区块链技术指南

作者：邹均

区块链技术指南

邹均　等著

ISBN：978-7-111-55356-4

本书纸版由机械工业出版社于2016年出版，电子版由华章分社（北京华章图文信息有限公司，北京奥维博世图书发行有限公司）全球范围内制作与发行。

客服热线：+ 86-10-68995265

客服信箱：service@bbbvip.com

官方网址：www.hzmedia.com.cn

新浪微博 @华章数媒

腾讯微博 @yanfabook

目录

本书作者

邹均： 中关村区块链产业联盟专家、服务合约（Service Contract）方向博士，关注与实践区块链技术与应用。擅长云计算、大数据、软件定义存储。现为海纳云CTO，曾任IBM澳洲金融行业首席软件架构师、多个云计算公司高管，是融智北京高端外国专家。在国际会议期刊发表论文20余篇，获2015年澳中校友会ICT和媒体类别杰出校友奖，区块链相关论文获2016年IEEE ICWS最佳博士论文奖。【欢迎加入罗友书社，微信：15535237487，罗辑思维，得到APP，樊登读书会，喜马拉雅系列海量书籍与您分享】

张海宁： VMware中国研发中心云原生应用首席架构师，西蒙弗雷泽大学计算机科学硕士，多年软件全栈开发经验，Harbor企业级容器Registry开源项目负责人，Cloud Foundry中国社区最早的技术布道师之一，国内最早的iOS开发者。在VMware公司先后负责开源PaaS平台Cloud Foundry、大数据虚拟化、软件定义存储VSAN等领域的技术布道和解决方案推广。目前着重关注区块链、容器和云计算等领域的研究和开发工作。之前曾担任IBM资深软件工程师、Sun公司资深解决方案架构师等职务。

唐屹： 广州大学教授、理学博士，专注于区块链安全与应用、网络信息安全、分布式计算等，为国外知名安全公司开发过椭圆曲线密码软件，获密码科技进步二等奖（省部级）。主持或参与完成多项国家级或省部级自然科学基金与人才计划等重点项目。

李磊： 合肥工业大学副教授，Macquarie大学博士。擅长数据挖掘、社会计算、智能计算。获2011年澳洲最优博士论文提名，并多次担任IEEE国际会议的程序委员会委员及组织者。在社会计算和区块链等领域发表论文40余篇，被引用350余次。

刘天喜： 深圳拓邦股份有限公司总经理助理，高级工程师、北京大学博士。在移动通信、集成电路、移动互联网、物联网等领域深耕多年，擅长技术产业研究、行业分析和战略规划，主导或参与中国工程院、中央网信办、工信部、国资委等十余项产业研究课题。发表学术论文10余篇。

陈晖： 区块链PPk开源项目发起人和主要开发者、巴比特网站专栏作者与区块链技术版版主。对网络与通信技术有深入实践与研究，十余年的软件研发和项目管理经验。通过深度实践以比特币为代表的数字加密货币领域，率先提出“区块链+网络通信”将最大化发挥区块链革命性价值的观点，并着力以开放开源项目的形式推动区块链与网络通信领域融合的技术创新和应用发展。

曲烈： Macquarie大学博士，曾任Macquarie大学研究员、助教。从事信息安全、密码学、区块链、服务计算以及信息系统等领域的研究。多次在国际知名会议和期刊发表论文，并受邀宣讲。

郑晓明： 中国电信云计算分公司工程师、Macquarie大学博士，专注于云计算、云存储、监控系统、推荐系统、模式识别等，近期研究区块链相关技术。

序一：什么是区块链

2015年是国外区块链的元年，世界许多重大组织，包括高盛、花旗银行、英国央行、美国央行等机构纷纷在区块链上面投资。大量的投资从2015年10月开始便进入了区块链，原因是在《华尔街日报》刊登一篇的文章，里面报道区块链经过了多次的实验和验证，许多金融机构证实了区块链是一个颠覆性的技术。之前华尔街日报甚至宣称，区块链是最近500年以来在金融领域最重要的突破。而这500年来有多少科技上的突破，但华尔街日报却说区块链是人类历史上在金融领域最大的突破。这可能是因为出现了一个新的货币媒介，而每一次新货币媒介出现，都会引发社会和经济上的重大改革。

