物联网的技术相关。

其他方面，很多人会想更加远的，比较牛的东西。比如将来汽车上会有很多的通讯和合约，举些例子——你可以要求前面的车拦个路，然后我给你 5 分钱；自动驾驶汽车之间做沟通，只要你给我让路我就给你钱，被邀请让路的人也可以挣钱。当然，这还有涉及安全的问题，这是个社会系统，这只是举个例子。

它慢慢在我们身边产生变革，无处不在的变革。数据达成协议，就会形成合约，合约是个程序，自动地执行，通过互联网手段回到物理世界里，否则是数字上面的东西，我想通过互联网的手段进入物理世界。

区块链也和生物识别的技术相关。生物识别技术本质上需要去认证你是谁，因为你的资产和操作，在区块链这样的系统跑了以后还是需要隐私和安全的保护。首先怎么保证这个隐私安全？我要知道你是谁，能不能碰到这个数据。

同时它和非常热的 AI 技术有关系。区块链跑的是什么？跑的是数据，数据到各个机构共享以后，肯定在上面要空前地利用多方可以互换的数据上做更多的挖掘和应用。

要做好区块链，物理世界里或者大规模应用里还是要有很强的工程管理能力，做个简单的应用非常容易，一旦上了量以后就会遇到很大的挑战，因为很多的共识算法就是这样的，节点越多，涉及的算法量和安全风险就会越大。

预测 2018 年

1.2018 年，区块链供应链服务管理上，我相信区块链应用从概念性证明会慢慢进入商业系统，今天分享的例子已经看到，它已经开始进入你的生活，真正发挥价值。越来越多的传统行业会思考现在的商业模式，来拥抱尝试区块链技术，它本质上是改变互助的生产关系，生产关系是无处不在的，开个会也有共识，这某种程度上也可以通过区块链技术实现。

2. 共识机制和网络决策等核心技术发展会改变区块链系统的性能和规模，以太坊后或会出现第三代区块链技术架构。现在币消耗电能没法搞，还是比较难持续的。所以它会形成第三代区块链技术架构。因为你不能空前消耗社会的资源，能源本来就是很少的东西，围绕这样的东西被大量消耗，总觉得有点不太对劲。

3. 区块链技术里隐私安全技术是非常非常相关的，因为数据要分享。我为了共识首先要分享，你如果不分享怎么达成共识，共识什么呢？共识之前还要讨论一个问题，什么东西可看什么东西不可看，因为加入进来是需要有一定的利益关系，要解决隐私的关系。全世界范围内看到了很多的进展，它的商用可以到秒级的水准，会进一步解决互信与隐私的矛盾，区块链技术的设计就是为了互信，得多方加入进来，互联网自然而然就会有隐私的问题，有一部分我愿意分享，有一部分我不愿意分享，这个问题怎么解决，很多东西需要技术来解决。

4. 在多个平台共存的情况下跨平台多链互联，实现跨链价值转移和数据交换肯定会成为区块链非常关键的重点。这相当于一个城市里，我

有公路网、航空网、铁路网，它是有每个链的，每个链解决一个问题。就像一个城市一样，把公路网、航空网、铁路网连到一块儿，保证公路进来的，现在进入环球中心了，一会儿我赶飞机，可以想办法从公路网转到航空网，达到我的目的，这里有很多的工作要做。大家都在搞很多的局域网，先要连一点，因为数据要在上面跑的，要固化的，价值要转移的。这里有非常重要的关键点。

（本文是蚂蚁金服副总裁兼技术实验室负责人蒋国飞出席 FT 举办的区块链交流会的分享，略有改动）

区块链在金融领域的应用分析和思考

从金融的实质寻找金融与区块链的结合点

金融，字面上看就是资金的融通，是对资金进行时空上的配置，服务于实体经济，本身并不直接创造财富。在金融业务中流通的资金以及金融工具，都与线下实体资产有一定的对应关系，也就是说是实体资产的一种影子。所以说金融是服务于实体经济，但是并不是直接创造财富，实际的财富还是现在的资产。

这里边提到一个概念，资产权益。金融工具是一种资产权益，比如股票、债券等，扩大这个概念，我国的法定货币人民币是央行通过储备资产发行的，从这个角度看，法定货币也是资产权益。围绕金融资产权益，金融业务主要有三个关键环节。

第一个环节，资产权益的评估。这个需要金融中介来对线下实体资产确定其价值，从而明确资产权益的真实价值。

第二个环节，资产权益证明的发放，也就是说确定了资产相应的价值之后，那么就会给相应的金融参与者一个金融资产权益的证明。比如

股权证明书基本上属于中介发放管理。

第三个环节，资产权益证明的流通，金融参与者持有资产权益证明，能够在金融过程中寻找其他参与者，对接他们的融资需求。现在一般的金融工具都是一种基于中介的流通化方式。对于法币来说，现金是线下点对点的流通，而电子支付是通过银行的系统进行中心化的流通。

从这三个环节切入，我们来看区块链具体在其中能够参与到哪些环节。

首先第一个环节，如果说要对资产权益进行评估的话，其实区块链很难以做到线上数据与线下实体的结合，不能够代替金融中介去评估一个实体金融资产价值。比如，房产证明，在区块链网络当中有房产证明这个文件，这肯定没有问题。但是线下这个房产是否还存在，以及线下房产现在是否已经归他人所有，其实本身并没有一个直接的对应关系。要保证这个对应关系，其实还是需要在中介那去进行一个权威的评估。

第二个环节，资产权益证明的发放，其实这个过程主要针对资产权益证明本身文件实现防伪，区块链可以做到电子权益证明去中心化发放，并且保证不可篡改。

第三个是资产权益证明的流通，这个环节反映金融工具的流动性。原来的方式中，其实这种权益证明的流动性较差。那么基于区块链，这个资产权益证明可以点对点流通，并可以再切分，所以流动性会大大增强。

所以综合这三个环节来看，金融领域中的中介其实有着非常重要作用，可以提供评估、风控、增值等服务，去中介不是必然趋势。

再回到区块链本身技术架构来说，区块链其实就是能够对链内所产生的数据进行有效管理和追踪。对于链外或者是线下资产，或者是对于

链外能够导入到链内的数据，本身并不能够进行有效管理，无法严重真实性及价值。

这其实可以举个例子，中本聪在比特币的创世区块当中写了一段信息，这个信息是当时泰晤士报的一个头版新闻标题，在后来的节点共识过程中，这个信息肯定是逐步的存在这个账本当中。大家都认为肯定不可篡改，这确实没有问题。但这条信息背后的含义是否真实？起码在区块链网络中是没法验证的。这也是区块链本身一个技术的架构导致的。

所以，综合以上的分析，我们认为，区块链可以用于资产权益证明的发放管理和流通环节，但是难以参与到线下的权益评估。

区块链在逐步对金融体系产生积极的影响

基于区块链在金融资产权益证明发放与流通中的应用，区块链正逐步对金融体系产生积极的影响。金融体系有五个构成要素，货币发行流通、金融工具、金融市场、金融中介以及制度与调控机制。

区块链最直接影响到的是货币流通与金融工具，它能够实现金融工具，也就是资产权益证明的点对点流通。在货币这个领域，目前以比特币为代表的加密数字代币创新性实现了虚拟货币点对点的流通，激发了人们对于区块链在当局货币发行流通中作用的探讨，因此各国开始探讨区块链在数字货币、货币流通过程中起到的作用，这也是现在中国人民银行要研究数字货币一个原因。

基于区块链对货币流通以及金融工具过程中实现电子化、点对点流通的创新应用，就能增强金融过程中的投资者与借款者之间的点对点关联。那么他们之间的关联增强之后，金融市场的运作效率会整体提升，

从而使得直接金融市场的规模增大。在这个过程中金融中介职能其实是下降的，也是聚焦的，今后金融中介职能主要会针对实现投资者与借款者的交易撮合、信息采集分析等，这些是最重要的功能。所以金融中介的职能在下降和聚焦，导致间接金融市场规模减小。

基于对于金融市场“升”与金融中介“降”的影响，从而推动制度和调控机制的创新完善，进而维持整体的金融稳定。

因此我们说，区块链目前对金融体系能够产生一个积极影响。

我们的课题报告从六个金融细分领域研究区块链应用，有数字货币、供应链金融、支付清结算、证券、保险与征信。下面将从数字货币、供应链金融与支付清结算三方面展开分析。

区块链在数字货币领域的应用分析及思考

数字货币的研究现状

研究数字货币，不可避免要探究其与当前的法定货币的关系。当前经济生活中的法定货币都是信用货币，信用货币是以国家信用为背书发行的货币，独立履行货币职能。

从资产属性来看，信用货币是央行通过储备资产发行，通过商业银行信贷活动进行派生。在数字货币这个范畴，加密数字代币，主要是以比特币为代表的代币，背后没有实际价值，没有国家信用作为背书，或者是规模很庞大的企业信用作为背书，它就是依托于自行的算法进行创造。按照目前央行研究的进展来说，法定数字货币肯定是要通过央行储备资产来发行。也就是说法定数字货币与现行的信用货币体系是一致的。

从流通属性来看，信用货币形态有纸币、金属硬币及电子货币，电

子货币其实就是银行的存款货币，实质上也就是电子支付工具。数字货币本身也是一种电子货币，加密数字代币主要是基于点对点非中心化的流通方式，法定数字货币的流通方式可以基于中心化的方式，也可以基于非中心化的方式发行，这与央行主导的模式有很大的关系。

因此说，数字货币应该是建立在信用货币体系下，选取适合的流通模式进行发行和流通。这也对应到前面所总结出来的观点，金融资产权益当中区块链的应用，就是应用于资产权益的流通及发行。

具体看一下加密数字代币和法定数字货币的研究现状。

加密数字代币无中心发行机构，点对点流通，无内在价值。当前人们持有加密数字代币，相当一部分是投机或投资，当然也有少数部分是用于支付交易。在某些国家，像日本、英国的一些企业与加密数字代币交易所进行了合作，推出类似于比特币支付的应用。

法定数字货币方面，未来银行间的大额结算将依托法定数字货币实现清算与结算的合二为一。其实在 2017 年 1 月央行已经开始在尝试在银行、金融机构间基于区块链的数字票据的应用，里面就包含了法定数字货币的应用，这也是法定数字货币比较适用的场景。

未来法定数字货币是否适合直接面向公众发行，央行也在探究当中。因为如果要发行，央行选择直接面向公众发行，或者还是通过商业银行进行发行，这牵扯到未来央行、商业银行的职能定位。

除此之外，我们还研究了法定数字货币与第三方支付间的关系，未来法定数字货币将挤压第三方支付机构支付业务市场空间，催使第三方支付机构发展金融增值服务。这一论题我们课题组单独进行了研究，欢迎大家与我们今天探讨。从研究现状来看，英国、加拿大、巴巴多斯等国央行都在研究法定数字货币，不过相关新闻基本都是在

2016 年，往后鲜有相关新闻，目前我国央行还在持续推进法定数字货币的研究。

总之，加密数字代币不属于现行信用货币体系，目前无法有效履行货币基本职能。法定数字货币未来可能融入信用货币体系，在履行货币职能的同时，其相关的支付清算系统有可能成为新一代金融基础设施，并对银行间清算结算、电子支付体系产生深远影响。

区块链与数字货币的关系

前面一直在探讨法定数字货币与信用货币，那区块链与法定数字货币有什么关系呢。区块链是否适用于法定数字货币，法定数字货币是否必须依托区块链发行流通，答案是否定的。

区块链只是法定数字货币的可选技术。这其中，需要认识到区块链技术不仅不是加密数字代币可选择的唯一实现技术，更不是法定数字货币的唯一实现技术。应当具体分析研究区块链的技术特性、模式与架构哪些适合应用于法定数字货币领域，哪些不适合。

区块链对法定数据货币的研究有一定的借鉴价值。区块链采用拜占庭共识协议防范恶意节点的攻击，为法定数字货币系统防范恶意节点攻击提供了很好的借鉴。区块链智能合约的模式奠定了智能化操作的可能性，为法定数字货币实现更高品质提供了重要参考价值。

所以，法定数字货币的实践应用，一定是结合经济生活的实际需求再采取合适的技术方式来实现的，因此说区块链是有益的参考，但不是唯一方案。

区块链在供应链金融领域的应用分析及思考

供应链金融，是一种 2B 的融资模式，依托核心企业，以供应链交易过程中的应收账款、预付账款、存货为质押，为供应链中小企业提供融资服务。

现在的供应链当中，肯定是有中间的一个核心企业。那么目前的供应链金融，它能够为核心企业的直接上下游企业，就是一级供应商跟经销商提供融资服务，因为其本身与核心企业有直接的贸易往来，但是二级三级的供应商与经销商因为本身跟核心企业没有直接的贸易往来，使得金融机构与其信息不对称，金融机构难以评估其信用资质，因此导致了融资比较困难。

它要进行融资，就对应另外一个问题，就是它与它的下级或者是上级的供应商、经销商进行了贸易，这个真实关系也存在一定的疑问。所以金融机构在面对它进行发放贷款融资的时候，要进行的风控成本是比较高的，这也导致其融资比较贵。

基于区块链的解决方案中，我们认为可以以节点可控的方式建立一种联盟链的网络，涵盖供应链上下游企业、财务公司、金融机构、银行等。接下来将各个节点贸易数据上链，上链目的就是为了让各个节点保持同步，金融机构可获取二三级中小型企业贸易的真实情况。有融资需求的企业将他们合同、债权等证明上链登记，可保证这些资产权益数字化以后不可篡改、也不可复制。最后在联盟当中流转这些资产权益证明，实现点对点的连通，极大的提升数字资产证明流动性。

但是，这应用过程中还面临不少问题，首先就是合规合法的问题。

现在供应链当中，金融机构银行不给中小型企业贷款的一个原因，就是因为银行非常关注收账款债权“转让通知”的法律效应，都会要求一级供应商或核心企业签回“债权转让同意书”，如果无法签回，会造成银行不愿授信。

因此，基于区块链的解决方案需要严格遵守供应链金融现行的法律规则开展研究应用。其他还有核心企业贸易信息隐私安全以及核心企业话语权的问题。

目前，国内区块链供应链金融应用发展势头迅猛，落地效果较好，整体已初具规模。但是，仍然面临一些问题。

区块链在支付清结算领域的应用分析及思考

支付清结算系统是经济金融活动的基础性支撑，是用以实现债权债务清偿及资金转移的一种金融安排，国际上尝试区块链应用的支付清结算系统有两类：一是各国用于商业银行、金融机构之间的大额实时支付系统，二是连接全球支付清算网络的跨境支付系统。

在大额支付系统中，提升金融服务流程效率与提高系统操作弹性，是区块链技术的重要应用场景与优势。

在跨境支付系统中，通过一种金融交易的标准协议，实现全世界的银行、企业或个人互相进行点对点金融交易，无须类似 SWIFT 的中心管理者，直接实现跨国跨币种的支付交易。

时间关系，支付清结算领域的区块链应用分析不具体展开了。

总结所探究的 6 个金融细分领域的案例，区块链在目前应用中面临的挑战有四个层面，商业挑战、技术挑战、金融设计挑战以及风险管理

的挑战。商业层面，面临成本收益、网络效应的挑战。技术层面，面临高并发、标准化及信息安全的挑战。金融设计层面，面临金融工具、金融中介定位的挑战。风险管理层面，面临诸多法律问题，如权利义务规定、牌照、反洗钱合规、治理等挑战。

当前，对于区块链的应用应该抱着一种比较包容的态度进行探索，现行金融、法律规则是基础，不能逾越。金融领域当中，区块链的应用只是提供一种新角度下的解决方案，并没有变革任何的生产关系，而如果要真的首先这种生产关系的变革，还是需要金融体系整体制度的支撑，所以区块链也颠覆不了现在的金融体系。不过在应用当中必须要探索包容的审慎监管，严防代币可能带来的区块链金融风险。

（王强，中国信通院产业与规划所数字经济研究员）

三、区块链发展进入新阶段

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。

——《中国区块链技术和应用发展白皮书》

区块链发展演进路径①

区块链技术起源于化名为“中本聪”（Satoshi Nakamoto）的学者在2008年发表的奠基性论文《比特币：一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新，从而实现以前未实现的功能。

至今为止，区块链技术大致经历了3个发展阶段，如图1所示。

① 本文选自《中国区块链技术和应用发展白皮书2016》。

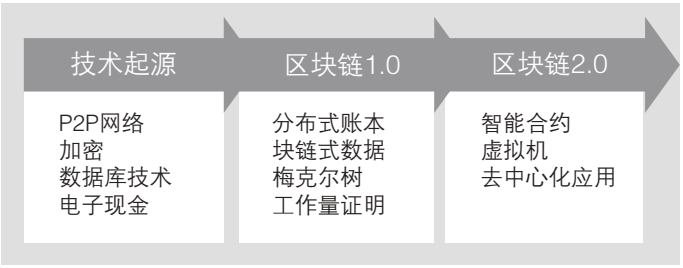

图 1　区块链的演进路径

技术来源

1.P2P 网络技术是区块链系统连接各对等节点的组网技术，学术界将其翻译为对等网络，在多数媒体上则被称为“点对点”或“端对端”网络，是建构在互联网上的一种连接网络。图 2 所示为一种 P2P 网络模式，图 3 为典型中心化网络模式。

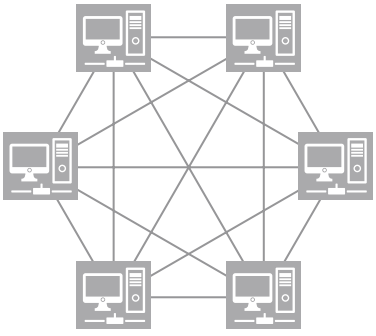

图 2　P2P 网络模式

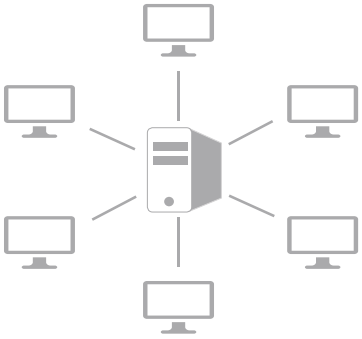

图 3　中心化网络模式

不同于中心化网络模式，P2P 网络中各节点的计算机地位平等，每个节点有相同的网络权力，不存在中心化的服务器。所有节点间通过特定的软件协议共享部分计算资源、软件或者信息内容。在比特币出现之前，P2P 网络计算技术已被广泛用于开发各种应用，如即时通讯软件、

文件共享和下载软件、网络视频播放软件、计算资源共享软件等。P2P网络技术是构成区块链技术架构的核心技术之一。

2. 非对称加密算法是指使用公私钥对数据存储和传输进行加密和解密。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方解密接收到的加密内容。公私钥对计算时间较长，主要用于加密较少的数据。常用的非对称加密算法有 RSA 和 ECC。非对称加密算法的过程如图 4 所示。区块链正是使用非对称加密的公私钥对来构建节点间信任的。

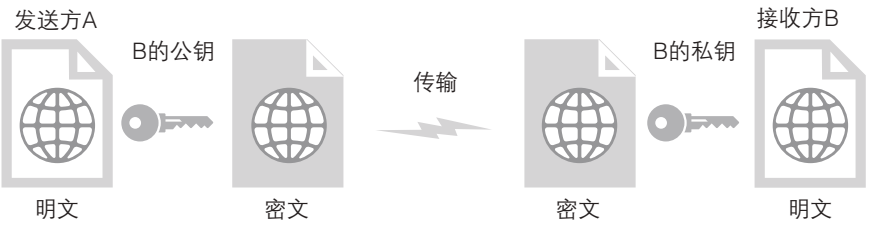

图 4　非对称加密解密过程

3. 数据库技术涉及计算机技术发展的大半历程，是基础性技术，也是软件业的基石。数据库技术脱胎于软件业，将数据储存独立于代码，改变了此前数据处理软件的架构。数据库技术从早期的网状结构、层次结构发展到基于严密关系代数基础的关系型。关系型数据库用简单的二维表格集存储真实世界的对象及其联系，有业界统一的 SQL 语言，被极为广泛地用于构建各种系统和应用软件。世界互联网产生的海量数据催生了以键值（简称：Key-Value）对为基础的分布式数据库系统。目前，世界上主要的互联网公司根据各自需要研发和构建了 NoSQL 数据库管理系统。在区块链系统建设方面，传统的关系型数据库和分布式键值数据均适用。

