大数据金融丛书

区块链世界

井底望天　武源文　史伯平　赵国栋
主编

BLOCKCHAIN WORLD

深度探秘区块链世界
全面解析区块链生态
科学推演区块链发展

全面了解区块链底层技术本源、流派类别和应用发展

中信出版集团 · CHINACITICPRESS

区块链世界

井底望天　武源文　史伯平　赵国栋
主编

BLOCKCHAIN
WORLD

中信出版集团 · CHINACITICPRESS · 北京

图书在版编目（CIP）数据

区块链世界 / 井底望天等主编 . -- 北京 : 中信出版社, 2016.11（2017. 1重印）
ISBN 978-7-5086-6903-8

Ⅰ . ①区… Ⅱ . ①井… Ⅲ . ①电子商务－支付方式－研究 Ⅳ . ① F713.361.3

中国版本图书馆 CIP 数据核字（2016）第 247014 号

区块链世界

主　　编：井底望天　武源文　史伯平　赵国栋
策划推广：中信出版社（China CITIC Press）
出版发行：中信出版集团股份有限公司
　　（北京市朝阳区惠新东街甲 4 号富盛大厦 2 座　邮编　100029）
　　（CITIC Publishing Group）
承 印 者：北京通州皇家印刷厂

开　　本：787mm×1092mm　1/16　　印　　张：23　　字　　数：245 千字
版　　次：2016 年 11 月第 1 版　　印　　次：2017 年 1 月第 2 次印刷
广告经营许可证：京朝工商广字第 8087 号
书　　号：ISBN 978-7-5086-6903-8
定　　价：59.00 元

“大数据金融丛书”编委会

《区块链世界》编委会

序

井底望天

一、战略

在中国从1978年开始的翻天覆地的改革开放发展历程中，“一带一路”发展战略无可争议地会是其中一个浓墨重彩的里程碑。

1978~2008年，可以主要看作是一个沿海经济区域参与国际经济大循环，以西方发达国家市场作为主要目标，进而介入国际分工的过程。在这个过程中，从简单的“三来一补”——依靠西方先进的技术、管理、市场营销，以及中国提供的政策、土地和廉价劳动力资源，带动中国的初级/中级制造业的升级换代。

沿海地区通过土地升值和城市发展，以及获得很多较高工资的智力岗位，老百姓的生活水平得到了大规模的提升，老百姓大多进入了中产阶级行列。

中部地区通过壮大农民工队伍，使之变成产业链的中上游的方式，获得了部分百姓的生活水平的提高。

西部地区则是依靠西部大开发的战略，提供能源和原材料等初级产品，参与了发展。

但是从2008年开始，美国金融危机、欧洲高福利和主权债务危机叠加、日本20年的衰退期的恢复依然长路漫漫，这些都导致西方市场日益萎缩；与此同时，中国长期高速发展导致的环境、产能、行业布局、产业结构等负荷过重和内外部压力，都宣告了传统的发展模式将无以为继。

在这种背景下，2013年9月和10月，中国国家主席习近平在出访中亚和东南亚国家期间，先后提出共建“丝绸之路经济带”和“21世纪海上丝绸之路”的重大倡议，得到国际社会高度关注。2014年10月24日，包括中国、印度、新加坡等在内的21个首批意向创始成员国召开会议，共同决定成立亚洲基础设施投资银行。2015年12月25日，亚洲基础设施投资银行正式成立。它不仅是首个由中国倡议设立的多边金融机构，它的成立预示着“一带一路”国家战略的扬帆起航。

在这个战略中，需要三个层次的互相配合，才可以保证成功。

第一个层次是国家在政府层面上，通过政治、外交和军事合作，达成的战略共识。这一点目前看来已经基本到位，尤其是中国重点的“中巴经济走廊”和中南半岛的中线。唯一需要加强的是，军事合作和对中国海外经济利益的保护。