2016年1月，英国首席科学家建议英国政府把区块链技术列为英国国家战略，这是区块链历史上一个重大突破，原因是基于华尔街以及金融机构对区块链的评价。但自从2016年1月以后，区块链的评价是基于科学历史悠久的英国官方的评价。从各样指标来看，英国在科学上的建树经常是排名第二，仅次于美国。而世界科学排名第二的英国甚至把区块链列为国家战略，表示区块链的重要性毋庸置疑，而且有深远的影响。能够成为国家战略必须在科学上被验证过，另外还必须带来巨大的商业价值，两者都不可缺少才能成为国家战略。笔者曾在2016年3月拜访英国首席科学家，他们认为，区块链可以在各行各业使用，带来行业公平，例如：诚实报税、政府监管、反洗钱、国家安全等。

2016年可以说是中国区块链元年，因为在2016年区块链在中国受到极大的重视。首先是1月的时候，人民银行宣布要使用数字货币。然后在30日以后，许多中国的组织单位就开始投资区块链。中国许多大学也开始研究区块链技术，大型金融机构都纷纷表态成立区块链团队来研究区块链，区块链的讨论班以及研讨会如雨后春笋一般大量涌现。

但到底什么是区块链？笔者在2015年开始研究区块链，就发现了一件事情：学生们在实验，提出来的区块链模型、算法，或者架构都是有偏差的，而且有时候偏差甚大，例如，在设计私有区块链的时候把公有区块链的全部思想搬过来。结果不像私有区块链，但也不像原来的公有区块链。另外发觉很多人对相关的算法不熟悉，所以有的时候会有一些错误的看法，例如拜占庭将军的问题是一门专门的学问，而区块链只是用了一个近似的算法，若是把两者混为一谈，就会让人感到迷惑。

再加上在讨论区块链时，有时候会有情绪化、宗教化或者政治化的言语出现，原来在数字货币领域，数字货币的先锋常带有一些政治思想，如无政府主义。再加上原来的数字货币过去有洗钱、犯罪的记录，所以在讨论时，有时候会失去焦点。这一点在英国首席科学家的报告里也有提出来，他们认为应该重视区块链，把区块链当做一门科学技术来看，而且是一门有助于经济的科学技术，而不是吹捧任何政治思想，或传递宗教概念。

笔者从今年初开始多次提出应该以系统工程角度来发展区块链技术，例如基于云计算、软件工程、数据库等系统工程技术来开发区块链，区块链不只是一个加密技术或是数字货币，而是一门系统工程。区块链不是某些特殊政治思想的乌托邦，或洗钱的工具，而是一门科学家和工程师可以研究的系统工程，而且这项技术可以成为国家战略，改变各行各业的流程以及基础设施。英国首席科学家已经做出这样的判断，英国央行也做出了类似的决定，英国政府已经派了两位部长来领导这项计划，这就是我们所期待的。

所以我非常高兴像邹均、张海宁、唐屹、李磊、刘天喜、陈晖、曲烈、郑晓明这些年轻的学者们开始书写区块链技术，因为现在市面上有关区块链的书都是在讲解区块链的概念及应用场景，但是今天描述区块链技术的书却很少。我们希望读者能多了解区块链技术，多发展区块链技术，并且加以应用。只有我们了解区块链技术之后，才能真正理解区块链的意义，而不会随波逐流，人云亦云，并且有自己的判断，希望读者们能够认真读这本书，了解区块链技术，相信必定会大有收获。

蔡维德

美国亚利桑那州立大学荣誉教授，北航区块链实验室主任

序二：区块链——未来已来，只是尚未流行

比特币诞生于2008年美国次贷危机的末期。在比特币白皮书，即中本聪的论文《比特币：一种点对点的电子现金系统》中，还没有“区块链”这个词，只有“区块”（Block）和“链”（Chain）。一些人为这种超越主权、不会滥发的虚拟数字货币而欢欣鼓舞，开始积极投入到挖矿、炒币中，甚至发行自己的数字货币进行筹资（ICO），俗称“币圈”。而另一些人，包括很多专家和学者，则专注于比特币底层技术，对区块链（Blockchain）技术和应用进行深入地研究，考虑能否将这个技术加以改进，运用到更多的领域中去，俗称“链圈”。