4 数字货币（Digital money）又被称为电子现金（Ecash）或电子货币（Emoney），视为对现实货币的模拟，涉及用户、商家和处于中心化地位的银行或第三方支付机构。数字货币是电子商务和网上转账的基础。现实中数字货币也指一类免密支付的卡，如公交卡。第一个数字货币方案于 1982 年被 Chaum 创造性地提出，致力于解决重复花费问题，使用了盲签名技术，可以完全保护用户隐私。完全匿名的数字货币不能满足政府和金融机构的监管要求，于是匿名可控的概念被学者们提出。匿名可控即在适当条件下可以撤销匿名性且用户无法察觉，也可以是在审计时用户主动撤销匿名性。数字货币的使用过程如图 5 所示。

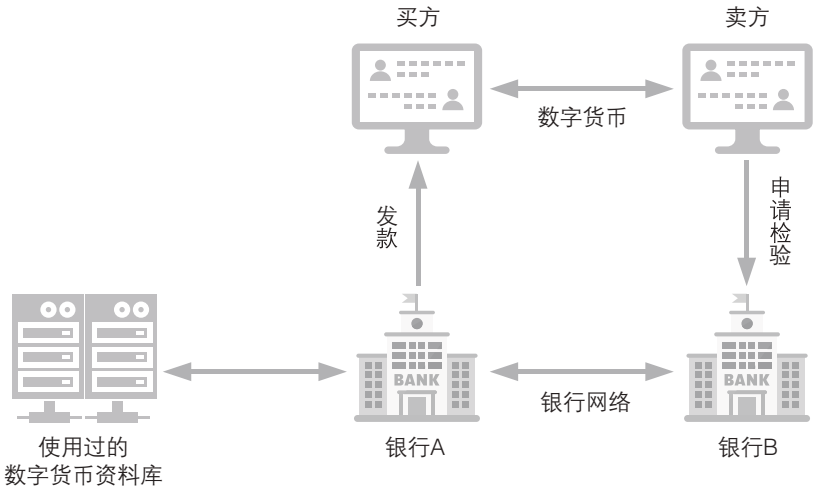

图 5　数字货币的使用过程

区块链 1.0——数字货币

2009 年初，比特币网络正式上线运行。作为一种虚拟货币系统，比特币的总量是由网络共识协议限定的，没有任何个人及机构能够随意修

改其中的供应量及交易记录。在比特币网络成功运行多年后，部分金融机构开始意识到，支撑比特币运行的底层技术——区块链实际上是一种极其巧妙的分布式共享账本及点对点价值传输技术，对金融乃至各行各业带来的潜在影响甚至可能不亚于复式记账法的发明。

若从其实质分析，区块链就是一种无须中介参与，亦能在互不信任或弱信任的参与者之间维系一套不可篡改的账本记录的技术。区块链 1.0 的典型特征如下：

1. 以区块为单位的链状数据块结构：区块链系统各节点通过一定的共识机制选取具有打包交易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发生的有效交易及其梅克尔树根值等内容打包成一个区块，向全网广播。由于每一个区块都是与前续区块通过密码学证明的方式链接在一起的，当区块链达到一定的长度后，要修改某个历史区块中的交易内容就必须将该区块之前的所有区块的交易记录及密码学证明进行重构，有效实现了防篡改。

2. 全网共享账本：在典型的区块链网络中，每一个节点都能够存储全网发生的历史交易记录的完整、一致账本，即对个别节点的账本数据的篡改、攻击不会影响全网总账的安全性。此外，由于全网的节点是通过点对点的方式连接起来的，没有单一的中心化服务器，因此不存在单一的攻击入口。同时，全网共享账本这个特性也使得防止双重支付成为现实。

3. 非对称加密：典型的区块链网络中，账户体系由非对称加密算法下的公钥和私钥组成，若没有私钥则无法使用对应公钥中的资产。

4. 源代码开源：区块链网络中设定的共识机制、规则等都可以通过一致的、开源的源代码进行验证。

以上技术的组合，就是区块链 1.0 的典型实现，其完整的技术架构如图 6 所示。

图 6　区块链 1.0 技术架构

区块链 2.0——智能合约

2014 年前后，业界开始认识到区块链技术的重要价值，并将其用于数字货币外的领域，如分布式身份认证、分布式域名系统、分布式自治组织等。这些应用称为分布式应用（DAPP）。用区块链技术架构从零开始构建 DAPP 非常困难，但不同的 DAPP 共享了很多相同的组件。区块链 2.0 试图创建可共用的技术平台并向开发者提供 BaaS 服务，极大提高了交易速度，大大降低资源消耗，并支持 PoW、PoS 和 DPoS 等多种共识算法，使 DAPP 的开发变得更容易。

区块链 2.0 的典型特征如下：

1. 智能合约：区块链系统中的应用，是已编码的、可自动运行的业务逻辑，通常有自己的代币和专用开发语言。

2. DAPP：包含用户界面的应用，包括但不限于各种加密货币，如以

太坊钱包。

3. 虚拟机：用于执行智能合约编译后的代码。虚拟机是图灵完备的。区块链 2.0 的技术架构如图 7 所示。

图 7 区块链 2.0 技术架构

随着区块链技术和应用的不断深入，以智能合约、DAPP 为代表的区块链 2.0，将不仅仅只是支撑各种典型行业应用的架构体系。在组织、公司、社会等多种形态的运转背后，可能都能看到区块链的这种分布式协作模式的影子。可以说，区块链必将广泛而深刻地改变人们的生活方式。区块链技术可能应用于人类活动的规模协调，甚至有人大胆预测人类社会可能进入到区块链时代，即区块链 3.0。

区块链技术走进大众视野

区块链技术的概念、优势与不足

区块链技术是以比特币为代表的数字加密货币体系的核心支撑技术。区块链技术的核心优势是不再需要一个传统的中心化机构，仅通过加密算法、共识机制、时间戳等技术手段，在分布式系统中实现了不依赖于某个信用中心的点对点交易、协调和协作，从而规避中心化机构普遍存在的数据安全，协同效率和风险控制等问题。

区块链技术起源于 2008 年，狭义的区块链技术是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构，并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账，能够安全存储简单的、有先后关系的、能在系统内验证的数据。广义的区块链技术则是利用加密技术来验证与存储数据、利用分布式共识算法来新增和更新数据、利用运行在区块链上的代码，即智能合约，来保证业务逻辑的自动强制执行的一种全新的多中心化基础架构与分布式计算范式。

与传统技术对比，区块链具有以下四个方面的优势：

一是难以篡改，更加安全。在传统信息系统的安全方案中，安全依赖于层层设防的访问控制。通过区块链技术，记录交易的数据库任何人都可以访问，但由于巧妙的设计并辅以密码学和共识机制，区块链的数据记录方式使得修改某一数据需要变更所有的后续数据记录，难度极大。实践证明，这样一个数据库可以确保市值达千亿美金的比特币，在全球黑客的攻击下，运转稳定。

二是异构多活，可靠性强。区块链每个系统参与方都是一个异地多活节点，是天生的多活系统。如果某个节点遇到网络问题、硬件故障、软件错误或者被黑客控制，均不会影响系统以及其他参与节点。区块链中的节点通过点对点的通信协议进行交互，在保证通信协议一致的情况下不同节点可由不同开发者使用不同的编程语言、不同版本的全节点来处理交易。由此构成的软件异构环境确保了即便某个版本的软件出现问题，区块链的整体网络不会受到影响，这也是其高可用的基石所在。

三是具备智能合约，自动执行。智能合约具有透明可信、自动执行、强制履约的优点。尽管如此，自尼克·萨博 1993 年提出以来，智能合约始终停留在理念层面。重要原因在于，长久以来没有支持可信代码运行的环境，无法实现自动强制执行。而区块链第一次让智能合约的构想成为现实。

四是网状直接协作机制，更加透明。区块链提供了不同于传统的方法，以对等的方式把参与方连接起来，由参与方共同维护一个系统，参与方职责明确，无需向第三方机构让渡权利，有利于各方更好地开展协作。作为信任机器，区块链有望成为低成本、高效率的一种全新的协作模式，形成更大范围、更低成本的新协同机制。

虽然区块链有上述优点，也很好地达到了比特币的预定设计目标，

支撑了比特币系统的正常运行。但也正因为区块链技术早期主要是服务于比特币，在某些方面有着明显的短板和不足。

一是性能和扩展性不能满足要求，从目前的情况来看，区块链的性能问题主要表现为吞吐量及存储带宽远不能满足整个社会的支付需求。同时，比特币随着时间的推移，累积的交易数据越来越大，对于普通电脑的存储来说，这是个不小的负担。如果只是简单提高区块大小来提高吞吐量，比特币很快就会变成只有少数几个大公司能够运行的系统，有违去中心化的设计初衷。在比特币、以太坊等公有链系统中，上述矛盾是系统设计时面临的最大挑战。

在联盟链中，因为参与记账的节点可选可控，最弱节点的能力上限不会太低，并且可以通过资源投入获得改善，再针对性地替换掉共识算法等组件最终获得性能的全方位提升。但作为智能合约基础支撑的联盟链另有考验：智能合约运行时会互相调用并读写区块数据，因此交易的处理时序特别重要，如果只能逐笔进行，这会严重制约节点的处理能力。

二是数据隐私和访问控制有待改进。现有公有链中，各参与方都能够获得完整数据备份，所有数据对于参与方来讲是透明的，无法使参与方仅获取特定信息。比特币通过隔断交易地址和地址持有人真实身份的关联，达到匿名效果。所以虽然能够看到每一笔转账记录的发送方和接受方的地址，但无法对应到现实世界中的具体某个人。对于比特币而言，这样的解决方案也许够用。但如果区块链需要承载更多的业务，比如登记实名资产，又或者通过智能合约实现具体的借款合同，这些合同信息如何保存在区块链上，验证节点在不知晓具体合同信息的情况下如何执行合同等等，目前业内尚未有成熟方案。而这些问题在传统信息系统中并不存在。

三是治理机制有待完善。公有链社区摸索出了“硬分叉”和“软分叉”等升级机制，但遗留问题有待观察。由于公有链不能“关停”，其错误修复也异常棘手，一旦出现问题，尤其是安全漏洞，将非常致命。

实际上，通过放松去中心化这个限制条件，很多问题能找到解决的方案。比如在联盟链这样的多中心系统中，通过关闭系统来升级区块链底层，或者紧急干预，回滚数据等，必要时都是可用的手段，这些手段有助于控制风险、纠正错误。而对于常规代码升级，通过分离代码和数据，结合多层智能合约结构，实现可控的智能合约更替。

互联网近年来的迅猛发展及其与物理世界的深度耦合与强力反馈，已经根本性地改变了现代社会的生产、生活与管理决策模式。可以预见的是，未来在中心化和去中心化这两个极点之间，将会存在一个新的领域，各种区块链系统拥有不同的非中心化程度，以满足不同场景的特定需求。

区块链技术最新的理论和实践进展

随着社区的繁荣，研究的深入，不同应用蓬勃发展，对于区块链技术的局限有了更深刻的认识，在此基础上，针对区块链的一些不足提出了很多解决方案，主要集中在共识机制，性能，隐私和安全，治理机制和跨链技术等方面。

首先来看共识机制。共识是各方对某种陈述达成一致的过程或结果。在博弈论中，每个人都知道的信息称为共有知识，仅是共同知识的一个层次。共同知识还要求每个人都知道别人也知道的信息，以至每个人都知道其他人知道，并且相互认同。以安徒生童话《皇帝的新装》为例，

在小孩戳破真相之前，每个人都知道皇帝是裸着的。但这是共有知识，不是共同知识。

区块链技术通过信息广播，交易签名，投票表决的方式，可以巧妙地将共有知识转化为高阶的共同知识。其中，节点签名并广播起到了让其他人知道我知道并认可该区块，从而达成共识获得共同知识的作用。在比特币中，其规则“最长链是全网的有效链”即是一种共同知识，矿工作为经济理性人使用该共同知识来支持高阶信念，对其他矿工的决策进行猜测，最终形成纳什均衡。

有后继研究认为，中本聪原始论文中 51% 的安全算力假设是有问题的。自私挖矿策略的存在使得比特币的理论安全阈值下降。自私挖矿简单说就是，挖到块后不发布，继续挖，如果挖到第二个块，这时再发布出来。如果在挖第二个块的过程中，有别人挖出的其他块被广播出来，则立刻广播自己之前挖到的块。经过理论测算，如果一个矿工有 1/3 的算力，则自私挖矿是有利于自己的。因此，基于掌握的算力份额大小，大小矿工的影响力是不同的，需要用新的计算模型求解博弈均衡点。

分布式系统的共识算法研究由来已久，20 世纪 80 年代就开始研究，Lamport 提出的 Paxos 以及后来在此基础上发展出的各种 BFT 拜占庭容错算法皆属此类，其核心在于通过节点投票达成分布式系统的状态一致性。比特币另辟蹊径，在技术之外叠加经济激励，以共识机制保证系统状态的全局一致。

古典共识机制的问题在于，一旦参与投票节点数量增加后，其共识效率会大幅下降以至于无法使用；中本聪共识机制的问题在于浪费大量能源以及交易确认时间长。

康奈尔和麻省理工的研究员提出了将中本聪共识和 BFT 类共识进行

有机结合的混合共识方案，是一个新的突破方向，有可能兼具两者优点，避免各自缺点。目前这方面的研究还在持续进行中。

技术改进的第二个方面是在隐私和安全方面。在公有链中，需要对交易数据、地址、身份等敏感信息进行保护，同时又能让记账节点验证交易的合法性；对于联盟链，在构建隐私保护方案的同时，需考虑可监管性 / 授权追踪。可以通过采用高效的零知识证明、承诺、证据不可区分等密码学原语与方案来实现交易身份及内容隐私保护；基于环签名、群签名等密码学方案的隐私保护机制、基于分级证书机制的隐私保护机制也是可选方案；也可通过采用高效的同态加密方案或安全多方计算方案来实现交易内容的隐私保护；还可采用混币机制实现简单的隐私保护。

以太坊自正式运转后发生多次安全事故，其中最大的一次是 TheDAO 被黑事件。TheDAO 是一个由程序代码管理的自治的风险投资基金，共募集了 1200 万 ETH。黑客利用 TheDAO 智能合约的安全漏洞，从合约管理的 ETH 中划走 360 万个 ETH。最终以太坊基金会不得不进行分叉以解决该问题。因为社区对分叉的处置手段有不同意见，此次事件后出现了 ETH 和 ETC 两种以太坊的区块链，坚持私产不可以任何理由剥夺的人群选择留在了 ETC。

TheDAO 事件折射出两个问题：一是智能合约尤其是公有链的智能合约的安全问题非常重要，出现漏洞或错误后，无法像中心化系统那样通过关闭系统，集中升级的办法进行修复。而智能合约往往直接管理资金，一旦出现漏洞会直接导致经济损失，因此需要更强的安全措施。目前在这方面的研究热点是把以往应用在芯片设计或者军事控制系统上的形式化验证的方法，应用到智能合约上，以数学证明的方式尽可能避免人为错误。

TheDAO 事件还折射出另外一个问题，即现有区块链缺乏一套完善的治理机制，当社区面临重大决策事件时，如何让社区参与进来，以某种机制形成社区意见，最终在区块链上表达出来。这些决策可能是不同的技术升级提案，也可能是 TheDAO 这样的突发事件处理，或者是该区块链某些基础规则的调整。如果缺乏治理机制，只能通过软分叉或者硬分叉解决问题，最终将导致混乱和分裂。

最近比较有趣的一个趋势是，代币持有者投票的链上治理机制再度作为多目标决策机制兴起。代币持有者的投票有时会用来决定运行网络的超级节点由谁操作，如 EOS、NEO、Lisk 等系统中的委任权益证明（DPOS）机制；有时用来对协议参数进行表决，比如以太坊的 Gas 上限；有时用来进行表决或直接实行批量协议升级，如 Tezos。在这些例子，投票都是自动进行的，也就是说，协议本身包含了更改验证程序集或更新其自身规则所需的一切逻辑，而且是根据投票结果来自动进行。

链上治理通常被认为具有以下几大主要优势。首先，与比特币所倡导的高度保守的理念不同，它可以迅速发展并接受必要的技术改进。其次，通过建立一个明确的去中心化框架，可以避免非正式治理上的已知缺陷，人们觉得非正式治理太不稳定，又容易出现链分裂，或是变得在事实上过于中心化。最后，链上治理有利于确保流程的贯彻执行，从而提高协调性和公平性，也允许更快的决策。

但代币投票机制饱受诟病的一点是，无论这些机制在何处尝试，其投票者参与度会往往很低。投票参与度低引发了两个问题。首先，投票要取得合法性认可比较困难，因为它只反映了少部分人的意见。其次，仅持有一小部分代币的攻击者就能够左右投票。

此外，有些人认为，链上治理存在风险，因为元系统一旦确定就难

以再改变。正如直接写入的代码一样，一旦有缺陷，就会更快也更容易地被利用。同时，链上治理让普通节点运营者对治理的参与变得毫无必要。这使得普通节点运营者无须做任何决定，而只是遵循链上流程所做出的决策。那么当出现财阀式的少数人链上治理时，普通用户利益将会被不相容，有悖公有链的价值观。区块链属于公众，为了公共利益服务。它不是为了让加密货币大户变得更加富有。区块链并不应该由谁来占有，更不用说一小部分超级富豪了。因此，有人反对链上治理。

总体看，关于链上治理机制，仍处于争议和探索的过程中，尚未有统一的意见，需要我们进一步关注和研究。

最后谈谈跨链技术。跨链技术可以理解为连接各区块链的桥梁，满足不同区块链间的资产流转、信息互通、应用协同。当下区块链技术纷繁芜杂，各成一派，彼此之间还无法进行价值和数据的交换。随着行业发展，链与链之间的互操作越来越重要。如果跨链没有解决，各大区块链都将会是孤岛，必定会降低区块链社区的活力，从而限制整个区块链网络和生态系统的发展。

跨链技术可以应用于跨链资产转移、跨链原子交易、跨链数据共享、跨链合约执行以及去中心化交易所等广泛场景，目前有三种技术模式：

一是公证人机制（Notary schemes）。这是中心化或基于多重签名的见证人模式，主要特点是不关注所跨链的结构和共识特性，而是引入一个可信的第三方充当公证人，作为跨链操作的中介。代表性方案是Interledger。

二是侧链 / 中继（Sidechains/Relays）。侧链是一种锚定原链的链结构，但并不是原链的分叉，而是从原链的数据流上提取特定的信息，组成一种新的链结构，而中继则是跨链信息交互和传递的渠道。不论是

侧链还是中继，作用都是从原链采集数据，扮演着 listener 的角色。侧链和原链不能直接验证对方块的状态，因为这样会形成循环，但相互只包含轻节点是可行的，相应的验证逻辑可由链协议本身或应用合约实现。一般来说，主链不知道侧链的存在，而侧链必须要知道主链的存在。代表性方案是 BTC relay 、RootStock、Polkadot 等。

三是哈希锁定（Hash-locking）技术。它在不同链之间设定相互操作的触发器，通常是个待披露明文的随机数的哈希值。哈希值相当于转账暗语，只有拿到这暗语的人，才能获得款项。同时，它还构造了两个退款（Redeem）合约，这两个合约需要双重签名且有时间期限，对方签名，自己未签名，当自己签名时，资产退回原处。其中一个关键技术设计是，制造转账哈希暗语的人的退款合约，在时间期限上要长于另外一个人，由此可保护他的权益。代表性方案是比特币闪电网络。