第二个层次是参与的中国企业在项目实际操作的过程中，如何通过国家层面的协调，达成经济溢出效应。

第三个层次是这个战略中的一个重要部分，就是伴随着人民币国际化的中国资本海外投资和跨境资本流动，会倒逼中国建立一个自己主导的、适用于“一带一路”的金融基础设施，来解决人民币的跨境支付和清算问题。目前央行主导的CIPS系统[①]，还是建立在传统的报文系统上面，据不

① 人民币跨境支付系统（Cross-border Interbank Payment System，CIPS），2015年10月正式上线。其目的是进一步整合现有人民币跨境支付结算渠道和资源，提高跨境清算效率，满足各主要时区的人民币业务发展需要，提高交易的安全性，构建公平的市场竞争环境。

完全统计，清算失败率比美元 CHIPS 系统[①] 要高 2.5 倍。

兵马未动，粮草先行。从 2010 年开始，我就一直思考在人民币国际化道路上，如何建立、通过何种方式建立中国主导的跨境支付和清算系统的问题。基于这个出发点，我与身在硅谷的一批青年才俊，试验性地建立了一家叫“井通”的科技公司，用于探讨在最先进的开创性技术区块链（Blockchain）上，实现人民币跨境通道的安全性、便利性、公信力和低成本。

区块链技术是最近在互联网技术前沿比较火的一个课题，它的出现解决了在点对点通信中一直存在的一个基本问题，即著名的拜占庭将军问题。通俗地讲就是在一个去中心化的网络中如何对一个信息传递（比如一笔支付）达成全网共识。国内目前的银行系统都是中心化的系统，银行间的结算最终都由中国人民银行的中心服务器作为所有支付行为最后的仲裁（即结算），从而解决各银行在结算中的信息不对称问题——因为所有的银行都会，也必须信任中国人民银行的结算系统。

不过在跨境人民币支付中，很多情况下由于不存在一个中心结算系统，无法快速有效地解决针对多币种跨境支付的结汇需求。目前的 SWIFT[②]、

① 纽约清算所银行同业支付系统（Clearing House Interbank Payment System，CHIPS），成立于 1970 年，由纽约清算所协会（NYCHA）经营。它是全球最大的私营支付清算系统之一，主要进行跨国美元交易的清算。

② 环球同业银行金融电讯协会（Society for Worldwide Interbank Financial Telecommunications，SWIFT），成立于 1973 年，是一个国际银行间非营利性的国际合作组织，总部设在比利时的布鲁塞尔，同时在荷兰阿姆斯特丹和美国纽约分别设立交换中心（Swifting Center），并为各参加国开设集线中心（National Concentration），为国际金融业务提供快捷、准确、优良的服务。SWIFT 运营着世界级的金融电文网络，银行和其他金融机构通过它与同业交换电文（Message）来完成金融交易。除此之外，SWIFT 还向金融机构销售软件和服务，其中大部分的用户都在使用 SWIFT 网络。

2016 年 4 月 25 日，SWIFT 通过路透社向客户发布警告称，“SWIFT 意识到，在最近的几起网络事件中，恶意攻击者通过金融管理后台的本地端口连接至 SWIFT 网络，入侵 SWIFT 客户端获得提交 SWIFT 报文的权限”。

TARGET[①] 等跨境支付结算组织都是通过建立结算中心和银行联盟，以便加入该联盟的金融机构都信任其结算中心来完成跨境支付。而在人民币跨境支付的推进过程中，要建立这种结算中心并推广使全世界的金融机构来信任是比较耗时费力的，尤其是在考虑到推行过程中某些国家的阻力时。

假如利用区块链技术，就无须建立这样一个结算中心，因为区块链技术提供了一种建立共识网络的方法而无须信任单个节点。这就使推行人民币跨境支付而无须建立像 SWIFT 这样的国际结算中心成为可能。