七年之后，以2015年10月美国《经济学人》杂志发表的《信任的机器》（The Trust Machine）的封面文章为标志，大家意识到，作为比特币底层技术的“链”，其价值远大于比特币本身。区块链可以让人们在没有中央权威机构监督的情况下，对彼此的互相协作建立起信心。简单来说，它是一台创造信任的机器。华尔街开始热捧区块链。Gartner发布的2016年技术炒作曲线图表明，当前区块链正处于期望的最高点，即“过度期望期”，这也意味着在未来不久的一段时间，区块链将坠入“期望幻灭期”。人们对区块链的过度期望，实际暗示着对其存在很多误解，其中最典型的有三个，因为其关键词的首字母都是D，所以笔者将其归纳为“3D误区”。

误区一——区块链是一种颠覆性（Disruptive）的新技术

首先，区块链不是一项新技术，而是一个新的技术组合。其关键技术，包括P2P动态组网、基于密码学的共享账本、共识机制（拜占庭将军问题，即一种分布式场景下的一致性问题）、智能合约等技术，都是已经有十年以上的老技术了。但是，中本聪将这些技术很巧妙地组合在一起，并在此基础上引入了完善的激励机制，用经济学原理来解决传统技术无法解决的问题。

其次，这个技术组合虽然有其独到的创新之处，但并非是颠覆性技术，是现有技术的有力补充。目前大部分人已经认同，区块链是“价值互联网”的基础协议，从这个角度看，其地位与当前“信息互联网”的HTTP协议相当，两者都是建立在TCP/IP协议之上的应用层协议，同是互联网的两大基础协议。因而，两者是互补而非颠覆的关系。

最后，这个技术组合，并未颠覆现有业务，而是引入了新的思想，去改善和改造现有业务模式，从而为大众提供更好的、普惠的服务。《华尔街日报》在2015年1月曾发表题为《比特币与数字货币的颠覆性革命》的文章，认为比特币的数字货币发行机制可能“颠覆”目前各国央行的法定货币发行模式，这算是最接近“颠覆”性的区块链案例。而实际上，比特币在经过8年多的发展后，虽然总市值发展到了100亿美元，但在全球经济活动中的比重还是微不足道。与此同时，也确实有一些国家的央行，如英国和中国，在考虑摈弃比特币的挖矿机制后，通过借鉴数字货币的一些机制，在一定范围内实现可跟踪、可追溯、数字化的法定货币。

误区二——区块链就是去中心化（Decentralized）的

首先，很多人认为Decentralized是区块链的核心特征，并将其翻译为“去中心化”。然而这个最早由国内“币圈”所做出的翻译，多少有一点主观和政治化的色彩。作为软件系统的网络架构一般有三种模式：单中心、多中心、分布式。单词Decentralized只是表明不是单中心模式，可能为多中心或弱中心，也可能是分布式的。所以在中国台湾地区，大多将Decentralized翻译为“分散式的”而不是“去中心化的”。

其次，在中本聪的整篇论文中并没有提到过Decentralized，而只有Peer-to-Peer（P2P）。在2016年6月召开的W3C区块链标准会议上，以太坊的核心开发团队EthCore就明确表示，不再使用Decentralized这个词，而是用P2P、Secure、Serverless这类纯技术性词语。

最后，The DAO事件表明，完全去中心化是不可行的。The DAO是一个基于以太坊公有链的众筹项目，它在短时间内就募集了价值1.6亿美元的数字货币，成为史上最大的众筹项目。然而由于其智能合约的漏洞，导致The DAO被黑客攻击并转移走价值6000万美元的数字货币，最后不得不黯然落幕。在挽回这个损失的过程中，原有的去中心化机制未能解决问题，最后还是通过“集中式”的方式，强制以太坊进行“硬分叉”完成交易回滚。但这也导致了以太坊社区的分裂，产生了ETH和ETC这两种同源却又不同价格的数字货币，给以太坊生态系统带来了很多负面影响。此次事件之后，很多人对区块链的“去中心化”进行了反思。前上交所总工、ChinaLedger联盟技术委员会主任白硕则认为“去中心化不是区块链的本质特征”。万向控股副董事长兼执行董事肖风则进一步阐述“区块链的核心是分布式而不是去中心”。