值得一提的是，跨链技术也得到了一些中央银行的重视。比如日本央行和欧洲央行合作的 Stella 央行数字货币试验项目，在第二期就着重研究了单链和跨链的 DVP 解决方案。

总结

区块链技术的进展，还有很多方面可以展开阐述，鉴于时间的关系，我就做一个简要的汇报，不当之处，敬请大家批评指正。应该说目前监管者面临的任务也并不轻松，面对不断演进的区块链技术，还需要同步考虑相应的法律法规和技术标准，以加强监管，防范风险。

总结来说，区块链是一种可能成为未来金融基础设施的新兴技术，对其进行深入研究是我国金融科技工作的应有之义。区块链技术有优点，

也有缺点，仍在不断发展演进中。目前看，区块链若要实现真正落地，支撑实际业务，在技术层面仍需大量改进工作。

在刚刚召开的全国网络和信息化工作会议上，习近平总书记做了非常重要的讲话，他指出：“核心技术是国之重器，要下定决心保持恒心，找准重心，加速推动信息领域核心技术的突破，要抓产业体系建设，在技术产业政策上共同发力，要遵循技术发展规律做好体系化技术布局，优中选优、重点突破”。习总书记的讲话可谓是语重心长，我们应该清醒意识到，区块链应用在我国是走过弯路的，所以易纲行长也指出要发挥区块链技术的正能量和更好地服务于实体经济。我们必须认真贯彻落实习总书记的重要讲话精神，在核心关键技术上下功夫，不受制于人，同时要促进区块链技术整个市场和生态环境的健康发展。

（姚前，中国人民银行数字货币研究所所长）

来源：《第一财经》

中国区块链行业发展报告 2018

中国区块链区块链行业发展速度

1. 区块链技术创新加速

技术创新是区块链行业深入发展的核心驱动力，中国区块链行业的技术创新正在经历着一个明显加速的过程。

以 2014—2017 年中国及美国区块链领域公开专利数量为例，从总体趋势来看，不论是中国还是美国区块链相关专利公开数量呈明显上升趋势，其中，美国公开专利数量从 2014 年的 150 件增加到 2017 年前 7 个月的 390 件，中国公开专利数量从 2014 年的 2 件增加到 2017 年前 7 个月的 428 件，中国区块链专利公开数量增速超过美国。

2. 区块链融资增长迅猛

2014—2017 年 7 月全球区块链领域私募投资金额总体呈现增长趋势，由于 ICO 的兴起，2017 年全球区块链领域私募股权投资金额较

2016 年下降，但相对 2014 年增长幅度明显，其中美国在该领域私募股权融资金额从 2014 年的 2.12 亿美元，增加到 2016 年 3.94 亿美元，增长幅度达 85.84%，而在此期间，中国区块链领域私募股权融资金额金额从 0.16 亿美元增长到 0.76 亿美元，增长达 3.75 倍，虽然中国私募股权融资规模小于美国，但增长速度明显高于美国。

3. 区块链应用范围广阔

得益于区块链技术的持续创新，以及中国庞大的互联网消费群体，区块链应用在中国也呈现出多元广泛、积极活跃的特点。2014—2017 年 7 月，中国区块链领域私募股权投资共计投向挖矿、钱包、虚拟货币、基础设施、底层技术、交易所、相关服务、区块链应用 8 个领域，中国区块链产业链可谓基本成型。

从占比最高的区块链应用来看，私募股权投资领域又可分为数据服务、金融、认证确权、文化娱乐等 10 个领域，其中数据服务、金融和认证确权三个领域占比较高，三项累计占比达 79%。

4. 区块链行业组织竞相成立

区块链技术的创新和应用落地离不开行业生态的构建和完善。自 2015 年 12 月至 2017 年末，中国成立区块链相关的行业协会 / 联盟近 20 个，中国区块链应用研究中心，GBBC 中国中心，中关村区块链联盟、中国电子学会区块链专委会、中国信通院可信区块链联盟等一大批区块链专业组织为行业机构和不同背景的人员提供了一个专业领域的交流及合作平台，对于中国区块链行业的长期、健康发展发挥极有益的作用。

在区块链技术的教育和培训方面，中国各地区相关高校也在积极开展，开设相关科目、课程，以多种形式的教育培训项目，为中国区块链行业创新发展输送人才。

例如，清华大学 iCenter、同济大学金融科技研究院、北邮在线区块链教育与研究中心等。其他各种区块链培训也在蓬勃发展，其中，由中国区块链应用研究中心联合 GBBC 组织的区块链应用培训目前已为中国区块链行业培训认证了近千名专业人才。

中国区块链行业发展面临挑战

1. 清退非法数字货币交易所

中国政府对于比特币一直持有谨慎的态度。早在 2013 年 12 月，中国人民银行等五部委就发布了《关于防范比特币风险的通知》，明确规定了比特币的性质，防范可能存在的过度投机炒作的风险、逃汇风险、洗钱风险以及涉嫌类证券的违规行为等隐患。因此，中国各比特币交易平台均未获得省级金融办的批准。

2017 年 9 月 4 日，受到 ICO 的影响，中国人民银行等七部委于发布《关于防范代币发行融资风险的公告》，在叫停 ICO 的同时，也对各数字资产交易平台提出了停业整顿的要求：“代币融资交易平台不得从事法定货币与代币、虚拟货币相互之间的兑换业务，不得买卖或作为中央对手方买卖代币或虚拟货币，不得为代币或虚拟货币提供定价、信息中介等服务。”

2. 叫停非法 ICO 活动

截至 2017 年上半年，中国 ICO 市场已初具规模，募资金额达到 26 亿元人民币。但与此同时，缺少政府监管的 ICO 活动催生了大量良莠不齐的 ICO 项目，存在发行方缺乏明晰的规范、投资者缺乏适当性管理、投资者非理性行为引发市场泡沫和不法之徒借机诈骗洗钱等隐患。

2017 年 9 月，中国人民银行联合七部委发布《关于防范代币发行融资风险的公告》，定义 ICO 为非法活动，全面叫停 ICO。

然而，监管政策针对 ICO 融资模式的叫停，并非对区块链在初创企业融资应用的否定，也并非对区块链及数字货币等金融科技的否定。

短期来看，ICO 有关行业的创新企业融资可能导致融资放缓，但从长远看来，此次监管收紧能够及时防止资金流向非法集资项目和传销诈骗项目，警示普通投资者审慎投资，防范市场过热引发金融风险。

3. 政府监管重安全和稳定

国务院设立了金融稳定发展委员会，强化人民银行宏观审慎管理和系统性风险防范职责。中国的监管机构一方面及时地预见风险，处置风险，叫停比特币和 ICO 代币的集中交易，降低数字资产市场风险，维护国家金融的稳定和安全。

另一方面监管者也明确表示，当前的一些监管措施并不是否定数字货币，更不是否定与之相关的技术，而是对其已经引发的金融乱象进行治理，对可能出现的金融风险加以防范。

在风险防范的同时，业界也广泛呼吁防止矫枉过正的现象，对于正

常的学术研究和理性探讨，应该给予足够的空间，同时积极应对交易所关闭后，大量交易转入场外交易、地下交易的新形势、新问题。

中国区块链行业前景积极乐观

1. 创业者积极参与，90 后大量入场

互联网已经颠覆了世界，区块链却要颠覆互联网。可以说区块链已然成为一个最大的风口。对于区块链这一最新领域，成长在数字社会的80、90 后有着超越其他时代人的认知能力，这一认知能力又转化为“认知红利”。

位于北京的互联网金融博物馆（the Museum of FinTech）每季度评比金融科技与区块链创新企业，超过 200 家公司的区块链创业者都是90 后。一批 90 后区块链创业者甚至投资人正在广泛的参与全球竞争，迎接属于他们的时代到来。事实上，全球区块链创业和数字货币的交易总量的重要来源都是中国的创业者。

2. 财富效应引起广泛关注

近年来，以比特币为代表的全球加密数字资产的规模不断扩大，据CoinMarketCap. 网站统计的数据，截至 2017 年 12 月 17 日，全球数字资产总市值已经触及 6000 亿美元。

而 2016 年 12 月 31 日，这个数字才仅有 177 亿美元。不到一年的时间里，规模扩大近 3300%，财富聚集效应引起了各方密切关注。区块链和数字货币已经成为中国大众的主流关注点和日常用语，私人和机构

的资产配置也在转向这一领域。传统机构和国企机构间接入场。

几年前，区块链技术还是极客世界中“自由”的代名词；如今，巨头已经纷纷宣布涉足这一领域。

中国平安，成为国内首家加入 R3 区块链联盟的机构，目前已在资产交易和征信两个场景中上线了区块链技术；万向集团成立了万向区块链实验室；中国银联与 IBM 合作，预研“使用区块链技术的跨行积分兑换系统”。

百度与 Circle 达成战略合作；阿里系的蚂蚁金服将打造基于区块链技术的公益平台；腾讯加入可信区块链联盟，中食、中粮等传统国企与太一云合作推进中国食品链；国家版权局与版权交易中心联盟联合发布了中国版权链，点融与富士康合作研发区块链供应链金融平台，其他众多上市公司、大型金融机构也纷纷推出区块链发展计划。

与其他创业公司相比，国企、行业巨头拥有更雄厚的资金和研究团队，也有更丰富的、可供区块链技术落地的场景。

3. 基金投资蔚然成风

着力金融科技领域的投资机构，对区块链技术持续关注。资本市场的玩家，有场景、有资金，但他们更多是要将区块链技术进行改造，真正实现降低信任成本和交易成本。

在去年的第一季度，全球区块链创业公司累计获得 VC 投资 15.7 亿美元，而在过去的三年时间中（2014 年—2016 年），全球区块链创业企业总计获得投资金额接近 150 亿美金。

据数据公司 CB Insights 于近日发布的一份报告，谷歌和高盛是当前全球投资区块链公司最活跃的两家机构投资者。国内清华启迪、万向

集团、复星集团等多家投资机构都已经发起了区块链创投基金。

4. 早期领袖机构的坚守底线，守法合规

中国区块链应用研究中心于 2017 年 8 月 16 日曾举办 ICO 专题恳谈会，召集了十余家在京区块链机构负责人，非常明确表达了呼吁监管介入，控制市场风险的意见。北京金融局党组书记局长霍学文发表了重要讲话，要求中心所属理事机构和北京地区的相关机构不参与任何 ICO 的发行和交易，严格自律，遵守相关法律。这次会议获得业界广泛认可和传播。

2017 年 9 月 4 日，中国人民银行及七部委发布的关于防范代币发行融资风险的公告。中国区块链应用研究中心全体理事共同发声，赞同监管部门的相关决定，并发表自律声明，全体理事进行了联署，在政府清理过程中，高度配合，没有出现重大的风险事件，彰显了中国区块链应用研究中心早期行业成员维护大局的担当。

5. 各地政府特别沿海地区高度鼓励区块链

国务院印发《“十三五”国家信息化规划》，区块链与大数据、人工智能、机器深度学习等新技术，成为国家布局重点。

中国人民银行印发了《中国金融业信息技术“十三五”发展规划》，明确提出积极推进区块链、人工智能等新技术应用研究，去年 10 月，工信部发布《中国区块链技术和应用发展白皮书》，这是首个落地的区块链官方指导文件。

央行正在进行的国家数字货币试点，区块链也是其实现的技术之一。

各地政府，特别是沿海地区纷纷成立区块链实验地、研究院。目前，

深圳、杭州、广州、贵阳、赣州等地政府都在积极建立区块链发展专区，给予特别扶植政策。

这些超过 500 万人口的城市大力推动区块链创新将建立一个个市场高地，开拓中国未来的空间。

来源：中国区块链应用研究中心

中国在区块链研发和应用居全球前列

区块链技术金融应用已取得突破。中国在区块链技术研发应用方面走在全球前列，央行在主导法定数字货币和数字票据的研究，未来数字金融将把“平面金融折叠成立体金融”。

区块链的本质是构建信任链接器有利于信用普及和普惠金融

金融界：区块链自 2009 年诞生以来，数字货币百花齐放，市场追捧热情高涨。您认为区块链的本质是什么？

李礼辉：区块链可以理解为“一系列信息区块组成的数据链”，它最重要的特点是，可以构造一个信任的平台、信任的链接器。我一直不认为“去中心化”是区块链的主要特点。随着区块链的迭代演进，去中心化的区块链技术结构，现在基本上是在参与者比较少的社区中存在，例如比特币、以太坊等。而在金融领域应用领域，区块链是有中心的，是多中心的一种分布式结构。

信用建立的传统方式，需要信用积累，需要经过中心节点，比如人

民银行的征信中心、支付宝等。对于大的企业机构以及富裕的个人而言，这是很好的方式。不过，对于小微企业和普通大众而言，通过中心节点来积累信用的机会并不多，可以积累的信用信息也非常少，这里就存在信任缺失或者信任薄弱的情况。在这种场景下，区块链通过数学和编程的方式解决信任问题，通过共识算法、智能合约等，在信任确实或信任薄弱的状态下，建立一种相互的信任。这是对商业信用的一种加持，即用技术的方式来增强商业信用，而不是取代商业信用。区块链为建立新的信任机制提供了可能性，并且成本更加低廉。

金融界：为什么我们需要区块链？区块链有哪些优势？

李礼辉：区块链技术相对其他技术有两个很特别的优势。一是，区块链可以建立信任的平台，在商业信用比较薄弱或者缺失的状态下，能够建立共同信任、形成以技术为核心的信任平台。从这个意义上来看，它有利于推进信任普及，推动普惠金融的发展，从而让更多个人和企业建立更加广泛的信任关系。

二是，区块链的核心技术之一是智能合约，它在多方参与、复杂交易的场景中有突出的优势。例如，传统的资产托管业务会涉及资产委托方、资产管理方、资产托管方、审计方、投资顾问等多个方面，在多方参与的交易场景中，多方之间需要重复校验，流程结构复杂，难以做到及时处理。目前，邮政储蓄银行的资产托管业务系统、微众银行的联合贷款备付金管理和对账平台，都引入了区块链技术。区块链技术的引入可以做到协同治理，归并校验，避免重叠，精简流程，使得交易更加简单，在信息共享的同时，提高交易的效率。

法定数字货币可以被追踪能够反洗钱、反腐败、防逃税

金融界：区块链、比特币，以及央行的数字货币，这三者之间究竟有什么样的区别和联系？

李礼辉：区块链是一种技术，它的底层技术包括智能合约、加密技术、共识机制等，这些底层技术使区块链区别于其他一些技术，例如大数据、人工智能等。这几年出现的“代币”应用了区块链的某些技术，更多的是披上区块链外衣来吸引大家的眼球，吸引投资者参与众筹融资。其中，绝大多数的代币融资并没有经过金融监管部门的批准，而且可能会涉及非法集资。

比特币之类的代币，虽然应用了某些区块链技术，披上了区块链外衣，但它本身并不是区块链全部，更不是区块链的本身。所以，把“代币”与区块链等同起来，是不恰当的。

与法定货币一样，法定数字货币应该是有区域的，有主权背书、有合格的发行责任主体，才能够成为法定数字货币。比特币及其他代币与法定数字货币最大的区别在于，比特币及其他代币只是在参与者认可的小范围内、虚拟社区内存在，没有主权背书，也没有合格的发行责任主体。

此外，一些代币本身也存在弊端，例如地下匿名交易、跨境非法流通。目前，一些非法交易，包括毒品、枪支就使用某些代币作为支付工具。与此同时必须看到，这些代币在参与者认可的虚拟社区范围内，实际上已经成为一种支付手段，成为一种记账单位，而且可以通过一些交易平台，与金融市场连接，可以与法定货币兑换，在这种情况下，代币已经

具备了金融工具的某些属性，因而必须纳入金融监督和管控的范围。

金融界：您认为央行的数字货币有可能替代传统的货币，成为一种主要的货币形式？

李礼辉：法定数字货币本身的信息是可以追踪的，并且效率可能更高。一是，法定数字货币有利于央行准确控制货币流量。二是用区块链技术研发法定数字货币，所有的资金流都是可以追踪的，对于反洗钱、反腐败、防逃税等有积极作用。

法定数字货币能否取代传统的支付工具？这个问题需要考虑成本、效率、可靠性，以及法定地位。

现在的支付宝和微信支付当然不是货币，而只是一种支付工具。这类电子支付工具在日常的小额交易中非常方便、效率很高且覆盖面很大。法定数字货币相对于这样一些新的支付工具，不一定有特别大的优势，在成本和便捷性方面与新的支付工具相比，法定数字货币并没有太大竞争力。

不过，在金融资产交易方面，例如证券交易、外汇交易、资产托管、数字票据等领域，法定数字货币将会有优势。

区块链技术金融应用已取得突破

金融界：目前包括中国、美国、日本在内，很多国家都从国家的层面上对区块链进行了布局。与海外相比，中国在区块链的研发和应用方面处于何种阶段？

李礼辉：区块链技术目前还处于初步发展阶段。2016 年以前，区块链金融应用并没有取得太大突破，在规模化应用方面没有取得太大进展。

不过，2017 年已初见曙光，在多方参与、复杂交易的场景中已有较成功应用，包括前面提到的微众银行、邮政储蓄银行的系统都运行得不错。

在规模化应用方面，区块链可能还有很长的路要走。因为科技金融、数字金融有两个最基本的要求：第一就是规模化。比如外汇交易、证券交易，每秒交易可能达到几千笔、几万笔，这属于规模化的应用。目前的区块链技术有了突破，但也只能做到每秒几百笔一千笔的交易。

第二就是可靠性、安全性的要求。这个是新技术金融应用的最基本要求。比如加密系统，加密要求太严格速度就会慢下来，但如果追求较高的速度可能会牺牲可靠性方面的某些要求，既可靠又快速的系统研发仍需要一个发展过程。

与其国家相比，中国在区块链技术研发方面走在全球的前列。刚才提到的应用都在中国出现，目前央行在主导法定数字货币、数字票据的研究，中国在区块链研发方面还有一个很突出的特点，这就是大中小微型金融机构、科研机构都投身其中。

不同国家对于区块链的态度不完全一样。我国对于区块链的发展态度趋于审慎。例如对代币发行，我国是及时采取措施加以限制，事实证明这样的限制是非常必要的。不过，也有国家采取宽松政策，例如，去年 9 月我们叫停 ICO 和代币平台，但日本却批准了 11 家代币交易机构，并且在去年三四月份，就已承认比特币的合法性。

金融界：近期针对区块链的炒作非常火热，深交所也及时地出台了监管的措施。想请问您觉得监管政策会如何影响区块链的发展，在数字金融当中监管应该扮演什么样的角色？

李礼辉：金融业涉及众多的投资者、消费者。从监管角度来看，有两个重要的出发点：一要防止发生系统性风险，二要保护金融消费者和投

资者的利益。

基于此，目前推行的各类金融创新，包括区块链金融、数字金融、智慧金融、大数据金融等，只要可能会侵犯金融消费者的利益，可能影响整个金融市场的稳定，造成系统性的金融风险，监管肯定是要出手管控的。

就中国的具体情况而言，大部分的金融消费者、金融投资者对于金融风险的认识，对于区块链技术特征的认知并不是那么到位，他们绝大多数都只是跟随者，因而国家有责任来保护他们，维护金融市场的稳定。

数字金融前景广阔制度建设是最大挑战

金融界：现在数字金融的应用研发已经在路上了，您怎么看数字金融未来的发展趋势。

李礼辉：数字金融应该会发展很快。过去的金融世界是平面的，随着数字金融的发展，这种平面的空间被折叠起来，变成了一个立体的金融空间。人与人的之间的距离，人与金融产品、金融服务之间的距离变得越来越短。大数据在推进普惠金融发展方面已经取得了不错的成就，人工智能打造智慧金融也取得初步的成功。