当然，如果认为区块链技术只专注于跨境结算，那说明我们的认知还不够全面和深入。

二、价值网

互联网在 50 年间实现了对世界无孔不入地渗透，回顾它的发展历程，有助于让我们理解未来。

1968 年，美国国防部高级研究计划局组建了一个计算机网，名为阿帕网（Advanced Research Projects Agency Network，ARPANET）。时逢美苏“冷战”，美国国防部认为，如果仅有一个集中的军事指挥中心，万一被苏联摧毁，那么全国的军事指挥将处于瘫痪状态，所以需要设计一个分散的指挥系统。它由一个个分散的指挥点组成，当部分指挥点被摧毁后，其他点仍能正常工作，而这些分散的点又能通过某种形式的通信网取得联系。1969 年阿帕网第一期投入使用，共有 4 个节点，分别是加利福尼亚大学洛杉矶分校、加利福尼亚大学圣巴巴拉分校、斯坦福大学和位于盐湖城的犹

① 泛欧实时全额自动清算系统（The Trans-European Automated Real-time Gross settlement Express Transfer，TARGET）、始建于 1995 年，1999 年 1 月 1 日正式启用，为欧盟国家提供实时全额清算服务。TARGET 由 16 个国家的实时全额支付系统（RTGS）、欧洲中央银行的支付机构（EPM）和相互间连接系统（Interlinking System）构成。

他州州立大学。位于各个节点的大型计算机采用分组交换技术，通过专门的通信交换机（IMP）和专门的通信线路相互连接。一年后阿帕网扩大到15个节点。1973年，阿帕网跨越大西洋利用卫星技术与英国、挪威实现连接，扩展到了世界范围。

发展到1975年，全球已有大量新的网络出现。由于最初的通信协议下对于节点以及用户机数量的限制，建立一种能保证计算机之间进行通信的标准规范（即“通信协议”）显得尤为重要。1983年1月1日，所有连入ARPANET的主机均实现了从NCP向TCP/IP（传输控制协议/网际协议）的转换。为了将这些网络连接起来，美国人温顿·瑟夫（Vinton Cerf）提出一个想法：在每个网络内部各自使用自己的通信协议，在和其他网络通信时使用TCP/IP协议——这个设想最终促使了Internet（因特网）的诞生，并确立了TCP/IP协议在网络互联方面不可动摇的地位，基于TCP/IP协议的公网的发展推动了互联网的发展。

互联网在发展的过程中，具有几个比较重要的特征。

1. 开放性

开放性，是指新的节点只要接受标准协议，就可以连接入网。虽然互联网起源于军事用途（阿帕网），用于连接有限的军事节点避免被同时摧毁，但是在设计之初，阿帕网就具备接入其他新节点的功能。在发展过程中，现代意义上的互联网逐渐吸收其他网络、技术、协议，在融合过程中变得越来越开放。

2. 去中心

互联网产生的初衷就是防止单点中心被摧毁而采用的多中心系统，随着后期更多的局域网和新组网技术的加入，互联网去中心的属性越来越明显。但是互联网并不是完全的去中心，在基础设施建设上，无论是根服务器还是光纤通道，都使得互联网呈现出一定的中心化色彩。另外，虽然互

联网底层是去中心的，但是建基于互联网之上的应用大多数是中心化的，以符合国家监管的需要。

3. 局域网（多样性）+ 互联网（一致性：TCP/IP）

互联网展现出一定的多样性，能够包容各类的技术、协议和网络。同时，互联网又具有一致性，网络之间主要的通信都可以通过标准的 TCP/IP 协议解决。

4. 协议分层

互联网兼具多样性和一致性的源头，就是协议分层的实现。无论是五层网络模型还是七层网络模型，核心思想都是在保持底层一致的前提下根据具体的应用扩展出市场需要的多样性。

5. 从量变到质变

在互联网的发展过程中，有一个从量变到质变的过程。当接入的节点数量相对少的时候，网络上的应用数量和社会对网络的关注相对少。整体处在技术积累的阶段。当接入的节点达到一定数量后，就出现了应用的暴发，也就是所谓的互联网革命。无数智慧和资本一起涌入互联网领域淘金、发掘创新红利，使互联网在很短的时间内得到了爆炸性的发展。