误区三——区块链交易存在很大的延迟（Delay）

在使用比特币进行支付时，一般需要10分钟才能完成一次支付确认。如果要保证支付交易的不可逆转，通常需要等待连续的6个数据块完全确认，这至少需要1个小时的确认时间。而我们通常使用的银行网银支付和第三方支付，通常都是秒级完成的。与之相比，使用区块链的比特币支付实在太慢。

然而，我们再考虑一下跨境支付的场景，当我们使用Swift完成一次跨境汇款时，通常需要3~5个工作日，对方才能收到相应的款项。而使用比特币进行跨境汇款，仅仅需要一个小时就能收到汇款。如此比较起来，比特币支付已经是非常快了。

为什么有两个完全不同的结论？因为，对于比特币支付来说，支付确认过程即是清算和结算的过程。如果把支付过程和清结算过程作为一个整体，来比较两类支付的延迟时间，使用区块链进行交易还是很快的。区块链交易的本质，是大幅减少了交易后的处理工作，消除了大量的人工干预过程，从而提高了交易效率。

通常我们把区块链分为公有链、私有链、联盟链三种，比特币和以太坊都属于公有链范畴。在数字货币之外的场景中，尤其是在金融领域中引入区块链技术，将面临很多问题。如何引入以及引入哪种区块链，还存在许多权衡决策方面的障碍。

第一，主流金融机构难以接纳公有链。 R3发布最新研究报告，证明公有区块链不可作为金融机构解决方案。2016年Swift发布白皮书指出，当前世界主流金融机构无法接纳公有区块链。对于这些金融机构而言，需要的是一个自主可控的系统，而公有链显然做不到这点。

第二，私有链与公有链架构差异大。 笔者曾仔细分析了以太坊和超级账本这两个典型区块链的模块结构，发现两者差异巨大。很多公有链的核心模块，如挖矿、PoW共识、原生货币等，在私有链环境中是完全不必要的，甚至是有害的。与此同时，公有链系统中还缺失一些诸如身份认证、权限管理等在私有链中必要的模块。以太坊创始人Vitalik也曾坦言，只有5%的以太坊程序可被金融领域使用。[1]

第三，私有链和联盟链还很不成熟。 目前，以比特币和以太坊为代表的公有链相对比较成熟，而私有链和联盟链则远远不够成熟。开源而且好用的联盟链，更是不存在。目前全球影响力最大的开源联盟链，是Linux基金会下面的超级账本（Hyperledger）项目，目前已有95个成员单位。旗下的Fabric子项目是以IBM捐献出的OpenBlockchain为主体搭建而成的，目前还处在0.6版的快速迭代过程中，到0.8将是Alpha版，而0.9则是Beta版，再经过3个RC版本之后，才会进入相对成熟的1.0版。

想要找到或研发出一个成熟稳定的、适合金融领域的联盟链底层系统，还任重道远，需要很多仁人志士的共同努力，踏踏实实地投入到区块链的基础研究中去。

在目前已出版的区块链书籍中，有很多都冠以“革命”、“重塑”、“重新定义世界”等煽动性词语作为书名，这更像是一种口号，而非切合实际的研究。我很高兴地看到，还有像邹均、张海宁、唐屹、李磊、刘天喜、陈晖、曲烈、郑晓明等这些研究者们，在踏踏实实地研究区块链底层技术，用普实的话语来介绍和普及区块链技术，让更多的人了解和接受区块链技术，实实在在地让人们了解区块链技术特征和特点，以及在现阶段环境下的不足，如何去改善这些不足等。知己知彼，方能百战不殆。世上没有“银弹”，没有哪一种技术能解决所有的问题。