与此同时，区块链在多方参与复杂的金融交易场景中，也已经表现出一些优势。此外，云计算技术应用，也已经取得很大的成果。这种新技术业态的金融应用，以后会出现更多的技术融合，例如，大数据和区块链技术的融合，大数据和人工智能技术的融合，可以解决包括智能信用评估、智能投资顾问、智能风险管控等问题。

数字金融的发展应该有很大的前景，而且会发展得非常快。罗兰贝

格咨询去年 11 月份发表的一个咨询报告称，中国将人工智能技术应用于金融领域，可以带来 6000 亿人民币的价值。巨大的市场空间推动下，技术也会日渐趋于成熟。

金融界：这个过程当中是否也会有一些挑战存在？

李礼辉：第一个挑战来自于制度建设方面。这些新的金融业态实际上重构了传统的金融业态，制度建设如何跟上非常重要。其中，不仅包括标准化建设，同时也包含金融监管制度的建设。这种金融监管的制度包括对机构、对产品、对服务渠道的监管，可能都要重构。希望我国在这个方面走得更快。

第二个挑战来自于技术层面。当推出一个新的系统时，如何评价系统是否有漏洞和技术后门，漏洞和应用是否会被人利用，这些都是潜在隐患。除此之外，从一种大的中心结构向分布式中心结构转变时，如何去做安全管控，防止黑客冲击，这些问题都需要重新定义和研究。这两方面的挑战在数字金融未来的发展过程中会变得更加重要。

金融界：请简单概括一下您对数字金融未来发展的期望？

李礼辉：我希望数字金融能够发展得更快更好，给老百姓，给大中小微企业，带来更多金融上的便利，能够让更多的人享受金融给他们带来的好处。同时我也希望，在发展的过程中，所有的风险都能够得到比较有效和比较适当的管控，这样才有可能保证数字金融这个新金融业态顺利健康发展。

（李礼辉，第十二届全国人大财政经济委员会委员，中国互联网金融协会区块链研究工作组组长）

来源：金融界网站

中国区块链产业发展的有利条件

我国拥有世界上最大的互联网应用市场，区块链产业具备走在世界前列的众多有利条件。应用场景的多元化，推动了区块链技术迅速发展；但同时，速度问题严重制约了区块链走向多场景应用。我国企业需要吸纳全球顶尖科技资源，建立中国区块链生态联盟，加快技术攻关步伐。

近日，工信部直属中国电子信息产业发展研究院会同北京天德科技有限公司发起设立的赛迪（青岛）区块链研究院落户青岛。我国千人计划专家、北航数字科技与区块链实验室主任蔡维德成为该项目首席科学家。他认为，我国区块链产业有望走在世界前列。

“区块链是一种分布式数据库系统，特点是不易篡改、很难伪造、可追溯。区块链记录发生交易的所有信息，一旦数据进入区块链，即使是内部工作人员也很难在其中做任何更改而不被发现。这个特点决定了其与互联网应用密不可分。”蔡维德告诉记者，“应用场景越大、越丰富，区块链技术和产业的发展就会越快。我国拥有世界上最大的互联网应用市场，因而区块链产业具备走在世界前列的众多有利条件”。

当前，区块链已在多个领域开始应用。8 月 28 日，国内首家区块链电商“媒购”面世，这也是全球首家区块链电商；8 月 17 日，“百度・长

安新生·天风 2017 年第一期资产支持专项计划”获上交所批准，百度金融作为其技术服务商搭建了区块链服务端 BaaS；前不久，信美爱心救助账户采用了蚂蚁金服区块链技术，用算法和技术架构解决多个弱信任机构间的信任问题，构建信任机制。

蔡维德认为，应用场景多元化，是区块链技术迅速发展的最大动力。“传统区块链技术速度慢，如比特币 1 秒只能做 3 笔交易，可上海股票交易所的交易量达每秒数万笔。如果不能解决速度问题，区块链多场景应用就不可能推广。”

强大市场需求和技术障碍之间的矛盾，促使众多科技企业加快攻关。3 月份，北京天德科技有限公司发布新一代区块链系统高新一号，在一家清算所实测平均交易速度超过每秒 4000 笔；其正在试验中的最新系统，已经做到每秒处理 33.34 亿次交易。2008 年至 2017 年，我国区块链技术领域专利申请数量全球第一，共递交 550 份专利申请，超过排名第二位的美国（专利申请数 284 份）。

蔡维德认为，这并非说明我国在区块链领域已做到世界第一。要真正走在世界前列，需要打造一个开放的生态系统，采取分享模式，吸收全球顶尖科技资源，减少无谓竞争，才能保证我国走在世界区块链产业前列。

“鉴于此，赛迪区块链研究院将联合金融领域研究机构、国家大数据（贵州）综合实验区区块链互联网实验室、青岛天德信链信息科技有限公司等单位，建立中国区块链生态联盟，并将推出三个面向全国的重点产业实施计划。”

蔡维德说，首先要建立中国区块链沙盒计划。该计划包含产业沙盒、保护伞沙盒和监管沙盒。其中，产业沙盒是在行业联盟指导下由企业自

行测试和评估工作；保护伞沙盒则由政府监管部门支持，委托权威机构评估区块链；监管沙盒是由产业发展到一定程度，且监管机制成熟后，直接由监管机构实施的区块链评估。“第一期首先推出产业沙盒后，将与监管机构密切合作推进保护伞沙盒和监管沙盒建设。”

蔡维德说，第二个计划是成立青岛区块链沙盒研究中心。该中心将推广中国区块链沙盒计划，通过政府、金融主管机构、高校及科研单位、产业基金及科技公司共同研究拓展沙盒计划。建立物联网、电子支付、保险、物流、医疗、海关区块链沙盒。

“最后一个计划是要搭建开放、共享的区块链沙盒测试与监控平台。该平台已建立我国首个支持区块链自动化处理的平台原型，支持金融监管、食药溯源、物流追踪、支付清结算等区块链应用。”蔡维德说。

（刘　成）

来源：《经济日报》

四、区块链发展带来新挑战

区块链的治理规则总体由区块链参与者设定的规则组成，规则本身又分为两大层面：一是技术层面的治理规则，由软件、协议、程序、算法、配套设施等技术要素构成。二是技术外部的、监管法规层面的治理规则，由法规框架、条文、行业政策等组成。兼顾两者，才更有利于保护参与者乃至全社会的广泛利益。

——《中国区块链技术和应用发展白皮书》

区块链是机会更是挑战

2018 年开局，区块链以一种让人摸不清头脑的姿态迅速大热，一时间，甚至连邻居大妈都在问区块链是什么……耳边也经常能听到这样的描述："二十年之后，人们会像今天谈论互联网一样谈论比特币，100% 的交易都会在区块链上完成"又或"如今已经进入'区块链 +'的时代了，不懂区块链相当于新时代文盲"，诸如此类的乐观预测像病毒一样在投资界传播、流行，造就出一场始料未及的狂欢。

甚至有人评价："区块链是世界第九大奇迹"。目前没有任何一种技术像区块链那样，会给未来社会的变革带来如此浩瀚的可能性。对此，安邦智库（ANBOUND）研究人员综合众多专家学者的观点，提醒投资者，面对区块链发展迅猛的势头，应冷静思考，做出理性判断，客观地看待接纳新生事物。

资本市场摩拳擦掌不甘寂寞

目前，在美股市场上，沉寂多年的胶卷制造商柯达，日前宣布发布柯达币，2018 年以来股价上涨 245.16%；中概股迅雷、第九城市、人人网、

中网在线等也因为涉及区块链业务而大涨。港股市场甚至出现了一则让人哭笑不得的消息：一家名叫“坪山茶叶”的公司宣布改名为区块链集团，在 A 股区块链概念大炒作的背景下，竟然也上涨了 23%。

不过，这场狂飙突进的资本盛宴，并非空穴来风。根据麦肯锡发布的区块链效用路线图，2017~2020 年将会是区块链技术基础设施的成型阶段。当前世界各大投行、科技公司纷纷加快其在区块链的布局。

主流观点认为，区块链经济的核心不在技术，而在于商业逻辑的重构。因此，这不仅仅是一场技术革命，更是一场认知革命。许多互联网界的大佬级人物看到了区块链技术的发展趋势与巨大潜力，纷纷打算做相应的布局与转型。国际上尽管有投资老将巴菲特与他更老的搭档芒格老大爷唱衰比特币的投资，但是更多的是各个主流投资人开始关注，甚至试水区块链与数字货币的投资。

最近，最引人注意的是脸书（Facebook）CEO 扎克伯格明确表态 2018 年他的重要任务就是把加密货币的新技术结合到公司的社交产品上去。随着去年对比特币升值 1700% 的铺天盖地的报道，这到底是个泡沫还是未来的争论引起了广大投资者的普遍关注。

许多保守谨慎的投资者也纷纷试水，用自己资产中的一小部分尝试购买，这个稳健的试水理财方式，业界认为是稳妥的，但坚决不鼓励加杠杆。事实上，数字货币的投资已经是全球性的现象，这也意味着，每个人的财富管理服务从今以后都会有一个新选项：数字货币，即在做个人理财时，可以拿出一小部分的资产做数字货币的投资。

但我们也必须清醒地认识到，凡是有名利的地方，就必然有灾祸，数字货币投资也是，有猛涨必然有暴跌，并且很多人压根儿就没有投资资格，涨了开心，跌了闹心，一时得了的便宜，迟早还会还回去。

多场景应用下的各种风险不容忽略

随着比特币近年来的快速发展与普及，区块链技术的研究与应用引起了政府部门、金融机构、科研企业和资本市场等领域的广泛关注。多场景的应用是“区块链 +”时代的标志，如

1. 区块链可应用于金融行业的支付、交易清结算、贸易金融、股权（私募、公募）、债券、金融衍生品（期货、期权、次贷、票据）的交易、众筹、信贷、风控、征信等方面。

2. 区块链可应用于医疗行业的医生预约、数字病历（体检记录、医疗记录、诊断记录、病人病历等）、隐私保护、健康管理等方面。另外在药品、医疗器械及配件来源追踪、审计方面也有较好的应用场景。

3. 区块链防伪、防篡改的特性能够广泛应用于政府主管的产权、物权、使用权、知识产权和各类权益的登记方面，如地契、房地产权证、车辆登记证、营业许可证、专利、著作权、商标保护、软件许可、游戏许可、音频许可、视频许可、书籍许可、建筑许可、艺术品证明、档案管理、遗产继承、个人社会信用、电子护照、合同、证书、学位、成绩、账号等方面的公共记录登记。

4. 利用区块链的智能合约，可以通过接口和物理世界做程序对接，实现物品可溯源、可防伪、可认证，提高网络的安全性、可用性、可靠性，达到区块链上一手交钱、物理世界一手交货的交易效果。

5. 在能源行业的发电、输电、用电、储电及金融交易等环节，区块链技术可以被充分使用。如，可以提供公正、透明的能源交易多边市场和碳交易市场，以达到降低对手信用风险，同时减少支付和结算成本、

提高效率的目的。

同时，可以根据发电、配电、输电、调度、用电、售电信息，提供公正、可溯源、透明的审计、监管记录。另外，在教育、保险、慈善公益、交通、文化娱乐、工业制造等行业同样拥有着广泛的应用场景。凡是数据上有防篡改、审计的需求，业务上涉及交易、结算、清算、仲裁的行业，都是区块链 + 的潜在应用对象。

由此可见，区块链的应用范围在不断扩展的同时，区块链本身也在不断地进行技术革新。除了以比特币为代表的公有链，目前还出现了联盟共享的联盟链，企业内部的私有链。为了降低主链的存储负担，提升交易处理效率，研究人员提出了侧链技术、闪电网络技术。

比特币经过近 8 年的实际运行，其安全机制承受住了理论和实践的考验。然而，现在众多的区块链应用为了提高效率，适应特定行业的需求，对底层结构和算法进行了大量的改变，由此，安全风险也随之而来。

2014 年 12 月 8 日，blockchain.info 爆出随机数问题；世界知名交易所 Bitfinex 因为多重签名缺陷导致 12 万个比特币，6800 万美元的损失；2016 年 6 月 17 日，最大众筹（1.5 亿美元）项目 TheDAO 被攻击，损失超过 6000 万美元数字货币；2016 年 8 月，以太坊的复制品 Krypton 受到了 51% 算力的攻击，导致 Bittrex 的钱包中共计 21465 个 KR 被盗取，价值约 3000 美金。

因此，区块链应用出现的安全问题无疑对“区块链 +”各行业给出了重要警示，尤其安全性威胁将是“区块链 +”时代面临的最重要的问题之一。

对区块链技术的质疑尚未消除

第一，区块链真的能完全实现去中心化吗？由于智能合约的代码漏洞，导致 TheDAO 被黑客攻击并转移走价值 6000 万美元的数字货币。在挽回损失的过程中，去中心化机制未能解决问题，因为智能合约的代码一旦发布出去，就无法更改，所以只能通过“集中式”的方式，先采用“软分叉”锁定账号，再采用“硬分叉”转移以太币，才解决这个问题。

但这也导致了以太坊社区的分裂，产生了 ETH 和 ETC 两种同源又不同价格的数字货币，给以太坊生态系统带来了严重的负面影响。此次事件，值得所有业内人士针对区块链的“去中心化”进行反思。

第二，矿池算力集中，但仍存在 51% 的攻击问题。以公共区块链分布式账本为基础的加密货币，如比特币、以太币等，需要分布在世界各地的矿工不停地运作来维持系统功能。随着全网算力的不断增加，单打独斗的小矿工已经没有规模的优势，为了使收入更加平稳，矿工们可以组成矿池。

矿池能够给矿工带来稳定的收入，但是也带来了新的问题。矿池会把分散的算力集中统一管理，随着矿池规模的不断扩大，算力总和达到或超过全网的 51% 时，从理论上说，就能够控制区块链的记账权，攻击者将可以修改账本和阻止他人挖矿，从而威胁整个系统的安全。

第三，密码算法的使用及密码协议的引入存在隐患。区块链技术目前涉猎随机数生成算法、哈希算法、数字签名算法等。而算法本身的漏洞或存在的后门对区块链系统的影响是不可估量的。当今设计的密码算法主要是可证明安全和计算上安全的算法，并非绝对安全的算法。

随着密码分析技术的进步以及人类计算能力的逐步提升，很多密码算法将会暴露出弱点。2004 年，国内密码学家王小云破解 MD5 等，揭示哈希函数的碰撞破解只是时间问题；2016 年，NIST 在标准随机数发生器算法中内置有后门。同时，零知识证明、承诺协议、安全多发计算等密码协议的引入，使得协议安全也将成为区块链不能小觑的风险点。

第四，不具备真正的匿名性，使得隐私性无法保障。瑞士苏黎世联邦理工学院和德国 NEC 欧洲实验室的学者们研究发现，即使采用了隐私保护措施，40% 的比特币用户身份信息仍然能够被识别出来。因为比特币的每一笔交易都会公开在区块链账本上，通过各种数据挖掘技术，分析每个地址发生过的交易，就可以发现很多账号之间的关系。

从积极的方面说，政府监管机构可以从中发现洗黑钱、行贿等犯罪行为；然而从消极的方面说，用户的隐私无从保障，一旦真实身份泄漏，所有的交易将暴露在公众面前。在当下的大数据时代，各行业在使用区块链技术时，采取怎样的隐私保护策略，将是研究的主要问题之一。

第五，“钱包”的安全防护还得打个问号？私有密钥是需要比特币用户自己保管和保密的账号信息，所以“钱包”的安全性是至关重要的，一旦丢失私钥，基于比特币的去中心化机制，用户则无法进行私钥重置，也就意味着将无法拿走账号里的比特币。

目前，私钥可以通过在线钱包、冷钱包、硬件存储（USB）、门限秘密共享存储、纸质媒介、人类记忆等方式进行保护。随着云计算的流行，出现了在线钱包的 SaaS（Software as aService）云服务，相当于密钥托管给一个可信机构，但这违背了区块链的去中心化思想；硬件存储虽然相对安全，但存在硬件丢失或破坏的风险；虽然通过纸质存储并保存进保险柜的方式可行，但不适用于频繁交易的资产。因此，根据区块链

的应用需求和资产情况，安全便利的“钱包”保护机制尤为重要。

第六，新技术、新应用带来新问题。为了进一步提升比特币特殊机制下的交易效率，研究人员提出了很多安全机制，如 POS（权益证明）机制、DPOS（授权股份证明）机制、PBFT（实用拜占庭容错算法）机制等。其中，为了解决 POW（工作量证明）机制浪费算力的问题，研究人员提出了 POS 机制，但是 POS 机制又带来了新的问题，即区块分叉时的“无利害关系”N@S（Nothing at Stake）攻击问题。

为了适应多行业的业务发展，联盟链以及私有链成为更优的选择。公有链的安全性由全体网络节点共同维护，但这种结构导致任何一笔交易都能够被所有用户检测。所以公有链的特性是银行等企业不能接受的，为此可以通过联盟链或者私有链在企业之间、企业内部之间搭建一个共享的、高效交易系统或者数据分享系统。不管是联盟链还是私有链，对于企业来说，安全运营是首要的，但目前国内外还没有较好的安全检测方法。

风险评估

近年来市场热度的持续升温和数字货币的持续走热，引发了越来越多的专家、学者和业内人士高度关注区块链技术的应用和创新。但是通过分析，我们发现“区块链 +”时代的到来挑战大于机会，尚存在很多没有解决的问题，目前还处在修炼内功的阶段。

要知道，区块链要改变别人，首先要反思，改变自己。在任何领域跨界应用的时候应先关注在这个行业中真正的落脚点是什么。无论是商业领域还是别的什么领域，最根本的是搞清楚区块链能解决的是什么问

题。因此，在区块链火爆的热潮下，我们要保持一份理性和冷静，区块链产业还存在很多缺陷尚处于萌芽阶段，但不可否认的是未来这块很有可能给经济模式和商业结构带来巨大的改变，让我们拭目以待。

来源：ANBOUND 产业研究中心

量子计算能攻破区块链吗

颠覆性、划时代、革命性……量子计算光环太多，又有不近人情的“高冷”。另一边，开年以来，区块链火得一塌糊涂。网上热传的“3 点钟不眠区块链社群”，神秘而火爆。

最近，它俩不期而遇了。据外媒报道，一台具有 4000 个以上量子比特的量子计算机就能瓦解区块链。若有人能做出这样的量子计算机，就能解出并验证每笔交易，未来产生的所有加密货币都会被其垄断，加密货币的信任系统也将被瓦解。

这听起来很可怕。俩“神仙”似乎要打架，是真有此事还是杞人忧天？

“攻链”威胁从何而来

在量子计算威胁区块链的相关论述中，持有此观点的一方给出的论据主要包括两点：一是量子计算会威胁比特币的安全协议；二是算力更大的量子计算机能垄断“挖矿”。

诞生于 2009 年的比特币是区块链技术最著名的应用。比特币的安全

协议涉及两种类型的密码学，即挖掘过程中使用的散列函数和用于在区块链上提供数字签名的非对称密码术。

在“击破论”支持者看来，量子计算机可能会对这两道安全防线产生巨大威胁。未来，量子计算机能很快破解哈希函数，从而垄断整个区块链，让比特币的安全协议“作废”。

“挖矿”是指利用芯片的计算能力，在比特币全球网络中不断进行哈希运算，比对手更快地求解，找出符合特定要求的随机数，以此赢得在公开账簿上的记账权，从而获得系统奖励的比特币。本质上，“挖矿”是个数学问题。

比特币常说的“51% 攻击”就是指在区块链中，如果一个矿工组拥有整个网络 51% 的算力，他们就会永远比其他拥有 49% 算力的矿工组更快地处理区块。也就是说，他们将垄断整个区块链，得到之后产生的所有比特币。

针对量子计算机威胁“挖矿”的问题，来自新加坡国立大学的戴夫士·阿加沃尔和该校研究人员在 2017 年 10 月发表了相关论文。他们认为，至少在未来十年内，ASIC 矿机（使用 ASIC 芯片作为算力核心的矿机）的“挖矿”速度会比量子计算机快，但十年后量子计算机的“挖矿”速度将大幅提升。