回顾了互联网发展的历史，让我们聚焦在区块链。眼下关于区块链的各类信息已目不暇接，我将其粗略地分成两类。

一类是将区块链技术作为一门比较有特点的技术，从技术的角度去改造现有的商业模式，创造新的商业模式。

另一类是把区块链技术放到通过交换创造价值这个大概念中，去发现价值网形成过程中的机会。

前者是主流的媒体和 PR（Public Relation，公共关系活动）爱好者所热衷的，而后者被很多人于无声处付诸实践。

人类社会在发展过程中，一直在追求更方便快捷的价值交换。按照交

易方式，可以大致地把人类社会分成三个阶段：物物交换、一般等价物（货币）、信用经济。我们知道，互联网对世界上的信息流通产生了根本性的变革：在传统的模型中，每传递一次物流和资金流，约有 3 倍的信息流产生和传递。互联网接入后，可以在同样的时间传递 100 倍以上的信息流。信息的充分沟通，使物流和资金流得到优化。但是由于互联网本身解决不了信任的问题，即使可以高效地实现信息和有价凭证的传输，也依然要引入第三方背书解决互信的问题。这个难题随着区块链的产生，第一次用技术的手段解决交易中的信任问题，实现为交易背书。

通过互联网与区块链的结合，可以产生类似互联网和共识协议的效果。首先，互联网提供了一个无所不在的联通网络；其次，资产和价值两端提供方（如银行）的 IT（信息技术）系统和公司的 ERP（企业资源计划）系统，可以看成一种基于价值交换的局域网；最后，当区块链技术演变成建基于类似 TCP/IP 协议之上的一种共识协议后，我们可以借助网络，连接各个局域网，构建出能够在全世界范围内进行资产交换和价值交易的价值互享网。

同时，更让我们感到欣慰的是，这种结合不同于 50 年前从无到有地新建一个网络世界，而是基于已有架构、现有软硬件布局的低成本耦合。通过盘活存量，可以塑造出一种全新的社会组织形态和商业模式。

让我们大胆地设想一下，未来的某一天，基于区块链技术的价值互享网将作为生产关系的一部分，对社会生产力产生重大的影响。因此从宏观意义上讲，区块链技术是一种可能会对人类社会产生重大变革的技术。

回顾历史，每次对社会带来重大影响的技术变革，都顺应了时代发展的内在需要。如微软操作系统的普及，顺应了基于办公自动化的社会化大生产要求；苹果文化的兴起，则体现了追求个性和解放思想的情感寄托，以及忠实果粉的文化归属感。

所以，任何技术解决方案，究其本源是要解决哲学观和方法论的问题。那么区块链技术又隐含着什么哲学观与方法论呢？

三、方法论

众所周知，区块链技术的第一个应用是比特币，比特币起源于硅谷的无政府主义者（主要是IT从业者）对华尔街作恶引发了2008年金融危机的不满。因此区块链技术从一开始就奉行极端的去中心化的思想（所有“矿工”都是验证节点）。早期的Ripple（瑞波币）、以太坊和比特币在极端的去中心化方面是一脉相承的。基于这个哲学理念，衍生出区块链技术的三个发展阶段。

1. 第一代区块链技术

第一代区块链技术发展出的去中心化、不依赖第三方认证的防止多重支付的技术解决方案，大幅度降低了中间交易和支付费用。另外就是依赖于密码技术，解决了参与方的信任问题。

但是这一代技术，在于哲学思维上对全民选举[①]形成共识机制的过于理想化的坚持，导致了效率的低下。比如比特币的任何交易和支付需要至少10分钟才能初步完成（通过改进的其他系统，可以缩短到2~3分钟），要60分钟才可以最终确认，无法满足现代网络商务要求的即时问题。

2. 第二代区块链技术

第二代区块链技术的一个方向就是像美国的Ripple公司（详见本书第四章第三节）那样，开始考虑用人民代表大会的代议制度[②]来达成系统共

① 全民选举：指类似一人一票的投票机制。

② 人民代表大会的代议制度：指通过选举人大代表，由人大代表来代理行使权利的方式。类似国外的议会制度。

识——就是对各种交易和支付的认定，不是传统中心化的单一中心认定，也不是第一代区块链技术的全民参与认定，而是依靠大家信任的人民代表大会制度来代议。

这个思路的变化首先是带来效率的提高，就是交易支付的时间缩短到3~5秒钟。但是这个技术的发明人，仍然受奥地利经济学派的影响太大，过于相信自由银行制度[①]，认为可以通过淘汰劣质个体，来达到系统最优化。殊不知，法国人勒庞在19世纪的《乌合之众》一书中就提到羊群效应的盲动性，以及带来的破坏的严重性。