希望读者们能够通过本书，深入地了解区块链技术。也只有深入了解其底层运作机制和原理，才能更好地灵活运用该技术，取得理想的效果。

未来已来，只是尚未流行，我辈仍需多努力。

张斌，联动优势科技有限公司CEO

[1] 参见《金融电子化（2016.5）》P60，《区块链技术在金融领域的应用解析》。

序三：区块链——连接虚拟与现实

我们对于一种新兴的技术，往往会在短期内对它有过高的不切实际的期望；泡沫破灭后，在长期的时间轴线上，又往往会忽视它的深刻影响，这一句话，用在区块链上，再合适不过。

区块链的发明，是建立在互联网之上。其所使用的技术，像P2P、分布式存储、分布式密钥的思想，十几年前就已经存在，但是如果没有中本聪那一篇开创性的关于比特币的白皮书，所有这些强大的工具，都还只是埋藏在学术论文堆里。因为这些工具单独使用，并不能解决问题，只有中本聪，出人意料地提出了一个系统性的、可供实践的解决方案。如果他能提前十年提出这篇论文，那么比特币就可以提前十年发明出来。所以，单个技术点，并非是区块链的魅力所在，运用这些技术的全新思想，才是区块链的本质和核心。

单纯把区块链等同于一种分布式数据存储技术，就像将浏览器说成是一个网页解释器，将手机说成是一台手持电话，将云计算说成是一个服务器的集群一样，说了等于没有说，甚至比没说更糟糕，更容易造成误解。当全球的用户都打开浏览器访问网页，当街上每一个人都携带着一台能拍照、能上网、带GPS，运算性能可以发射登月火箭的智能手机，当我们所有的工作和生活数据都发生与存储在云上的时候，我们看到在浏览器、移动互联网和云计算上所承载的产业生态，跟最初的技术描述相比不知道差了多少万里。所以有人让我用一句话解释什么是区块链的时候，我往往会争取机会多说几句，争取让人更多了解一点。

从功能上说，互联网实现了信息的传播，而区块链实现了价值的转移。互联网在最开始的时候，就是以信息传输管道的模式进行的设计，TCP/IP协议底层并不关心上面传输的数据有什么差别——对于底层的交换机和路由器来说，一切都是0和1而已。无差别的信息传输，创造了信息复制的便捷通道，也造就了今天信息爆炸的信息社会。但是互联网虽然解决了信息传播的问题，却带来了信息权属的新问题，我们可以将一首歌曲或者电影，在几个小时内传遍全球，我们却不能知道，究竟是谁拥有这部电影的权利，是通过什么样的路径进行的传播。而区块链则可以做到，我将一个数据，发送给另外一个人之后，我自己就不再拥有这个数据的所有权，从而实现了可以利用一个虚拟的系统，来传输实际的价值。

从机制上说，如果说TCP/IP是机器与机器之间的通信协议，而区块链就是机器与机器之间的信任机制和合作协议。对于不需要验证真假的信息传输来说，TCP/IP已经足够可用，但是一旦属于不同实体的计算机，需要彼此之间进行自动化的沟通和合作的时候，问题就会变得相当复杂。现实世界公司与公司之间的合作，有律师和合同来进行条款约定，有执法机关来保障合同的实行，而在虚拟世界，计算机没有办法开设银行账户，属于不同实体的计算机，也没有办法去法院起诉对方，因此在沟通和合作的时候，一定要有一种有效的机制，来快速实现共同协作。区块链就可以起到这样一个作用，所以在区块链行业中有一句话：代码即法律（Code is the Law）。未来不管我们的生活还是工作，都会有越来越多地需要计算机参与，人类将整体进入后人工智能时代，区块链就是在为这个时代的到来进行前期的铺垫和准备。未来我们将会看到无人驾驶汽车，通过区块链协议自动缴纳过路费用；智能投资顾问自动为我们计算各种投资组合；未来最先进的金融公司，也会像现在的无人工厂一样，看不到太多工作人员，只有无数的计算机，在快速地缔结无数的智能合约，进行精确到小数点后的资产配置。

因为区块链的以上属性，区块链将会是连接虚拟世界与现实世界的最佳桥梁。在未来，区块链所连接的，不会像比特币一样是无法辨别的匿名账户和价值不定的虚拟资产，而将会是千千万万真实存在的个体和公司实体。上面所承载的资产，都将具有现实的价值和对应物，而这个虚拟的网络上发生的一切，也都会直接作用于现实世界。这一过程，需要的不仅仅是单纯的技术，还需要金融、商贸、法律、政府等各方面专家和人才凝聚在一起，来保证这一映射的有效性，也是我们一直在努力推进区块链生态系统和可信区块链概念的原因。区块链有巨大的潜力和未来，而这些潜力和未来，需要社会的共识与力量来共同推进和实现。