“攻破”一说为时尚早

针对“4000 量子比特的量子计算机能瓦解区块链”的说法，中科院微电子研究所集成电路先导工艺研发中心研究员吴振华表示这并非空口无凭。

“这个是有依据的，是比对了枚举法破解区块链所需要的计算能力和4000个量子比特的计算能力之后做出的判断。当然要求也很高，需要4000个量子纠缠的比特，同时要保证极低的错误率。”吴振华解释说。

而现实情况是，目前的量子计算机最多实现72比特的计算能力，并且越往上增加难度越大。

作为国内最早的区块链技术研究者之一，中科院自动化所副研究员袁勇的态度非常明确：“总体上来说，我不太认同量子计算对区块链产生威胁（的说法）。”

“首先，对方并没有以发展的眼光来看待问题。量子计算和区块链，或者说量子计算跟密码学一定会呈现共生演化的趋势，二者互相促进，不能用十年后的量子计算与现有的比特币密码体系相提并论。”袁勇说，“我相信密码学体系和区块链的技术一定会有相应的手段应对量子计算的威胁。”

针对量子计算算力惊人的观点，袁勇也予以了反驳。据他介绍，比特币的共识算法是以算力为基础的，因此可能面临量子计算的威胁。但是区块链技术体系中的共识算法自PoW（即Proof of Work，工作量证明机制）之后，呈现出百花齐放的发展态势，目前至少已有30余种共识算法。很多其他加密货币的共识算法都不是以算力挖矿为基础，例如权益记账、代表记账、随机记账等。此外，还有Paxos和Raft传统分布式一致性算法可以运用，这些共识协议在很大程度上可以抵御量子计算攻击。所以，如果量子计算确实产生威胁，区块链可以通过切换共识协议来解决。

袁勇解释说：“当然，这些新共识协议，特别是用于公有链的共识协议，还未能证明其有效性，目前最安全的还是比特币的PoW共识。但这

些共识算法的未来可期，我们实际上有很多选择。”

袁勇笑道：“量子计算对比特币有威胁，但它对传统银行体系的威胁更大。天塌下来有个子高的顶着，以体量来说，还轮不到比特币‘杞人忧天’。”

短期内或难实现“量子霸权”

量子计算近来捷报频传。3 月 6 日，谷歌宣布推出一款 72 个量子比特的通用量子计算机 Bristlecone（“狐尾松”），其错误率低至 1%，与 9 个量子比特的量子计算机持平。此前，IBM 刚刚曝光其 50 个量子比特量子原型机的内部构造。

本土力量也不甘示弱。近日，中科院院士、中国科学技术大学常务副校长潘建伟正式发布中科院联合阿里云打造的 11 量子比特超导量子计算的云平台，这是继 IBM 后全球第二家向公众提供 10 量子比特以上超导量子计算云服务的系统。郭光灿院士团队也介绍其本源量子计算云平台已成功上线 32 比特量子虚拟机，并已实现了 64 量子比特的量子电路模拟，打破 IBM Q 的 56 位仿真纪录。

这一系列动作，让今年的“量子霸权”争夺战来得比预期更早。“量子霸权”又被称作量子优越性，即 50 量子比特的量子计算机优于现在的任何一台经典计算机，达到“量子霸权”才算真正意义上的量子计算机。

量子计算可以颠覆现有计算行业，它能轻易通过枚举算法解决大量现有复杂算法才能解决的问题，对量子效应实现直接模拟仿真。但吴振华表示：“虽然量子计算的功力没有被夸大，但它的实现难度很大。由于种种原因，现在很多观点或报道（对量子计算的预期）过于乐观。”

谷歌推出的量子计算器 Bristlecone 能够支持多达 72 个量子位，号称“为构建大型量子计算机提供了极具说服力的原理证明”。而如果能将量子处理器的错误率控制在足够低的水平，在解决明确的计算科学问题时就能超越传统硅计算机，实现所谓的“量子霸权”。

但实现“量子霸权”要克服很多困难，何时成真还没有定论。

量子计算伴有噪声，即随机波动和错误。对此，技术乐观派们认为“降噪”是个技术性、工程性难题，迟早可以解决。

另一拨人却不这么想。耶路撒冷希伯来大学数学家吉尔·卡拉伊是反量子计算的代表人物，他一直关注量子计算复杂度与噪声问题。在他看来，噪声的降低必然伴随着量子比特数指数式的增加。由于后者无法实现，因此“量子霸权”也难以实现。

（崔　爽）

来源：《科技日报》

比特币、区块链及其法律变革

问题的提出：10 亿人民币买两个披萨

什么是“比特币”？什么是“区块链”？这些概念已被社会广泛关注。从 2009 年中本聪提出比特币概念至今，短短不到 10 年，比特币竟然已成为全球通用的“货币”，而且它的价格还在向上攀升，截止到昨天，每一个比特币价值近乎 16000 美元（约合 10 万人民币）。如果拉斯罗 . 汗耶茨（Laszlo Hanyecz）听到这个消息，估计要跳楼，他可以说是比特币历史上最悲催的主人公。在比特币产生初期（2010 年 5 月），他曾拥有过 1 万比特币，当时比特币还不被人们看好，他就用这 1 万比特币买了两个披萨，当时 1 万比特币市值约 30 美元，时至今日价值约 10 亿人民币。

一直以来我有一直有一个疑问：“区块链”技术到底好在哪？为什么“比特币”——这样一个非官方发行的货币竟然会火得一塌糊涂？直至 HOW 实验室真正布局区块链技术，本人也亲自试验了“区块链”技术（包括布局智能合约），才真正发现它具有传统技术无可比拟的“信用优

势”！我尽可能用最简单的语言来描述它与传统技术的区别：传统互联网主张实名制，试图通过实名认证构建信用体系；然而“区块链”恰好相反，它完全是匿名的，例如在比特币的交易，买家根本不知道卖家是谁，但每个人都会遵守信用，真正完成了一个“匿名”社会下的信用构建，它到底是如何做到的？稍后本文将通过一系列的实验结果揭晓这一秘密。

“信用”是法律的基础，任何法律无一不是构建“信用”基础上的。“诚实信用”是私法体系的帝王法则，“罪刑法定”体现的是公法领域的国家信用。没有的了信用，也就没有了法律的信仰。区块链技术带给我们的全新的信用体系，可以大胆想象，它所撼动的不仅仅是传统货币，甚至是传统信用体系的社会制度。洞察区块链技术背后的法律本质，预测它对社会制度的冲击和影响，将成为这里的重点。

区块链：匿名社会的信用

1. 区块链不等于 AI：前者是“信用”，后者是“智能”

很多人将区块链和 AI（人工智能）混在一起，这是一个基本的常识错误。我在实验中同时用到人工智能技术和区块链技术，可以说这完全是二门不同的技术。人工智能的技术点在于“智能化”，以神经网络布局为例，它能够计算出人脑无法想象的结果，这是人工智能的特点。然而，区块链技术缺乏智能化的特点。恰好相反，区块链的运行速度甚至还不及普通程序快，以付款为例，通过区块链完成付款往往要几分钟后才能付款成功，原因在于区块链技术需要制作和同步账本，需要大多数结点都收到这个账本后才视为付款成功。

因此，区块链技术最大的优势在于“信用”，并且是匿名信用！传统的编程思想是“中心主义”的，比如一个网站或者一个 App 是架设在一个中心服务器上，这个服务器就是绝对的中心，任何人使用网站或者 App，本质上就是在访问这个中心服务器，这依然是当下主流的编程思想，我在 HOW 实验室做的绝大多数实验也都是采用是中心主义思想。然而，区块链技术的创新就在于“去中心化”，以当下流行的比特币为例，完全没有一个中心服务器，每个人都会有一个“账本”（电子化的）来记录自区块链产生开始至今所有的交易记录。

我在试验中还发现，当一个新的结点加入到区块链之后（如用 geth 语言连接），首要的第一件事便是同步区块，程序会自动将所有账本上传到本机。

2. 区块链的关键词：区块（block）和链（chain）

区块链有二个关键词“区块”（block）和“链”（chain），所谓区块，可以理解为一个小账本，用计算机命令打开区块后就会发现，它记录了近 10 分钟的所有交易，所以可以把它理解为一个小账本。而所有区块按时间接点连接在一起就是“区块链”，一个总账本。“区块链”上的每一个结点都有一个总的账本。那么，这个账本是如何产生的呢？这要归功于矿工的功劳。（以下详述，此不赘述）

这里还要澄清一个“分布式”的概念。“区块链”实现了分布式数据存储，简单地说就是将账本同步给每一个结点。很多人将这里的“分布式”概念与大数据中的“分布式”概念混淆。这些技术我在实验室中亲自操作过，比如在大数据处理方面，我用到了“hadoop”和“spark”（大数据处理是人工智能的底层），这里的“分布式”运算的机理是将海量数

据打成一个个小的碎片，然而交给多台服务器（如成百上千台服务器）并行计算，从而实现海量数据的快速运算。然而，“区块链”中的“分布式”几乎与大数据没有任何关系，它的“分布式”，实质上是将每一个账本同步到网络的每一个结点，以比特币为例，整个账本才不到 70G（在大数据领域分布式计算领域，70G 简直不值一提），乙太币账本的账本更小，也就是说你的电脑硬盘如果大于 70G，你就可以申请成为区块链的一个结点。

3.“挖矿”挖的到底是什么？

在区块链技术中，有一个重要的角色叫“矿工”，他们通过挖矿获得“比特币”。事实上，所谓“挖矿”只是一个形象的描述，在计算机的世界中除了“0”和“1”的代码之外，别再无其他，更无所谓“金矿”一说。

这里的“挖矿”，在本质上是为区块链网络提供计算资源。前文所提及区块链中会同步账本给所有的结点，这就需要记账，谁来记账并且负责发布账本呢？这个人就“矿工”，由于他们为区块链网络做出了贡献，所以会赢得比特币（在以太坊中是以太币）。所谓“挖矿”实质上就是向整个区块链网络提供“算力”，负责制造和发布区块（block 即账本），它对电脑 cpu 和电量的消耗是很大的，我有一个直观的印象，每一次启动“挖矿”命令后，电脑 cup 的占用率都会超过 300%，电脑会热得像冬天里的烤火炉一样。

矿工们做出的贡献是需要肯定的，他们会基于挖矿而获得奖励（比特币或乙太币），区块链的技术设计是比较科学的，矿工们完成制作“区块”（账本），但却无法修改账本中的交易记录（通过加密技术这些交易记录无法篡改）。区块还将发给每一个结点，这样又进一步保证交易记录

的真实可靠，完全无法篡改的。这比中心服务器的信用要可靠得多！如果账本存在一个中心服务器中，无论是服务器管理者修改账本抑或是被黑客攻击，都意味着账本会被完全篡改。而在区块链中，几乎没有人可以篡改账本。如果是黑客想篡改这个账本，原来是黑进一台服务器即可，而现在是要黑掉所有结点上超过 51% 以上的电脑才可以，这几乎是无法完成的。

矿工的工作是制作账本，并将账本同步给每一个结点，从而保证交易记录的真实可靠。如果没有矿工挖矿，交易（Transaction）便无法进行，在构建联盟链的过程中我曾用计算机命令停止挖矿动作，此时，任何付款都将失效，道理很简单，在区块链中付款生效的条件，是这一笔交易被记录在区块中，并且这个区块发布给了区块链中绝大多数的人，而这一切又是由“挖矿”来完成的，如果没有了挖矿，这一切当然就无法生效。

智能合约（smart contract）的魅力？

1. 智能合约的二个关键词

“智能合约”（smart contract），有二个关键词，一个是“合约”（contract），一个是“智能”（smart）。对于“合约”的概念，大家并不陌生，“合约”即“合同”（也称协议），从传统的押字画押，演变到今天的电子契约，其本质就是合同。“智能合约”中的另一个较为重要的关键词即为“智能”（smart）。首先要澄清这里的“智能”与人工智能中的“智能”并非同一概念。这可以在二者的英文表述中得到区分，智能合同中

用的“smart”，而人工智能用的是“intelligence”。因此，如何理解这里的“智能”概念，也成为理解智能合约的关键所在！

2. 尼克·萨博（Nick Szabo）与智能合约

或许你没有听说过尼克·萨博（Nick Szabo），但一定听说过中本聪明，他是比特币的发明者，他也是一位很神秘的人物，几乎全世界都在猜测他是谁？2010 年 12 月 5 日，中本聪在比特币论坛里发了一个帖子后便神秘消失了。没有人知道他是谁，但有猜测他就是尼克·萨博。尼克·萨博何许人也？他便是“智能合约”概念的提出者，他是一位计算机科学家、加密大师，他在 1993 年左右提出“智能合约”的概念，就于 1994 年他写成了《智能合约》（Smart contracts）论文，是智能合约的开山之作。

近几年来，“智能合约”作为关键词，不断刷新人们的眼球。有很多朋友都曾向我提及过这个问题：啥叫智能合约？比特币之后又兴起的以太币，它所依赖的平台（以太坊），即允许用户自由布置智能合约。当然，在以太坊上部署一个智能合约是需要花费以太币的，因为它需要“矿工们”把智能合约的代码记录在区块里，并且发送给每一个结点，因此智能合约同样是不可修改的。

3. 理解智能合约，从“滴滴打车”开始

时下盛行的“滴滴”或“Uber”，可以理解为“智能合约”的雏形。乘客发出请求，司机做出承诺。在智能合约下，几乎不存在违约的情况，例如乘客打车后拒绝付款会被剥夺再次打车的权利。那么，在“滴滴打车”的样态中，司机与乘客的权利义务不是写在纸上，而是写进了计算

机代码，所有人的行为及后果均是由代码决定的，这便是“智能合约”的雏形。

怎样才能把传统协议变成智以合约呢？我抵押协议来例，在抵押协议中客户向银行做出承诺，如果届期不还钱，车辆归就归银行所有。如果要把它变成智能合约，就需要把这个承诺写进计算机代码，这在智能驾驶时代是可以实现，比如通过计算机代码的设置，客户届期未按时还钱，车辆将会拒绝客户使用，反倒是将驾驶权限（如新的使用密码）发送给银行，银行转而拥有车辆的使用权。因此，智能合约的本质在于将合约的履行或者违反合约的后果都写进计算机代码，由计算机程序自动执行。在智能合约下，任何任性的行为，计算机代码都会赋予其相应的代价。

与传统合约相比，智能合约的特质是清晰的：合约订立和履行是一体的，这也可以从根本上解决“执行难”的问题。传统合约的订立和履行是分离的，合同订立了但未必就能履行，法院在合约执行中依然发挥主导作用。然而，智能合约的订立和履行却是一体的，完全由计算机代码完成。在区块链中编辑“智能合约”的语言叫“solidity”（事实上，除了设置“智能合约”外，编程中很少用到“solidity”）。智能合约中的“smart”有“便捷”的意思，事实上，协议的自动履行倒是更符合智能合约的本质。

4. 区块链语境下的“智能合约”

为了进一步说明“区块链”语境下的智能合约，这里我引用 Lessig 在他的《代码：网络空间的法律》一书中的观点。为了解释代码在赛博空间（syberspace，可以理解为计算机程序所架构的空间）中的作用，

lessig 引入了“架构”的概念。根据物理空间的形状，你的身体可以穿梭其中，这一切是由它的架构决定的，例如建筑环境（建筑物、街道等）。按此道理，虚拟空间的形状则是由代码决定的，所有应用和协议就建立在代码上面。因此，代码便是虚拟空间的架构。法律和架构在管理参与者方面是皆然不同的。法律依赖于个人将规则内化为自觉进而规范人的行为，个人行为一旦超越了法律的界线还需要法院强制执行。然而，架构通过塑造空间本身管理行为，它既不依靠个人对规则的信仰，更不依靠法院执行。因此架构在效率上明显优于法律。依据架构执行合约时，不需要任何个人或者组织来决定如何执行合约，你可以称架构执行为自我执行（self-enforcing），在这种情况下，违约甚至不可能发生。

“区块链”语境下的“智能合约”，还有一个重要的特点：去中心化的，或者说它是不可修改的。“区块链”背景下的智能合约，则是分布在每一个结点（可以理解为一个服务器）上，它的内容是不可调整的。以借钱的合约为例，合约一旦订立，它就发布给每一个结点，合约内容不可更改；而且一旦届期，合约会自动从借款人账户中扣掉比特币或乙太币给借款人。

区块链背后的法律变革

1. 安全、公平、信用：传统法律价值的危机

现有财产制度大都围绕“资产”这一概念展开的。所有被称为“资产”的东西，都需要法律的保护，比如钱、股票、债券、音乐、知识产权等等。法律制度所要解决的恰恰是这些“资产”的所有、使用、管理、保护等

等一系列问题，物权法、合同法、证券法、知识产权法等均为如此。现代资产的管理是以政府或者金融中介为核心完成的，比如房屋交易需要到房管部门办理登记，证券交易需要到证券管理部门交易结算，银行转账同样需要由银行来最终确认。因此，当下的金融管理体系奉行的是中心管理模式，政府或者少数几家垄断金融机构便是财产管理的核心，他们拥有财产管理的一套账本，这套账本便是公民权利的最终评证。

如果黑客黑掉这套唯一的账本，公民的权利将会遭受巨大影响，很多银行、政府机构都曾遭受过黑客的攻击，就连摩根大通、美国联邦政府也难以幸免于难。中心账本所带来的安全隐患确实存在。比安全隐患更为严重的还是信用问题，中心账本，一家独大，如何保障账本的真实可靠一直都是民众关心的问题，就像手机收费，总有民众对于移动、联通这些大服务商们出现的错误计费愤愤不平。民众在创造财富的同时，总是希望能够得到公平的待遇，这种诉求也会与中心管理模式发生了急剧的冲突，以跨国银行转账为例，一般要收取 10% - 20% 的手续费，而且周期很长。

不可否认，长期以来，中心管理模式所爆发出来的安全、信用、公平等价值危机，愈演愈烈。或许可以从现代法律价值的危机中去寻找区块链技术盛行的动因，区块链技术旨在实现完全的“去中心化”和分布式账本，它所迎合的是去中心化的民主思潮！

中心记账所导致的系列危机，让人们产生了这样的联想：建立一个全世界统一的大账本，甚至每个公民都拥有这样一套账本，任何资产都可以通过它实现存储、转移、交易、管理等。区块链技术恰恰就是由这一伟大思想催生的产物。比特币的成功应用，恰恰反映这“去中心化”思想的成功。在这一基础上 Vitalik Buterin 又创建了乙太坊，不仅可以发

行电子货币，还可以在此基础上实现“智能合约”。毫无疑问，这一切对现在法律制度都将造成巨大冲击！

2. 区块链技术对“物权登记”的挑战

世界各国大多奉行“物权登记制度”。据统计世界上有 70% 的人对于土地拥有所有权，然而基于物权登记制度，他们当中的绝大多数拥有的十分脆弱的所有权，比如你在洪都拉斯拥有一套房屋，如果哪一天有一个独裁者上台了，只需要将政府账单上的名字改成别人，那么你将彻底失去这间房屋，这种事情在洪都拉斯时有发生。这种财产登记所带来的不安全感在很多地方都会存在，人们总是担心政局不稳或者政权交替而让自己的辛辛苦苦积累下来的财富付诸东流。

区块链技术则可以有效解除人们的顾虑，它所实现的是分布式账本，试想如果将房产登记在区块链上，这样就相当于每个公民都有一个房产登记的账本（匿名设置还可以有效保障人公民隐私），这样公民的财产就变得异常牢靠，传统的多数人记账信用也就转化为多数人信用，人们再也不用担心由于政权更替而导致房屋产权的变化。事实上，不仅不动产登记可以应用到区块链中，其他任何需要登记确权的财产制度，诸如知识产权登记制度等都可以和区块链技术相结合。