以美国在美联储建立之前的1907年自由银行体系下的金融危机为例，当时美国金融体系靠的是人治，因为劣质银行的倒闭带来系统崩溃危机时，依靠的是老摩根[②]的个人领袖魅力，在全系统里面达成了共识（中心化决策机构），从而避免了灾难性的打击。美联储机制形成以后，是用制度建设代替了人治，让情况有了改善。不过很遗憾，制度也要靠人来执行，当执行的人乱来一气时也会出现系统风险。所以我们看到了格林斯潘和2008年的金融危机。

客观地说，虽然2008年的金融危机是由于西方金融系统里面的央行不负责任、商业银行和投资银行自私自利，导致社会大众对金融体系产生了信任危机，但是，人类社会的结构本身就发源于人类成员之间的相互信任。所以，正确的做法是从技术上解决系统性风险“地雷”，同时在法律和制度上加强监管，而不是彻底放弃中心化，完全丢弃人与人之间的互信这个社会基石。

任何技术的发展，都要以服务于社会需要为原则。所以区块链技术真

① 自由银行制度：指的是一种完美竞争的金融体系，在这种体系中，私人银行可以在没有重大法律限制的情况下，竞争性发行通货，而不是由国家设置的中央银行来垄断发行。

② 约翰·皮尔庞特·摩根（John Pierpont Morgan Sr.，1837~1913年），美国银行家。

正的社会目的，是撼动目前的金融体系，迫使银行系统进行改革增强自我约束，重新建立社会的信任，而不是彻底丢弃人类的信任，来开发出一个完全无信任感的交易支付系统。

不同于推崇个人主义的西方文明，东方文明更加重视人与人的互信和中庸，东方人的科技创新和优化，也正是这种文明熏陶的必然选择。

3. 第三代区块链技术

第三代区块链技术版本的核心用一句话概括，就是变“绝对去中心化”为“有效去中心化”。据我所了解，我是最早提出这个概念的人，而井通公司则是第一家将其付诸实践的商业化公司。因为下文会提到“有限去中心化”的概念，为了更好地理解“有效去中心化”和“有限去中心化”，有必要在这里先对两者的区别做个介绍。

有效去中心化：在哲学理念上我们认为中心化和去中心化，是阴阳互补而非对立。因此着重点是通过保存中心化优点的同时，有效地利用去中心化的技术，来实现更加优化的效用平衡。有限去中心化：是在事后（而非像我们是事先）因为彻底去中心化的失败而做出的一种改良反应。认为也许只有自动放弃完全去中心化的立场，才可以在现实中走得通——算是承认了完全去中心化存在技术短板。

在第二代区块链技术版本上发展的第三代区块链技术，首先是对底层的区块链进行了改革。其次是在这个层次上面建立了实名认证的用户体系。这个体系和区块链信息的关联，是属于非公开的保密信息，用来保护企业和个人的隐私。当然国家监管部门出于对金融安全、反洗钱和反恐金融的原因，可以随时查阅，并可以提供限制、封锁账号和监控的功能。最后就是在用户体系上建立类似于社交网络的关联逻辑，从而提供低成本的信用体系评估。

在井通发展初期，市场还是厚此薄彼的：对这个技术非常有看法的先

驱人士，包括硅谷的安德森[①]等，还是用小写的比特币（bitcoin）来描述比特币系统，而用大写的比特币（Bitcoin）来描述比特币系统底层的区块链技术。而且在如何使用区块链技术来解决实际问题的实施策略上，也存在两种不同的路径。