邓迪

太一云科技有限公司董事长兼CEO

序四：区块链——转型之擎

邹均先生在国内外企业的IT架构、云计算、大数据、IT产品创新方面有很多年的经验，邹均本人也是我多年的好朋友和同事。这次邹均先生主写的这本区块链的书，相信一定会在IT业内，特别是在企业IT架构圈内产生巨大的反响，一定会深受广大区块链爱好者、参与者、实践者的热烈欢迎。

我和邹均先生工作背景相似，曾经从事过多年企业IT工作，从2009年开始，做云计算的创新，近年来也做金融科技的创新。从我这一年多时间的区块链的实践中，我个人看到区块链目前虽然还在发展初期，而每天区块链技术都有新的变化和突破，每天都是“山雨欲来风满楼”。但是区块链这样一个意义重大的技术，对整个IT的架构、基础协议、标准、运营、环境具有颠覆性的意义。因此我们应当充满紧迫感，应当预先了解区块链技术、商业模式和发展趋势，加强与国内外各界的合作，特别是在区块链的底层领域、区块链的平台领域和区块链的应用领域的合作，我们应当在区块链的全球协议和标准方面要占据主动。

区块链技术具有全新的理念和逻辑结构，并且它每天还处在发展变化过程中，因此区块链技术与应用在企业内不可能单打独斗，区块链的应用必须在企业架构中上着天、下着地，和企业现有的应用系统相互关联。我们不应该简单地把区块链理解为一项技术，而应当考虑它在更高的企业IT架构转型层面的作用。区块链的应用不是简单地提供一个只能追加、不能更改的分布式数据库解决方案，而是要把区块链与云计算、大数据和传统企业的系统相互关联，使得企业系统由原来的传统系统和云计算这种“双核驱动”转变为传统系统、云计算与区块链的“三核驱动”，让企业的异构系统更好地发挥协同效应，一起解决原来传统IT系统难以解决的问题，这样才能更好地发挥区块链的独特性，才能够使传统企业IT架构更好地转型。

本质上，因为区块链链与链之间具有隐私、安全、共识、自治、价值共享的特性，所以在技术层面解决了互联网上的价值传递问题。同时，区块链又具有底层开源和改变业务规则、创新业务多方共识等逻辑，因此区块链是未来整个IT架构和互联网转型的重要支撑。而企业与互联网IT架构的转型也为未来经济的转型、服务模式、信用交换和商业规则的转型提供了关键支持，因此研究和应用区块链不仅要研究技术，更要注意在互联网时代赢者通吃的规则，重要的是要研究和应用区块链带来的商业规则的改变。

以前我们的信息化，不管是企业信息化、政府信息化，还是个人信息化，实际上都侧重在机构内部的信息化。这几年随着互联网、云计算、大数据、平台经济的蓬勃兴起，现在IT正在促使企业由内部信息化转型为外部信息化，最终通过平台转型为信息化的企业，由政府信息化转型为信息化政府，由个人信息化转型为信息化个人，这些词虽然相似，但性质具有很大的不同。它们在逻辑关系、业务处理方式、信息的确权、信息的使用、组织流程的改变、企业治理结构方面有很大不同，信息化已经不再是工具、手段和渠道。这样一个信息化平台的升级，未来会使得实体经济更好虚拟化，使得虚拟经济更好地结合实体化。

实施区块链既需要具有传统IT系统的经验，也需要有互联网、云计算、大数据的实施经验，需要对整个IT系统变迁具有很强的洞察力，需要把整个IT系统协同起来，让整个IT系统互联互助，相互合作。因此，区块链系统在企业的应用，必然需要结合本地的实践，发挥原创的精神，必然还要有互联网时代产品开发的能力。而做一个好的区块链应用更需要研究共享经济理论、价值互联网和金融科技的创新与发展。这一切都需要在区块链理论与研究方面走到前列。