3. 区块链技术对“国际汇款”的挑战

据统计，从发达国家到发展中国家最大的资金流动便是汇款，那些背井离乡的人们总是不忘给老家人汇款，然而人们却需要支付高达 10—20% 的手续费，时间一般要 4—7 天才能完成。这一切所彰显恰是中心记账的不足，货币移转、结算需要耗费较长时间，管理者需要收取巨额

管理费用。

Abra 是一款基于区块链的应用，如果通过它来完成国际汇款一般只需要几分钟，手续费也只有 2%，它是如何完成的呢？比如，甲在 A 国向 B 国的乙汇款，甲在手机上完成汇款手续后，几分钟后在 B 国的乙就会通过手机查询到已收到该笔汇款。这时乙就会联系自己最近的“出纳员”，这位出纳员会将现金直接拿给乙。事实上之所以会这样快，并且手续费如此低廉，是因为整个交易是以比特币为媒介完成的，而没有通过跨国银行的转账系统。

可以想象，像比特币为越来越多的人所接受，人们更愿意通过它来完成交易，而并非是传统的银行。以银行为核心的传统金融体系也正面临着来自区块链技术的挑战。

4. 区块链技术对知识产权资产管理的挑战

当下的艺术创造市场还是完全掌握在一些大的平台手上，这让很多音乐人、艺术家很费解：努力创作却为他人作嫁衣，这也在一定程度上打击了源创艺术创作的积极性。然而，区块链技术却给了音乐人和艺术家自己当家作主的权利。获得格来美奖的音乐人伊莫金·希普就利用区块链技术设置了自己的应用“菌丝”，这让伊莫金·希普可以自由地管理自己的音乐，“我的地盘我作主”。根据智能合约，任何人要收听伊莫金·希普的歌曲，或者需要把它放到自己的影片中抑或是作为手机铃声，只需要支付不同的价格即可。更为重要的是，所有的交易记录以及评价记录都是绝对真实不可更改的，这也为其他人选择提供了最真实的参考。

结语

技术革新必将产生法律变革。时至今日，我们依旧在怀念互联网时代所带给全社会的制度变革，甚至看着川流不息的人群小偷们也哭了……无现金的生活，让他无从下手，现在几乎人人都不带现金出门，一切都靠手机小偷——一个存在了几千年的职业就这么被毁了。事实证明，最终干掉小偷的不是警察，而是互联网……

比特币，一个不需要任何政府组织出来站台的货币，竟然成为全球通用货币，区块链技术所彰显的生命力令人吃惊！当然，区块链还仅仅是一个新生事物，它带给社会的到底是什么？这仍然是一个需要我们继续探所的话题！所有人的在激动、兴奋后还带有一丝恐惧和迷茫！一方面，区块链技术还存在诸多缺点，诸如一旦发布智能合约就难以再次修改（这与中心服务器模式不同），这也给人们的应用带来了诸多困难；另一方面，利用区块链技术发行的货币的合法性问题也是备受争议，2017 年 9 月 4 日，央行等 7 部委叫停了各类代币发行（ICO）融资活动，当天还导致比特币、以太币的价格都大幅跳水。新生事物就是这样，它要历经质疑、论证、甚至恐惧和迷茫！

然而，全球化格局下民主思想的原动力不可小视！这可以从近期比特币价格又大幅反弹效果再一次得到印证。大禹治水的方法再次教导我们，对于像区块链这些新兴技术，不能简单划归洪水猛兽，努力洞察、善加利用或许是更好的办法！

（杨延超，中国知识产权交易网——知易网创始人）

来源：《经济参考报》

区块链对金融领域的冲击和影响

区块链应用的最大挑战在于金融服务和数据服务的“模糊地带”。毫无疑问，区块链技术对金融的核心作用，是依托新的模式来确定价值、储存价值和交易价值。实际上，分布式技术最终影响的是人的“身份信息”在金融意义上的体现，即账户形态。在区块链引领从信息互联网向价值互联网的过渡中，这一挑战始终存在，需高度关注监管适应性、风险控制等问题。

作为比特币背后的分布式账本技术，区块链的热潮似乎已经无可阻挡。无论是积极拥抱，还是存有疑虑，人们都开始正视区块链究竟给经济金融带来怎样的冲击。

从理论上讲，区块链技术的应用范畴，可以涵盖货币、金融、经济、社会的诸多领域，但现实中并非这么简单。本质上看，区块链技术发展仍然处于萌芽和完善阶段，亟须“呵护”和避免“捧杀”。尤其是在金融领域，其行业特殊性及我国面临的独有格局，都需要我们深刻思考一系列重大难题与挑战。

挑战之一：区块链技术能否真正“练好内功”

正如“一千个人眼中有一千个哈姆雷特”，随着区块链的日益火爆，人们对其解读也“五花八门”。原本坚持“去中心化”“不可篡改”的内在特质，在现实中也逐渐动摇。由此，当我们在讨论区块链技术时，可能需要跳出比特币、以太坊等典型案例的约束，更准确地描述区块链技术不变的本质内涵。

需要承认的是，作为新兴技术的区块链必然有诸多不成熟的地方，亟待自我完善和理性质疑。在金融领域，区块链的倡导与应用者，也需要从早期的“币圈”与“技术极客思维”，逐渐转向技术与金融思维的有效融合。

例如，我们可全面反思公认的区块链特点。一是透明。那么，初始规则设置是否有利于多数人，是否有误导和信息扭曲？绝对的信息透明是否可能，会否带来信息保护难题？二是信用。从信息到信用，意味着要改造成为可交易的金融信息；基于区块链规则的“智能权责处理”，与线下资产确权如何关联；区块链线上生态的智能交易和责权约束机制，覆盖面有多大，可否脱离现有体系？三是不可篡改。据 Gartner 专家估计，粗略估算第三方用 4 亿美元，就能够改写比特币区块链账本，那么“超过全网 51% 的算力才能攻击”的成本难题，与真正安全之间的距离有多远？ DAO 事件带来的“硬分叉”争议、Krypton 受攻击等，是否已经改变了区块链的特质，各种账本维护者是否有道德风险？四是低成本。账本规模会否膨胀？交易费用与能耗会否快速上升？

所有这些都需认真审视。正如：想要改变别人，先要改变自己；想要融合别人，先要健全自己。通过技术、金融、法律等跨界合作，共同寻

找区块链的缺陷和不足在哪，才能使得这一革命性技术迎来更长远的生命力。

挑战之二：区块链解决的是“人与人”“机器与机器”还是“人与机器”的价值交换

经济学家罗伯特·希勒认为：“金融系统实质是一个信息处理系统——一个建立在人力基础而非电子元件基础上的系统，而且人工智能离彻底取代人类智慧还有很远的路要走。”从某一方面看，希勒可能有些保守，新技术已经对传统理论带来巨大影响。例如，行为金融学力图揭示金融市场的非理性行为和决策规律，对其一个普遍性批评就是缺乏合乎经济学研究范式的模型和实证体系。但信息、大数据和区块链带来了变化，个体行为与价值传递可能有效地被观测和甄别，这是否意味着微观金融学的假说基础真正被挑战？

金融交易的实质也是交换和处理不同节点之间的特定信息，有人认为区块链可使机器成为金融活动的主体。就技术对金融的影响来看，其路径是从“人与人”的金融，到“人机协作金融”，再到“机器之间的金融”，现实显然距离第三阶段还甚远。考虑金融活动，离不开对人的非理性行为与道德风险的关注，区块链共识规则与网络节点背后，仍隐含着人性带来的不确定性。

挑战之三：区块链带来的担忧是中心化还是去中心

应该说，金融交易中的信息不对称、搜寻成本、匹配效率、交易费

用、规模经济、风险控制等，决定了中心与中介存在的必要性，如央行、金融机构或中央对手方机制。新技术环境下中心（中介）的价值在变化。例如，从解决信息不对称，到大数据时代对信息泛滥的甄别。一方面，在新金融创新与变革过程中，有大量的“伪去中心”，例如不管是互联网企业做金融，还是许多 P2P 网贷和股权众筹平台，实际是以新的中介形式出现。另一方面，在现有经济社会组织模式下，真正的大范围去中心基本不可能，更多是有限小规模的“试验田”，有意义的是多中心或弱中心，实现共享型的金融发展。由此，虽然在技术上无可厚非，但当区块链应用于金融等领域时，应淡化“去中心化”，而强调分布式、弱中心特征。

同时需要注意几点：一是传统金融机构拥有巨大资源优势，完全可以利用区块链技术，在改良中发挥中心作用。如果出现内部制度失控，可能带来更大风险，近期德意志银行、富国银行的“神话破灭”已经给我们警示。传统机构的创新失控与道德风险，可能在区块链创新中被进一步放大，尤其是在其大量介入区块链生态圈建设之时；二是对政府或公共机构，也要防止其利用“无所不能”的新技术，超越合理权力边界；三是对于那些逃避监管的、打着去中心旗号的灰色或黑色金融活动，则是需各方唾弃的“劣币”。

挑战之四：区块链前景取决于利益、效率与安全的“三角制约”

区块链带来的变革，也离不开路径依赖突破下的制度变迁。所谓路径依赖，是指人们一旦选择了某个体制，由于规模经济、学习效应、协

调效应及适应性预期，以及既得利益约束等因素的存在，会导致该体制沿既定的方向不断自我强化。所谓制度变迁，包括自下而上的诱致性制度变迁（需求主导型制度变迁）和自上而下的强制性制度变迁（供给主导型制度变迁）。区块链能否真正获得生命力，在传统规则里“突围”且融合，取决于其能否找到“三角制约”的平衡点。一则，达到利益均衡并有利于多数人，是一项变革可否延续的出发点，需要充分预期到打破既有利益格局的阻力。如公有区块链可以用来安全、低成本地保存证书和文凭，但会对传统证书认证中介、非法产业和个人信息保护都带来挑战。二则，金融运行的效率有时并非“越快越好”，如高频交易对资本市场的“双刃剑”已经使我们警惕。三则，新技术和规则还需要基于安全的压力测试，包括产品安全、技术安全、系统安全、信息安全、资金安全、国家安全等。简而言之，区块链的内在理念实际已探索多年，现在更需回归主流，找理论扎根的“土壤”，探索与主流金融体系的结合点，从颠覆到补充，实现共享、融合的新生态。

挑战之五：区块链能否应对金融发展中的“短板”

例如，我们研究发现，2015 年支付清算业务规模与 GDP 总量之间的差距在进一步拉大，创造 1 元 GDP 所需的支付系统业务规模从 2014 年的 53.25 元上升为 64.77 元，其增长率达到了 21.65%，是 2007 年以来的最高值，而到 2016 年前三季度支付业务金额则高达同期 GDP 总量的 71 倍。近年来，支付清算系统业务指标与宏观经济运行之间的相关性也出现了显著的弱化现象。在 2015 年，基于支付清算指标所进行的宏观经济变量拟合效果普遍不尽如人意。除了非现金支付工具中的票据之

外，基于其他支付清算指标所给出的经济增长率或通胀率都大大超出了实际值。这说明，有相当多的支付活动并没有对实体经济作出有效的贡献。换句话说，支付清算业务反映了金融市场的活跃性在提升，而实体贡献度却增长乏力，金融的“自我游戏”在增加。

这里的关键，就是区块链金融创新能否促进金融服务实体、解决困扰中国金融改革与发展的诸多矛盾。如：规模增长下的结构与功能失衡、“两多两难”等，还是可能会加剧某些矛盾，如金融自我游戏、结构金融产品创新失控、场外要素市场的混乱等。

挑战之六：区块链应用场景从“宏大叙事”到“小而美”

对于区块链的应用需降低预期，因为其通往可编程经济的道路非常漫长。在此过程中，需拒绝“万能论”，区块链能有一部分场景得以应用就已有巨大价值。其中，在金融体系的“大树”之上，区块链应用就如同先修剪和嫁接“枝杈”，从小做起。在连接产业与金融的路径上，努力做一些优化和贡献。就区块链金融应用中的模式看，纯商业模式的落地并不容易，因为不仅需项目清晰、话语方式转换、盈利点明确、有更大的场景依托，而且也是更努力地在弱中心、弱中介链条上寻找中介存在的价值。同时，公益模式则可以更广泛应用，只要排除某些“假公益”。

此外，新技术使得金融要素的边界变得更加模糊，当叠加上区块链技术之后，更需要从金融主体逻辑到功能逻辑。具体而言，区块链应用不再局限于金融机构、产品、市场角度，而是从改善和优化金融功能入手，包括：清算和支付、融通资金和股权细化、为在时空上实现经济资源转移提供渠道、风险管理、信息提供、解决激励等。

挑战之七：区块链距离技术标准化时代是否还很远？

以 R3 为代表，愈来愈多的组织希望推动区块链技术标准的探索，而在我国除了民间组织，也有许多政府背景的机构介入。但客观来看，区块链似乎仍然距离标准化发展的成熟阶段尚远，因为还存在许多不足，也没有经历市场和行业的充分检验。此外，还需视以下几种情形的变化：一是在现代金融体系发展过程中，无论是中前台还是后台，都存在中心化标准与“弱中心”标准的同步演变，如在美国监管者推动金融市场基础设施的中央对手方机制建设同时，美联储去年又认为，与通过中心辐射状网络结构清算交易相比，金融机构间基于公共 IP 网络的信息分布式架构有可能降低成本。中央当局要在中央总账里建立报文标准、通信、安全和记录交易的通用协议，以便利相应的银行间结算。二是区块链标准需面对不同层面的矛盾，如基于市场化原则与国家金融利益与安全，可能带来不同的标准制定思路，基于软件标准和硬件标准的配合，在金融应用中同样不容忽视，基于商业化原则还是公共性原则，针对区块链技术底层还是应用层，都带来不同的标准与场景等。应该说，区块链标准探索虽然重要，但也不能脱离实际和急于求成，近期 R3 遭遇的危机也体现出这一点。诸多所谓区块链标准的竞争时代，会否造成市场混乱和泡沫，也值得充分思考。

挑战之八：区块链的最大挑战在于金融服务和数据服务的“模糊地带”

归纳来看，未来区块链应用的核心在于如何真正实现价值互联网。

从技术层面看：一是数字化代币账本，如数字资产、数字资产请求权；二是活动登记簿，如数据记录（代表某些商品或服务；金融数据或许代表交易事实）。当前，随着互联网时代新技术的快速演进，金融服务与数据服务的边界已经模糊。后者如 2014 年 5 月，美国联邦贸易委员会曾发布报告关注数据服务商的不透明；前者如 2015 年英国财政部引导成立了开放银行工作小组，以探索如何使用银行对外开放的数据，协助人们交易、存款、借贷以及投资，银行也成为数据服务商。

毫无疑问，区块链技术对金融的核心作用，是依托新的模式来确定价值、储存价值和交易价值。实际上分布式技术最终影响的是人的“身份信息”在金融意义上的体现，即账户形态。在区块链引领从信息互联网向价值互联网的过渡中，这一挑战始终存在，需高度关注监管适应性、风险控制等问题。

挑战之九：区块链应用于全面风险管理是核心“抓手”

对各类新金融创新来说，风险是各方最担忧的。因此，一方面需深入研究，作为一类新技术，区块链是整体上增加了风险，还是减少了风险；另一方面，完全可把初始区块链创新应用的较大重心，放到金融风险管理的应用上。进一步来看，在利用区块链进行金融风险管理时，先要区分传统金融风险和新型金融风险，前者如信用风险、流动性风险等，后者如互联网时代的长尾风险、羊群效应放大等。其次，从风险的影响程度来看，一是系统性风险，考虑的是大而不倒；二是非系统性风险，则是金融创新中不同参与者制造的风险或面对的风险，包括：个人（金融消费者保护）、平台（传统与新型风险，KYC，AML）、企业（非法集资，

财务管理）等。由此来看，区块链应用于新金融风险管理的优化，可有不同着眼点：一是监管层面，全面推动类似于英国的 RegTech 探索；二是行业层面推动信息透明，在机构风险控制模型中运用；三是结合保险、担保等，开发出新型的风险管理产品。

挑战之十：区块链创新监管需要“底线思维”

这里同样可延续互联网金融监管思路的转变，通过穿透式监管，剥离出虚假区块链项目的“外衣”。在实践中，一是要对区块链创业企业推动“良币驱逐劣币”，真正使得有核心竞争力的企业获得有效支持，而促使“噱头大于内涵”，甚至“挂羊头卖狗肉”的“人人喊打”；二是需要把基于区块链账本的数字货币，与区块链在金融交易中的应用区分对待，前者由于挑战了央行货币发行权，更需严加监管；三是在金融组织的非核心系统、金融市场的边缘和小规模地带，给予相对高些的创新空间和容忍度。

总之，可以围绕区块链金融活动的实质，以及参与者的行为性质，厘清区块链金融创新的“底线”。近期几大监管重心则包括：以区块链项目为名，实际却是非法集资的活动；打着数字货币旗号的各类传销币；区块链创业项目的高杠杆风险等。

（杨涛，中国社科院金融所研究员）

来源：《上海证券报》

区块链投资者的教育和保护

为什么投资者保护与教育是当前区块链行业的首要工作?