第一种路径，就是利用比特币系统已经存在的现有架构，对比特币协议里面的部分内容进行重新定义，从而开发出新的应用。走这条路子的，包括 Metacoin、Colorcoin 等[②]。这种做法的优点是显而易见的，因为可以依赖比特币系统底层而无须自己开发。但是其缺点也显而易见，因为如果应用需要通过底层功能改进而实现的话，很可能难以说服比特币技术委员会来落实相关改动。而且更重要的一点是，目前比特币社区关于保持或扩张区块规模的争论[③]，不仅是关于定义比特币系统作为一个现金支付系统（中本聪的原意），还是成为一个交易清算系统（目前的发展趋势）的区别，更牵涉比特币系统是应该坚持彻底去中心化道路，还是向现实妥协转为有限的去中心化的哲学观之争。

基于与上述哲学观的不同，我们从一开始就选择了第二种路径，即建设自己的底层系统，同路人包括我们熟悉的 Ripple、以太坊。当然，这些系统的方向，是不应该和拷贝比特币系统的山寨币（莱特币、狗币、元宝币、暗黑币等）相提并论，毕竟自建系统的目的是更好地服务于各类产品的应用。

在研发初期，我们曾深入研究过 Ripple 的技术模式，但因为发现其存在很大的缺陷和漏洞，所以硅谷团队从 2011 年就开始重新进行底层架构

① 马克·安德森：出生在爱荷华州一个小镇的普通家庭，9 岁开始接触计算机，1993 年他同吉姆·克拉克一起苦干 6 个星期，开发出 UNIX 版的 Mosaic 浏览器。后来公司的名字被改为“网景”（Netscape），浏览器的名字也被改为 Navigator。马克·安德森被誉为“因特网的点火人”。

② 以比特币系统建基的支付应用、开发智能合约等应用领域不在此列，如 Circle、Coinbase 等。对于这类应用而言，比特币底层已能完全实现其需求。

③ 一种观点是继续保持区块 1MB 的规模（每秒钟只可以处理 7 笔交易），另一种观点是依靠硬分叉扩张到 2MB 的规模。

设计，经过了多次推倒重来，最后终于搭建了一个具有完全知识产权的区块链底层平台，并从2014年开始通过商业应用开发进行验证。在自建系统的实践过程中，我们逐步形成并总结提炼出符合我们老祖宗的哲学观和方法论。与西方思想更容易接受非黑即白的判断题相比，东方思想更像是有多种选项的选择题。

（1）当作为中心化的云计算、大数据方兴未艾的时候，作为其对立面的去中心化的区块链也风起云涌，正好是中国人阴阳平衡思想的体现。因此，与我们海外同行追求“替代中心化的极端去中心化路线”的观点不同，我们认为区块链不是云计算、大数据等中心化的替代，而是有益补充和平衡。正如古人所言，“阴在阳之内，不在阳之对”。中心化和去中心化，就是一对阴阳，你中有我，我中有你，相辅相成，缺一不可。

（2）基于此，我们认为，相对于彻底或者极端的去中心化的想法，我们追求的是一种中心化与去中心化的平衡，我称之为“有效去中心化”。经历了“The DAO”事件（详见本书第四章第二节）后，行业人士也逐步达成了“有效去中心化或者成为区块链主流”的认识。对此我们可以很自豪地说，有效去中心化一直是我们这三四年的基本方针。

（3）有效去中心化的基本思路就是，如何在保持中心化带来高效率的同时，避免其带来的可靠性的不足。对此，我们的解决思路是选择一个有效的优化区间，而非一个优化点。从绝对的中心化到彻底的去中心化，中间有很大的一个区间，我们完全没有必要画地为牢，自我限定只能选择两个极端，而要因势利导、对症下药：可以根据不同应用的场景，结合不同行业的实践，来找到最符合使用者需求、成本最经济、使用最便捷的那个平衡点，即选择一个有效去中心化的节点。在这个节点，既能够享受去中心化的安全和成本优势，又不至于过度地去中心化而降低效率。

（4）当然，有效去中心化也需要符合区块链技术的核心要求，如节