因此，我希望邹均先生等人写的这本区块链的书籍，会连接IT架构的过去、现在与未来，开启大家创新的热情，会对行业产生影响，同时为大家开启一扇协同企业传统系统、云计算、大数据和区块链新的大门。

黎江

北京世纪互联创新研究院院长

前言

为什么要写这本书

1900年9月8日，一场4级强度的飓风横扫德克萨斯州的加尔维斯顿。这个位于墨西哥湾的岛城，靠近德克萨斯海岸，在灾难来临前拥有37000人口和光明的经济前景。飓风猛烈攻击了这个毫无防备的低海拔城市，给该市带来了巨大的毁坏。飓风风速为每小时225千米，毁掉了3600座建筑，使占整个城市3/4的12个街区彻底消失，死亡人数为8000~10000人。是迄今为止，美国历史上死亡人数最多的自然灾害。

而2016年8月2日在中国华南沿海登录的“妮妲”台风，风力14级，最高风速每小时151.2千米，台风过境的广东、广西、湖南、贵州、云南5省（自治区），虽然也造成了重大经济损失，但在人员伤亡统计报告中，只有1人失踪。

这两次自然灾害的结果如此不同，归功于人类掌握了计算这个神奇工具。在妮妲形成过程中，美国、日本、中国气象监控部门就不断跟踪，通过监控数据，气象数学模型和强大的计算能力，对台风进行了准确的预报和预警。在台风到来前，有关部门做了积极准备，7.6万人得以紧急转移安置，使得损失得以降到最低。

今天，IT已经渗透到各行各业，人们已经能近距离接触无人驾驶、机器人、虚拟现实（Virtual Reality）、增强现实（Augmented Reality）等先进技术，当人们在享受IT给人们生活带来的各种便利和好处的时候，也日益感受到来自不当使用科技所带来的挑战。例如，国内日益猖獗的电信诈骗，全球范围内黑客的攻击和安全勒索，以及未来基因技术和AI（人工智能）技术给人类所带来的伦理、生活和工作方面的全方位冲击，都使得有识之士开始思考如何应对科技发展所带来的风险。

一直以来，笔者对计算技术有一种既感恩又敬畏的情结。首先感恩我们的时代，计算技术的发展使我们避过很多前人无法避过的灾难；但高速发展的计算技术必然导致机器的智能超过人类自身，因此而产生的未来不确定性也使笔者的敬畏之心油然而生。

笔者也一直有一个预感，未来可能需要针对IT，特别是与业务结合紧密的云计算和智能设备建立监管、问责的机制。笔者的意思不完全是对从事IT或智能设备的人进行监管问责，甚至要考虑对智能设备进行自动问责。这个看似荒谬的想法促使笔者选择了云计算的问责机制（Accountability in Cloud Services）作为博士研究方向。

所谓云计算的问责机制（Accountability），指的是在云计算架构中，能建立一个自动化的问责机制。该机制包括形式化的标准服务合同定义，服务合同的发布，服务合同执行的监控，合同违约方的自动发现，违约方的罚则和执行，以及合同双方争议的仲裁。举个例子来说，今天公有云的提供商，都没有提供能让电脑理解的云服务合同。合同双方的责任、义务和权利没有精确的界定；云服务提供商的服务好坏，是否遵从合同，都没有自动化的方法去检测；服务故障责任也没有办法界定；出现争议也只能靠人工去解决。而云计算的问责机制，旨在建立一个自动化的体系来让电脑自动规范电脑的行为。

可想而知，这个研究课题非常有挑战。在博士研究的过程中，笔者也走了很多弯路，一直没有找到好的解决方法，直到三年前接触到比特币，突然意识到区块链技术是提供问责机制的最理想平台。这是因为区块链技术中的防伪、防篡改、交易可追溯、数字签名和智能合约技术提供了一个公正、可问责（Accountable）、自动执行的技术平台基础。

但是区块链目前还停留在概念炒作阶段，很多关注点还停留在金融应用，特别是虚拟货币方面的应用。笔者认为，区块链未来可能最适合作智能设备的“警察”，为物联网和智能设备的自治管理提供一个基础平台。区块链技术应该推广应用到除金融外的行业，因此萌生了写这本书的念头，作为博士研究工作的一个延续。