1. 当前存在较为严重的风险与乱象

第一，与股市 IPO 相比，ICO 具有短线交易的风险，由于区块链行业特别是数字货币的价格波动较大，怀有强烈投机目的的投资者倾向于选择在代币价值的最高点将其抛售来牟取利润，甚至不在乎项目本身的盈利情况，导致 ICO 发行的代币价格严重偏离其项目的内在价值。

第二，还具有金融“脱媒”风险，与传统融资模式不同，ICO 能够使资金供给绕开现有的商业银行体系和证券发行体系，直接输送给资金需求方和融资者，完成资金的体外循环，导致金融交易脱离现有的监管。

第三，去年 9 月 4 日央行禁令后，ICO 的热度不减反增，部分虚拟货币交易平台出走海外，在境外注册并继续向境内用户提供虚拟货币的交易服务。

部分 ICO 平台以所谓的“新技术”为噱头诱骗投资者，涉嫌“拉高

出货”和“市场操纵”的欺诈行为。

甚至还有少数平台打着 ICO、虚拟货币的幌子涉嫌传销、非法集资等刑事犯罪。对于部分原在境内的出走海外的 ICO 项目，同样存在着项目不实乃至传销、欺诈等风险。

由于项目主体已迁移境外，投资者一旦遭受欺诈或其他犯罪侵害则将可能面临难以维权甚至无处维权的窘境，难以追回损失。

2. 韭菜、投资者是风险的主要承担者

区块链技术应用于金融业态的兴起，即在于其吸收了小微投融资者，并对金融资产做了小额化处理，将融资者和平台能提供的市场流动性，与投资者投资额度及所能承受的金融风险相匹配。

因而，（要）把传统金融极少能覆盖的小微初创企业、新兴行业和社会公众，都融入到金融交易之中。然而，融资者负债和市场杠杆也随之增加。区块链技术应用于金融业态在包装和销售小额化金融资产的同时，也将金融风险扩散到了广大小微投融资者之间。

以 ICO 为例，若投资者的风险意识不强，在不了解 ICO 相关知识的情况下，在不安全的环境里盲目投资，那么金融消费者保护的形势会更加严峻。

ICO 具有流动性高、变现能力强、融资流程简单等特点，当前基本未设定投资者门槛。

在 ICO 纷纷出海的背景下，相关的交易主体、交易环节均在国外发生，政府难以对其进行有效的监管，犯罪诈骗活动就此泛滥，反映出投资者权利失衡的现实性及权利保护的急迫性。

3. 投资者是区块链应用于金融业态的重要基础，金融科技必然回归到投资者保护

我是最早研究区块链和众筹融合的研究者之一，一直致力于将自己提出的众筹金融理论（Wefinance）成果成功应用于实践，并被贵阳市政府采纳成立了第一家注册金融交易所即贵阳众筹交易所，并协助举行了2万多人的世界众筹大会等。在长期理论研究和实践之中，充分认识到投资者保护和教育对于互联网金融、金融科技发展的重要性，区块链应用于金融业态也往往是互联网金融、众筹金融模式的重要应用。

依托于高速发展的移动互联网、大数据、云计算、搜索引擎、社交网络等互联网技术能在更广泛的范围内方便快捷地将资金需求者与资金提供者联系起来，具有开放、平等、共享、去中心化、去媒介等属性。

我在2014年给互联网金融界定为：基于移动互联网、大数据、云计算等技术，实现支付清算、资金融通、风险防范和利用等金融功能，具有快速便捷、高效低成本的优势和场外、混同、涉众等特征，并打破金融垄断，实现消费者福利的创新型金融。进一步而言，我更乐意将这一新兴业态定义为众筹金融。

相对于“互联网金融”，“众筹金融”更能体现出“互联网+金融”这一新业态场外、混业的内在特征和其草根、普惠的精神，众筹金融是互联网金融的核心体现。也正是因为此，我将“众筹金融”译作“We Finance”。

ICO基于区块链等技术发行数字代币以向大众募集比特币等虚拟货币，可以将其视为区块链的众筹应用，只是换了一种方式，以币融资（币）。

具有众筹性质的区块链相关金融业态服务于社会大众，也依赖于社

会大众，应当切实维护欠富裕人群通过区块链相关金融业态获得金融福利的机会，因而也必须首要保护投资者，特别是一般的中小投资者。

从金融法原理而言。金融风险的主要问题，在投融资两端，都从较为抽象的、金融资产价格形成过程中投融资风险与收益的不确定关联，具体化为投资者风险吸收能力与金融资产风险的匹配程度。因而，实现投资者风险吸收能力与金融资产风险的匹配，也成为金融法风险规制的主要逻辑。

如何保护区块链行业和数字货币的投资者？

1. 首先应当控制源头，从资产端抓起，制定相关标准

在我们校友高瓴资本的张磊支持下成立的人民大学大数据区块链与监管科技实验室正在联合相关机构进行区块链相关项目、资产、生态的评级工作。

我们将依据项目（战略定位、项目必要性）、团队（技术团队、运营团队、投资人、顾问）、履约能力（白皮书规划节点履约情况、代码更新质量）、市场（交易所支持、价值稳定性）、风险、热度等对区块链相关业态提供的资产端进行评级。

2. 投资者进入市场应该有一定的门槛

我国可将投资者分为非成熟投资者和成熟投资者，可建立以年收入或净资产为基础，以投资损益记录为附加的复合分类标准。

事实上，美国《乔布斯法案》也规定，如果个人投资者的年收入或

其净资产少于 10 万美元，则投资限额为 2000 美元或者年收入或净资产 5% 中孰高者。若投资者年收入或净资产中某项达到或超过 10 万美元，则投资限额为该年收入或净资产的 10%。

英国《众筹监管规则》也规定，非成熟投资者是指投资 2 个以下众筹项目的投资人，其投资额不得超过净资产（不含常住房产、养老保险金）的 10%，成熟投资者不受此限。

3. 投资者适当性，这个问题非常重要，与前几天李笑来老师他们讨论的韭菜的智商税问题相关（我不同意智商税的说法）

要实现资本形成与投资者保护之间的平衡，就要把握区块链行业投资项目满足小微投融资者需求的关键，在于拆分资产而后向仅具有小额投资能力和风险承担能力的中小投资者配售资产。因而，投资者分类是首要的、与融资者和平台分拆和错配金融资产的营业行为相匹配的制度，是重塑投资者适当性及保护投资者的前提。

投资者适当性管理包括产品风险评估（KYP，Know Your Product）、投资者评估（KYC，Know Your Custom）、信息披露、产品与投资者的匹配、投资者教育、资产管理机构或中介机构的责任义务等一系列环节工作，力求实现资产端与资金者端的精确匹配。

将大数据技术嵌入投资者适当性管理制度是一项庞大而紧要的系统性工程，除了资产端在紧锣密鼓地创造新兴业态，资金端也需要与时俱进地确保投资者风险防范。唯如此，两者才能实现平衡，在维护广大投资者利益的前提下推动普惠金融向纵深发展。

应当加强大数据和征信体系等信息工具应用的基础，也凸显了互联网的信息优势，实现从信用风险到公共信息工具的转变。

在投资者保护层面上，也可以借由信息技术促进金融科技融资中的低成本的充分信息披露与合理的风险揭示，同时通过行为数据准确画出金融消费者的风险画像，掌握其行为规律与准确的风险承担能力，防止不正当销售，提供给其更为合适的产品。

人工智能技术的进一步发展，也将很大程度上提高投资者的金融能力。

当然这个过程中，区块链技术的运用是必须的，也就是大数据技术、人工智能技术的完美运用，离不开区块链技术。投资者适当性问题中，隐私和个人信息保护是关键，需要区块链技术。

4. 发挥一行三会投资者保护部门的作用，加强行为监管

我长期以来一直坚持研究金融消费者和投资者保护，2008 年美国金融危机之后研究了几个重要成果，在 2013 年和 2014 年分别出版了《金融服务统合法》和《金融消费者保护统合法》，一直也参与了一行三会的金融消费者保护和投资者保护部门的诸多合作（美国金融危机之后美国成立了一个消费者金融保护局，而我们一行三会都成立了保护局，可见我国政府对这个问题的重视）。

一行三会的金融消费者保护、投资者保护部门在区块链行业和数字货币相关问题中可以切实发挥作用，加强行为监管，维护投资者的合法利益。

5. 完善投资者争议多元解决机制

我长期以来也一直研究金融 ADR（多元纠纷解决机制），区块链相关金融业态也应完善投资者多元纠纷解决机制，相关项目方可发布自律

公约，自觉履行小额纠纷调解协议的义务，进一步明建立金融申诉专员制度（FOS），对处于弱势地位的投资者给予倾向性保护。

我们在 2014 年就成立中国金融消费者保护和金融 315 网站等受理金融消费者和投资者的投诉，招募广大的律师志愿者，为投资者提供免费的律师服务。

加强区块链应用行业和数字货币的投资者教育工作

1. 完善区块链应用行业和数字货币投资者教育的制度建设

中国的国情和国际经验告诉我们，投资者教育是投资者保护最重要的内容和维度之一，投资者教育工作是最为基础性的工作，必须加快建设。

区块链引导的金融创新泥沙俱下，鱼龙混杂，甚至有不少打着“金融创新”的旗号损害投资者、金融消费者的违法犯罪。

对此，监管部门必须切实负担起监管责任，但同时也必须加强投资者教育，提高投资者风险意识，自觉抵制非法金融行为。

2. 建设区块链应用行业和数字货币的投资者保护教育基金、基地

我也一直研究投资者教育工作，也是证监会首批全国投资者教育基地的评审专家，为保护缺乏专门知识与自卫手段的消费者，金融消费者和投资者风险防范宣传教育是维护公众利益和金融市场健康发展的应有之义，迫切需要加大行业政策解读力度，强化正面宣传，提升公众风险意识。

而对投资者宣传教育方式的多样化则有待加强，比如香港地铁设置了对加密货币的风险提示公益广告值得内地学习，可以使投资者在潜移

默化之中提高风险识别能力、风险意识。

3. 如何加强普通投资者教育工作？

普通社会公众的金融知识和风险意识普遍需要提高，金融行业具有专业性和风险性，但大部分金融消费者和投资者非金融专业人士，缺乏金融知识和风险意识。

针对区块链金融业态，还需要教育普通民众关于区块链及其法律风险、风险防范等基本常识。尤其是教育相关自我保护措施、争议解决措施。

投资者教育能够提高投资者的金融认知与风险识别能力。但教育是很难的，除了传统知识灌输的教育模式，大数据技术在投资者教育方面亦大有可为，把投资能力可视化，显性地呈现给 C 端客户。

通过对自身投资特征的了解，认识到自己有盲目频繁交易换手的错误进而遭致财产损失，投资者才能真正使其反思，改变错误的投资观念，最终达到教育投资者的目的。

4. 加强专业投资者教育

专业投资者在传统金融领域有着充分的经验和能力，但并不一定理解区块链模式下的金融业态，特别是各类境外的复杂的数字货币，风险极大，即使是专业投资者也会不理性，也需要加强他们的更加复杂科技金融知识和风险承受能力的训练。对于希望进入金融市场的区块链专业人士则应加强金融方面的教育。

5. 发动社会广泛参与

投资者教育作为一项普惠全社会的活动，其实施主体包括监管部门、

金融机构、行业协会及其他组织，甚至广泛发动全社会的力量，一个完善的投资者教育环境还需要包括教育机构、新闻媒体等社会各个方面共同参与。我们人民大学与新华网等权威机构每年315举行金融消费者保护高峰论坛，迄今已经举办四次，马上今年3月15日举行第五届，并且成立金融消费者和投资者教育基金，配合政府开展相关工作，也是金融消费者和投资者教育方面的一个实践案例。

（本文是中国人民大学大数据区块链与监管科技实验室主任杨东于2018年3月6日在“3点钟无眠区块链”微信群做的分享，略有改动）

五、区块链未来前景展望

整个人类的历史是分久必合、合久必分，区块链技术使得互联网时代也到了一个新的分久必合、合久必分的时代。我们正是面临着区块链和去中心化技术给这个时代带来的一场新的革命。

——丹华资本创始董事长　张首晟

区块链的应用前景

这一年，区块链火遍中国，出租车司机都知道它是互联网经济新风口。最新发布的数据显示了它在中国的热度——世界知识产权组织统计，中国去年申请 225 项区块链技术专利，占了全球（406 项）的一大半，其次是美国（91 项）和澳大利亚（13 项）。这些专利并不包括加密货币的领域。

有报道称，中国的互联网公司和金融服务商竞相申请这种“分布式账本”技术的专利，是看好它会给金融和其他供应链带来革命。与“炒币”无关，在区块链的试水者看来，新技术可以补上至关重要的一环——信用。

交易量不大，金融巨头却不敢掉以轻心

区块链是一种去中心化的记录体系，区块链的账本，由参与交易的所有结点共同记录，因此，从投资者到互联网黑客，都对区块链蕴含的前所未有的“无权威、防篡改”特质大感兴趣。

许多“炒币”的人知道，中国拥有的比特币和其他区块链货币的“矿

场（参与区块链计算的计算机）”之多，在世界上数一数二。与此相仿，2012 年到 2017 年，区块链技术专利申请最多的 9 家企业，有 6 家来自中国。

不过，近五年来最活跃的专利申请者，是总部位于美国的支付巨头万事达，其次是列支敦士登的 n 链控股。

研究机构广州联瑞指出，申请区块链专利的著名公司还包括美国银行和英国电信等。美国银行计划开发一款支持人对人的支付系统，各方均可化名交易；英国电信的技术则可以检测针对区块链的攻击；万事达则注重支付追踪，以及上传销售数据到区块链。

其实目前区块链体系的交易量，和主流的世界金融交易体系相比，仍是九牛一毛。各巨头积极于专利布局，也是为了提防万一，避免在未来被设置障碍。

区块链将说服你，这只大闸蟹来自阳澄湖

在物联网专家、国家物联网基础标准工作组总体组组长沈杰博士看来，区块链的分布式账本和信用体系，为解决一些征信问题带来了机遇，由此还可以发掘金融价值。

“农产品的流通中，数据是容易掺假和丢失的。”沈杰举了个例子，比如市场上有许多声称是阳澄湖生产的大闸蟹，都有证书或某些“权威”数据记录来证明，但那么多大闸蟹不可能都产自阳澄湖，消费者怎么知道哪些是真的？

“现在的农产品溯源，需要很多环节，从种苗、药剂到环境，各种数据要齐备，但现在国内信用缺失的问题严重，到消费者手里无法确认是

好的农产品。农产品不能卖高的价格，农民利润也越来越薄。”沈杰说，“现在政府、电商作为单一力量去推动溯源，成本很高。”

物联网技术，利用大量设备采集物理世界信息，以更好地感知和管理，本来是很好的溯源手段；但如果只有物联网，各个主体传递数据到平台，仍不能排除造假和篡改的可能性。沈杰说：“要确保从设备端到平台不可被篡改，就可以用到区块链底层的征信机制。”

据报道，京东等企业正尝试在农业中引入区块链技术，做到一头牛从出生到屠宰到商场上架，每一步数据都上传区块链，做到可以信赖。

一块田，或将被区块链征信成为资产

“以往，物理世界的实体在流通中的价值挖掘是不充分的。”沈杰说，“比如我在农村有一块田，但没有人投资，它只是一块田。如果它数字化了，就可以交易，可以分享权益。”

沈杰认为，物联网本可以将这块田，映射为数字资产。但过去要让金融机构用上物联网数据不那么容易，而区块链让传感器数据和金融的结合有了场景。

“物联网加区块链，可以帮助银行和保险公司获得可靠的数据，解决信息不对称的问题。在农民和金融机构之间建立了征信机制。”

沈杰介绍了一个正在推进的案例，是将区块链技术应用于渔业。物联网传感器能够监测和管理鱼塘的水质，同时还可以帮助金融机构采集农民数据，给予贷款。在农民拿到更多利润的同时，提升产品的品质，做到可追溯。

而且区块链的数据有跨平台的可信度。“阿里巴巴芝麻信用积分，出了阿里巴巴的体系就没有意义。”沈杰说，区块链技术依靠多主体之间的协同和数据传递，将让数据的金融价值像物理世界一样实在。

从医疗保险到游戏积分，信任不再难

江苏恒为信息科技公司是较早涉足区块链技术研发的一家公司，企业负责人徐钰淳说：“你可以把区块链通俗地理解为‘全网公开的分布式电子账本技术’，它实现了低成本的信用体系建立和价值传递，能解决金融、公益、监管、打假等很多领域的痛点和难点。”

徐钰淳说，利用区块链技术，可实现在医疗、医保和医药“三医联动”中，健康医疗数据查询和使用记录不可篡改；而在金融方面，利用区块链技术可实现企业征信数据的真实性和可追溯性，实现供应链溯源防伪、自动化智能合约、订单履约追踪、应收款项管理、抵质押品认证等功能。

或许正因为区块链公开透明的天生特质，正好契合中国缺乏信任的应用场景，从而引发企业研发和申请专利的热情。

沈杰认为，在一些已经数字化的领域，区块链的信用优势会更快显现。

“一个是数字版权，比如互联网音乐的知识产权，区块链应用发展可能比较快；一个是博彩业，过去互联网上博彩难以避免欺诈的可能，有了区块链，信用可以建立。”沈杰说，“另一个可能是游戏的虚拟收入，比如积分，过去离开了游戏这些积分就没用了，区块链可能推动各种游戏的互通。”

沈杰说，数字化的银行票据等领域也在积极试水区块链。他认为，现在还是区块链技术的早期，大家一股热情去推动发展；但创新进入深水区后，一个点或一条线的突破都不够，需要生态和系统性观念的配合。

（高　博）

来源：《科技日报》

抓住区块链这个机遇

区块链的诞生，将大幅降低价值传输成本，又一次极大解放生产力。目前，区块链底层技术还不成熟，基础设施还不完善。区块链难以篡改、共享账本、分布式的特性，更易于监管接入，获得更加全面实时的监管数据。区块链迅速发展不是偶然，它能极大降低信息价值传输成本。

区块链发展如此迅速，背后有深刻的必然性。自互联网诞生以来，人类社会的信息传播成本得到极大的降低，信息传播效率的飞跃带来生产力的极大解放。

然而现在的互联网也存在固有的缺陷，它更关心的是信息的送达，而不太关心信息的所有权，出现了“数据裸奔”“信息无主”等问题。而有些信息具有很强的价值属性，比如汇款转账信息，这些有价值信息的传递需要依赖第三方来“保驾护航”。因此，目前信息的价值传输成本依然高企。

区块链的诞生，带来了解决这个问题的曙光。由于区块链公开透明、难以篡改、不依赖中介机构的特点，区块链可以实现安全、高效、低成本的价值传输。人们有望基于区块链建成价值传输的互联网。在价值互联网中，价值传输成本将极大降低，生产力将又一次获得极大解放。

区块链独特的优势，如数据的确权使用、价值的高效传输，可以广泛应用于很多行业，比如金融服务、合同契约、慈善公益、物联网等，区块链将在未来改变很多行业的面貌。

因此，区块链绝非无足轻重的领域，而是国际上的兵家必争之地，我们必须给予足够的重视。

最近，区块链概念很火，区块链的春天似乎已经到来，那么，爆发就在眼前吗？

我们不应该如此乐观、如此急切。区块链技术诞生以来，尽管技术创新与突破层出不穷，但社会级别的大规模应用实践仍然不足。区块链底层技术不成熟，基础设施不完善的状况并没有获得根本改观。

首先，当前主流的区块链系统，包括比特币、以太坊等，其成熟度都不能支撑大规模现实商业场景。其次，在现有系统中，价值往往只能在同一个区块链内进行传递，于是，看起来热闹的众多区块链实践，事实上搭建了更多的价值孤岛，这与区块链“价值互联网”的美好愿景南辕北辙。

然而，区块链底层技术获得实质性突破之前的这个阶段，恰恰是一个战略机遇期。我们应该深耕技术，以期通过技术优势在未来的国际区块链竞争中立于不败之地。如果急于在并不牢固的地基上搭建城堡，很可能因小失大。

监管之道在于通过区块链技术本身实现对技术的监管。区块链行业健康发展，亟须科学监管。由于处在发展的早期阶段，区块链从业人员鱼龙混杂，甚至有的从业者发布一些只有名字、无战略、无团队、无开发的“空气项目”，吸引风险承担能力不足的散户参与其中，这不但是对行业自身的戕害，还给社会稳定带来了隐患。2017 年 9 月 4 日，7 部委

发布了《关于防范代币发行融资风险的公告》。对于行业内野蛮生长的代币融资行为，将其定性为“非法公开融资”。这是一次非常及时的监管介入，对后续监管也有很好的借鉴意义。

有观点认为，区块链的匿名性与弱中心化的架构，与现有的监管体系存在某种程度的天然冲突。实际上，两者并不冲突，区块链技术最终必然演化为“监管融入技术”的模式，区块链的难以篡改、共享账本、分布式的特性，更易于监管接入，获得更加全面实时的监管数据。让监管机构本身也参与到技术中去，通过技术本身实现对技术的监管，将最终化解区块链与监管的冲突。

（窦佳丽）

来源：《人民日报》

区块链是互联网世界新的分合转折点

差不多在四年以前在区块链出现的时候，我就对这个领域非常的关注。我认为世界历史可以用两句话来描述：分久必合，合久必分。我们的互联网行业也体现了这一种规律。过去，美国网络的资源几乎被 AT&T 一家垄断，这和当时候的网络技术 Circut Switching 有很大的关系。最初，AT&T 也面临过一定的竞争，但等到公司足够大，效率和规模足够优秀，最后就会出现一家垄断的现象，垄断美国战后三四十年的网络市场。

但是，往往技术的发明会导致合久必分。TCP/IP 协议的发明，就促进了互联网时代的到来，Packet Switching 取代了 Circuit Switching。我们所有的通讯都是通过一个个小的 Packet 相互通讯，这使得通信效率提高。在这样的情况下，就没有必要有一家公司来垄断整个网络的资源，这样就迎来了一个合久必分的时代。

当合久必分的局面持续了一段时间后，人们发现一个问题：虽然最底层的网络通信非常去中心化，大家也会在每个网站发表自己的信息，但

是对整个信息没有一个系统的组织架构，这使得信息很难被找到。在这种需求的推动下，美国就出现像谷歌这样中心化的一个搜索公司。

它做的事情和我们过去在工业时代做的事情几乎一样：只是把重组原子改为重组信息。比如大型石油公司开采原油，而原油也是一些原子组成的。石油公司的做法近乎将原子重新组织了一下，将它变成了化学品。像谷歌这样的新一代企业，它们擅长的是重组那些 Bits、信息。谷歌并没有建立那些网站，而是利用自己的算法，对已有的网站进行排序，使得每个公司都能在这个网络世界里被很容易地找到。它驾驭了这个网络世界，是凌驾网络的新型组织机构，也导致了它的一个新的垄断时代到来，导致了分久必合。

这些都是组织信息的大平台，但是现在整个互联网行业到了一个新的阶段。如同当年 TCP/IP、Packet Swtiching 能够打败一个 AT&T 这样的巨人，区块链又让一个网络去中心化的时代来临，又到了一个合久必分的时代。人和人之间又可以通过区块链回到一种 P2P 的交流方法，更加神奇的是，人们可以在这个平台上交换价值。

价值是一个很难交换的东西。互联网第一波只是交换信息，但到了第二波希望能够交换价值，因为价值的核心就是要大家有一个共识。在一个 Distributive System（分布式）系统里面，达到共识是一个非常难的事情。每个网络的节点都有时间的延迟，计算能力也不一样。有的计算机有良好的行为，有的计算机确实有一些不良行为。在一个复杂的网络系统里面，如何达到一个共同的价值，这在那个计算机科学里面也是一直没有解决的问题。因此计算机科学中有一个 Fischer-Lynch-Patterson 定理，在采取一种完全 Deterministic（固定）算法的时候，共识是永远无法达到的，因为这个网络的系统实在太复杂。

后来，大家就想到区块链的技术可以把经济行为加上随机的数学算法使得网络达到共识，比如说通过计算一个 Hash 函数的办法，对共识进行投票，这就是整个区块链上面达到了一个新共识的机制。

大家可能很难理解，为什么这个共识的机制本身会有很大的价值。事实上物理学里面有一个非常深刻的概念叫熵增，就是物理世界看起来是总是走向无序。但是生命世界和物理世界不太一样，生命世界确实越来越走向有序。走向有序的行为是把熵减少的一个行为，但是整个系统的熵还是在增大。因此，生命行为就是把自己的熵减小了，使周围的熵增大了。

这在共识机制上也是一样。如果我们要达到共识就是要把熵减少，大家如果意见非常不一样的话，熵也就很大，因为非常无序。但是如果能够统一意见，达到一种非常有序的状态，它必然是减小熵的一种行为。然而，减少熵的行为必然会增高周围世界的熵。

因此，当时提出来的算法是通过一些 Hash 函数的计算，这虽然看起来是浪费了一些周围世界的能量，其实得到了一种更可贵的财富，也就是共识。

在这个意义下，区块链的共识系统有点像生命系统本身，自己的熵在减弱，它达到了共识，但使得周围的系统熵变大。这是一个代价，但相比别的系统来讲，这个代价还是非常小。

所以，一旦我们有了共识之后，就会有一种信任，人和人之间会有一个新的合作机会。所以，我把这个新的时代称为：我们的信念是建筑在一个数学的算法上面，In math we trust。在今后的系统中，中心化平台就不再需要，取而代之的是我们能够建立一些 P2P 的区块。通过开源的投票模式，大家可以用透明的算法，定义这个 Community 里面的

游戏规则。这就更能导致一个新的互联网的革命，一个合久必分的时代就又会到来。

最近大家都对人工智能比较感兴趣，但其实人工智能现在碰到了一个很大的瓶颈，因为如果 AI 要非常大的进步，它必然要需要很大的数据，但是现在的数据提供方都没有足够的激励机制提供极大量的数据。但一旦有了区块链之后，如果创造数据能被价值化、共识化，就会形成一个大的数据市场，使得人工智能也能够更往前进一步。

当然，我们最大的愿望，是通过区块链的技术使得我们的社会能变得更加美好，使得人们能够通过数据的分享创造和达到价值，这样也能使社会能够更加公平，让大家有更多新的机会。

所以总的来说，就像整个人类的历史是分久必合、合久必分，我觉得区块链技术也使得互联网时代也到了一个新的分久必合、合久必分的时代。我们正是面临着区块链和去中心化技术给这个时代带来的这场新的革命。

（本文是斯坦福大学终身教授、富兰克林奖章获得者、中华人民共和国国际科学技术合作奖获得者张首晟教授于 42 章经组织的区块链主题分享会上所作演讲，略有改动）

区块链代表着互联网的第二个时代

唐·塔斯考特（Don Tapscott）被誉为“数字经济”之父，在2017年11月公布的全球Thinkers 50榜单中，唐·塔斯考特因为对技术影响力的长期研究，成为全球排名第二的思想家。《哈佛商业评论》中文版在维也纳举办的“全球彼得·德鲁克论坛”上采访了他，他谈到区块链应用的最新发展，并指出，这项技术是人类千载难逢的机遇。算机科学发明以来最大的创新。

HBR 中文版：区块链的革命性体现在什么地方？

唐·塔斯考特：首先我要强调，区块链和比特币并非一回事。区块链是一个分布式的账本，但它所代表的东西远不止于此。我认为，它代表互联网的第二个时代。

信息互联网时代，如果我通过互联网发给你一份文件，都是发送了一个副本。对信息来说，这样做没问题。但是对经济真正重要的事，例如资产，包括金钱、知识产权、股票、碳信用、音乐、艺术品、身份信息、能源等有价值的东西，复制不是好主意。如果我转给你1000元人民币，要确保我手上少了1000元人民币，否则我还可以给多人转账。这就是长期以来密码员称为重复花费（double spend）的问题。在管理经济时，我们是通过银行、政府、信用卡公司、社交媒体公司等中介机构完成的。

他们确定交易双方身份，留下记录，完成交易。

除了信息互联网，我们还有价值互联网，一个覆盖面巨大的分布式账本：从金钱、股票到身份信息、音乐都可以储存其中，并能够完成点对点（peer to peer）交易——信任不是由中介机构创造，而是由加密完成，由协作的功能完整的代码完成，这就是区块链。

我们不再需要强大的中介机构，而是通过原始的价值媒介完成交易。我认为，这是计算机科学发明以来最大的创新。

区块链的潜力还体现在，它能够提高效率、降低风险。区块链是分布式的，与今天中心化的计算机系统相比，更能防御黑客攻击。这只是冰山一角，还有更多机会蕴藏其中。区块链能够通过不可更改的记录保护权益，还能创造真正的共享经济。

HBR 中文版：区块链目前有哪些应用？

唐·塔斯考特：最为突出的应用是针对那些所谓颠覆性的公司，例如优步、滴滴、爱彼迎（airbnb）等自称共享经济模式的公司，其实这些公司不是真正的共享，而是聚合服务提供商。区块链的软件完全可以完成爱彼迎的工作。我们假设一家叫作 b-airbnb 的公司，是一款区块链的分布式应用软件，所有想出租房屋的人共享这个软件。当某个人想租房子的时候，用这款软件筛选条件，找到合适的房间，用区块链处理合同、身份验证、数字支付等问题，无须任何独角兽公司作为中介平台抽取中介费用。

这项技术还可以应用在供应链方面。所有的贸易金融业务都可以通过区块链完成，它的前景无限。价值互联网方面，目前正涌现出成百上千的应用。

HBR 中文版：哪些应用已经有了实践？

唐·塔斯考特：无须银行作为中介的汇款平台已经有了。贸易金融方面也利用了这项技术：跨境送货涉及船运公司、物流公司、托管代理、

清关公司等各种不同的参与方。利用这项技术，所有人都能看到账本，能够共享状态。这非常具有革命性。

HBR 中文版：区块链技术发展的生态环境哪些方面还不够成熟？

唐·塔斯考特：就像第一代互联网一样，区块链不是由政府管理的，而是由自下至上、自我组织的生态系统管理。很多事情还需要完善，比如需要更好的研究、更好的政策环境、需要标准——这点非常关键。对于一些区块链应用来说，标准制定的过程很糟糕，比特币就是一个例子。而信息互联网当时有清晰的标准，比如有国际互联网工程任务组，这样专门为互联网制定标准的机构。还有万维网联盟为万维网制定标准。而区块链方面，目前仍是荒蛮阶段，尚未有标准。这就充满了迷惑、乱象和灾难。

HBR 中文版：你如何评价比特币？

唐·塔斯考特：我不是很关心比特币。政府也不应该过分关心它。我认为比特币永远不会成为任何国家法定货币的竞争对手。

HBR 中文版：区块链技术将如何影响企业运营？

唐·塔斯考特：影响非常大。在区块链技术研究所（Blockchain Research Institute），我们针对这个问题进行了 70 个有关项目的研究。举个例子，对于企业的首席财务官来说，现在大家通用的是复式记账（double-entry accounting），但在区块链技术下，我们可以引入第三个项目，给某次交易盖上时间戳的收据，从而实现三式记账法（triple-entry accounting），能够对公司内一切账目进行实时审计，这样首席财务官就不需要在年末进行审计了。

还有首席法务官。以太坊区块链由一位加拿大人开发，它能够实现智能合同，可以自我执行，处理人们之间关于执行、管理、绩效、支付等问题的协议。社会活动很多都基于合同缔结，有正式的、非正式的，

当这些合同都变成智能合同会有重大影响。想想这对律师来说意味着什么？公司的营销部门、法务部门都会受此影响。

此外还有首席运营官，他们通常管理着供应链，供应链成为区块链后是革命性的变化。因此，所有管理者都应该对这项技术保持关注。

HBR 中文版：区块链很具颠覆性，企业该怎么做才能不被其颠覆而是利用好这项技术？

唐·塔斯考特：这个问题很重要。如果你抗拒它或者忽略它，可能会变成危险的事情。但如果你拥抱它，可能会成为助力公司发展的强大力量。企业要开始了解这项技术，不断试验，培养相关人才，鼓励政府制定合理的法规。打个比方，做外科手术的时候，要用解剖刀，不要用锯子。目前区块链应用方面的主流方式更倾向于用锯子。

HBR 中文版：作为个人为什么要关心这项技术，该如何利用？

唐·塔斯考特：举个例子，我所在的城市多伦多，居住有近 100 万中国人，他们会向在中国的亲友汇款。这是一个数额巨大的市场。传统的汇款机构要向他们收取较高的手续费，但你现在可以通过区块链平台完成，只需要 1% 手续费，7 分钟就搞定。从这个例子中我们能看到，点对点的资产流通，能为这些家庭带来革命性的变化。

如果你是音乐家，没有得到合理的报酬，那么可以利用区块链技术平台实现。它还可以保护隐私。区块身份出现后，你可以把所有信息放到区块中，包括交易信息、教育信息、医疗信息、社交媒体等，都在你的身份中，由你控制并能够货币化。你可以决定如何利用这些数据。

这项技术很快将会对我们的生活产生巨大和深远的影响。第一代互联网，即信息互联网，为我们带来了财富，却加剧了社会不平等，导致了一系列社会问题。而在价值互联网中，我们能够通过将财富创造过程

民主化的方式，预先分配财富。这从一开始就改变了财富创造的方式，让更多人参与经济，得到合理报酬。

HBR 中文版：你考虑过这项技术的负面问题吗？

唐·塔斯考特：确实有许多负面问题，例如政府可能利用这项技术来控制民众；它可能会带来结构性失业；罪犯会利用这项技术牟利；. 还要小心，技术可以自主学习，它们可能学会做其他事情，最后发展成某种病毒，这点也令人担忧。技术无法带来繁荣，人类才可以。区块链给了我们一个解决很多困难问题的机会，要看人类如何利用。

HBR 中文版：现在技术发展似乎有点失控了，你如何看待技术的未来？

唐·塔斯考特：我认为未来不能靠预测，而是靠人类的实践去探索。我们要十分小心技术的边界，尽量让它做好事，为下一代创造一个更美好的世界。

HBR 中文版：说到下一代，我们该教他们什么，才能让他们更好地适应未来？

唐·塔斯考特：你无须教他们技术，他们会教你。对他们来说，技术就像空气。我更注重教育孩子学会正直和自律，永保好奇心，要有基于信任的良好的人际关系，有朋友、家庭和社交资本。我总说，我不关心你做什么、赚了多少钱，我希望你有原则，做改变世界的事。

（牛文静）

来源：《哈佛商业评论》

人才依然是区块链解决数据行业痛点的关键

智能风控的目标

在银行业，智能风控一方面是识别客户的身份，另一方面是识别客户的还款意愿和还款能力。还款意愿的判断主要通过风控建模。从模型角度可以分为反欺诈模型和信用评估模型。反欺诈模型是第一道墙，信用评估是第二道墙。业界有很多种机器学习的方法，金融业用得最多的是有监督机器学习和无监督机器学习，其中，有监督机器学习更有效。在金融行业，有监督机器学习一般通过逾期的坏样本来建模，进而通过借款人的其他特征预测一个客户是否会逾期。这里先介绍反欺诈，我们自主研发了挑战问答系统，淘宝和微信在你换手机登录时会问你最近买过的东西是什么，以及以下哪几个头像是你的好友，利用这种只有客户本人才知道的隐私信息，别人想盗取你的账户，即使破解了登录密码也无法登陆。而银行从哪里获取类似的信息呢？其实征信报告里有很多类似的数据，例如，客户在自己申请信用卡的时候填写的账单地址、工作单位、配偶信息、第一张信用卡额度等都会记录在征信报告中，把这些

信息结构化以后抽取出来作为问题，就可以对客户提问，附加一些干扰项，这就可以很好地起到防止伪冒欺诈的作用。真正的智能体现在哪儿？例如，根据客户回答的正确与否和回答的时间长短，动态调整第二个问题的类型和干扰项，通过跟客户交互来可以判断他身份的真实性。

信用评估方面，判断还款能力需要收集很多数据，除了人行征信报告之外，还需要收集场景中合作方的数据。我们打造的综合金融 SDK，获得了人民银行科技发展奖一等奖。我们把所有银行服务打包成 SDK，上海的一家租房平台青客把 SDK 植入进去，客户可以无跳转在里面申请租金贷，只需提供征信查询授权和租房相关数据。其中，在通过各渠道获取数据时，有一个问题是怎么保证数据的真实性，这个时候就要用到区块链。

前面提到，建模里最有效的是有监督机器学习，即已知坏样本的前提下如何建模。具体而言，可以分为四步。

第一，数据清洗。收集到的数据一般会存在以下特征：数据缺失、数据重复、数据错误、数据不可用。为此，必须花大量时间进行清洗。这个“脏活”“累活”的过程不能省。整个数据清理过程大概占建模 80% 的时间，但这是非常重要的。

第二，数据建模。将数据拆分成训练集和测试集，还有 WOE 转换、IV 值、模型逻辑回归、衍生变量等等。

第三，模型评估。要判断模型的质量怎么样，KS 值就是判断一个模型区分好坏的能力，值越高说明模型区分好坏的能力越强。

第四，模型验证。拿预测数据去验证，确定 cutoff 值，当模型返给你一个值，比如 0.6，他告诉你 60% 的可能这个人会逾期。实际产品中 0.6 算逾期还是不逾期，一旦确定了这个值，通过率、拒绝率、损失率都

可以算出来。

假设我们已经找到两个特征比较强的变量，根据客户的“人行征信被查询次数”和“尚未结清的个人消费贷款笔数”判断客户未来是否会逾期。最后的模型其实就是根据这两个变量通过一个多项式计算出一个客户违约的概率，而所谓建模，就是找出这些变量及计算公式。

利用区块链解决数据行业痛点

数据行业痛点

所有智能风控的过程都依赖于数据是真实可靠的，如何保证数据的真实可靠？现阶段数据行业有三大痛点：

第一，机构之间互不信任。不管是我们和合作伙伴还是金融机构之间共享数据，现状是机构之间共享黑名单，白户当黑户共享出去，这样这个客户就总是被别的机构拒绝，只能在自己平台申请借款。类似的，还有虚构交易数据等等现象。

第二，个人隐私及授权，即如何保证本人授权及真实意愿表达，在自己不授权的情况下如何保证别人看不到这些数据，这个问题一直没有很好地解决。当前，这一问题可以用区块链加密技术来进行解决。

第三，数据溯源及贡献计量，在数据共享体系里有一种机制，传的越多查的越多，交叉验证，多传多查，而且，链上的数据可以有机构签名。这也可以用区块链的 Token 及签名等机制解决。

下面从技术层面讲一下区块链为什么能够不可篡改。以比特币区块链为例，所有的区块都包含上一区块的哈希值，本区块内会把所有交易

哈希值打包，所有区块串起来，这样任何一个交易被改变都会导致这个区块的哈希值被改变，从而与下一个区块中的【上一区块哈希值】不一致，这个区块就不会被矿工承认。

利用区块链加强信任

我假想了这样一个场景，金融机构之间共享数据，机构 A、机构 B、机构 C、机构 D，这些金融机构都会和客户发生一些交易，他们首先把交易上链（黑色粗线表示链上），客户不在链上。假设开始是这样的场景，在链上的首先解决了机构之间多查多传的问题，我经过 A 上传一笔交易数据，获得一些 Token，查询的时候消耗 Token，但是没办法解决数据造假，也没办法验证这笔数据到底是谁的。如果加上机构 A 的私钥签名，这里用到数字签名技术，机构 A 私钥加密的信息只能用机构 A 的公钥去解密，公钥可以公开给所有人，一旦用机构 A 的公钥解开说明只能是机构 A 发出来的，因为这个私钥只有机构 A 有。我把信息用机构 A 的私钥签名以后就可以知道这个信息是机构 A 发出来的，别人知道这个信息是谁的就可以溯源。

解决了溯源的问题，但是没办法解决造假的问题。如果我知道是假的可以找到 A，但是无法知道交易是真的还是假的。我的想法是，只有把个人拉到链上（见图 5），让个人信息和交易信息加上个人的公钥，再套一个机构 A 的私钥，个人和机构 A 共同证明这个交易是真实可信的，如果机构 A 要作假，他就要和每个客户联合作假，成本是非常高的。个人理解区块链的核心在于提高造假成本，而不是完全不能造假，只要造假成本高于造假收益，我们的目的也就达到了。

个人加上公钥签名以后，个人授权问题也可以解决，他向机构 B 申

请贷款的时候，机构 B 首先在链上查询是否有这个人的交易，一旦查到以后发现这个交易是用机构 A 的私钥签名，用机构 A 的公钥去验证，可以解开得到用个人的公钥加密的信息，此时再去申请个人的授权。因为个人要向机构 B 申请贷款，所以肯定会授权给我私钥，私钥解开这个信息以后我就可以得到交易信息。这个过程很好地解决了几个问题。第一，我知道这个信息是这个人和这个机构 A 发生的交易，两方都认证了，我获得了个人的授权，其他机构看不到，因为他没有授权拿到个人的私钥。

这个机制比较好地解决了目前的一些问题，但是机构 B 一旦拿到了个人信息和交易信息，你没有办法防止他不把这个信息泄露出去，他可以在链下卖给另外一家机构。有人说我可以用机构之间的竞争，机构 B 有了这个客户是不希望别人拿这个数据的，但是如果机构 B 觉得服务这个客户的利润已经足够了，卖出去的话还可以额外赚一笔，他还是会把客户信息卖掉。因此，技术只能是部分地解决或者增加作假成本，不是万能的。

综上，区块链有助于建立信任机制，但是无法建立信用，大数据也只能辅助于信用的判断，技术非万能，人才是关键。

（本文是上海华瑞银行大数据中心副总经理张鲲于 2018 年 3 月 24 日在“聚焦区块链等新技术与智能风控的发展”会议上所作演讲，略有改动）

编辑后记

区块链技术迅速发展，为云计算、大数据、移动互联网等新一代信息技术的发展带来了新的机遇，有能力引发新一轮的技术创新和产业变革。我们选取了《人民日报》《经济日报》等权威报刊的重要文章，从不同角度对区块链进行了详细阐述和解读。希望能够帮助广大党员干部深入了解区块链的发展趋势和规律，从而加速推动我国区块链技术和产业发展。成书过程中，为规范图书体例、格式，对部分文章进行了编辑修改。此外，因时间仓促，我们未能及时联系到部分作者，敬请相关作者见书后联系出版社领取稿费和样书。