而写这本书的另一个原因，也是深感在学习区块链技术过程中碰到的参考资料不足的痛苦，希望能整理过去的学习所得，对区块链初学者有所帮助。

从2008年中本聪发表比特币白皮书算起，区块链技术才走过短短8年的时间。虽然区块链1.0、2.0和3.0的架构理念已经提出并得到一定程度上的认可，但区块链的技术发展仍然处于初级阶段，区块链的应用还刚起步，成熟的区块链应用除了比特币系统，还寥寥无几。在这种情况下写关于区块链的书籍，其实面临一个两难境况。一是区块链的技术变化快，像个移动的靶子；可供参考的资料又少，要准确把握一个快速变化的技术非常困难，而且受限于写笔者的水平，实践经验，写出来的书难免有很多错误，弄不好会贻笑大方。而另一方面，正因为变化快，资料少，广大区块链技术爱好者又渴望能找到一本对他们学习、理解、掌握区块链架构和技术有所帮助的书。

目前在市场上的区块链书籍大致分为两类：一类是以梅兰妮·斯万（Melanie Swan）的《区块链：新经济蓝图及导读》为代表的，谈区块链对整个宏观层面所带来的革命性影响的战略性书籍；一类是以安德鲁·安东普洛斯（Andreas M.Antonpulos）的《精通比特币》，以及普林斯顿大学以阿文·拿瑞延南（ArvindNarayanan）为首编著的《比特币和密码学技术》为代表的专注于比特币的技术性书籍。这些书籍满足了目前市场上一部分对区块链在行业中的应用有兴趣的偏业务的人士，以及对比特币技术有兴趣的偏技术的人士的需求。

在这两类书籍所覆盖的市场中，其实还有一个很大的空白。我们发现，在对整个区块链架构（包括区块链1.0、2.0和3.0）进行系统性剖析，包括对其中关键技术（密码学、共识算法）等进行系统性论述，对不同的区块链架构形式（联盟链、公共链、私有链、侧链、多链、互联链等）进行系统性介绍的书好像还没有。而这样的书对理解、普及区块链技术，推动区块链应用落地可能会有所帮助。因此，与其等待这样的书籍出现，不如自己行动，为区块链技术的推广尽绵薄之力。笔者也就自不量力，把可能被同行笑话的风险置之脑后，鼓起勇气集合几个对区块链着迷、志同道合的朋友，在条件不成熟，时间比较仓促的情况下，经过不少不眠之夜的努力，克服重重困难，特别是在机械工业出版社华章分社编辑高婧雅的大力协助下，完成了该书。

本书的缺点是显而易见的。

一是因资料匮乏、技术变化快而难免出现技术错误。因此，本书的目的，主要是抛砖引玉，欢迎读者多提宝贵意见，争取在下一版本能纠正大部分的错误，不断完善、提升本书的质量。

二是缺少应用案例。其实目前网上的应用案例也有不少，但是我们认为，如果只是拿别人在网上的案例加工修改，从深度、广度方面都经不起推敲，起不了真正案例的作用。除非由真正落地该应用案例的主要负责人来写，才能使读者有真正的收获。受限于我们的人脉圈子和条件，目前只能请到PPKpub.org开源社区组织者陈晖先生来写一个区块链在标识注册方面的应用案例。在此鸣谢陈晖先生的大力支持，将来也欢迎有更多的区块链应用的领军团队提供应用案例，在未来更新的版本中补上在应用案例方面的短板。

本书特色

1）和目前市场上主流的区块链书籍强调区块链去中心化的概念，以及对业界带来的革命性影响不同，本书主要是从技术的角度，介绍区块链的基础概念，特别是对区块链的架构进行了详细的剖析。

2）对区块链的关键技术，包括区块链架构（1.0、2.0、3.0）、密码学和共识算法等做了一个详尽的介绍。

3）提供了比特币开发指南，通过以太坊智能合约开发来帮助初学者入门。本书也用专门一章来讨论区块链的常见问题，包括对近期发生的DAO攻击事件，都有详细的分析。

4）在区块链技术落地方面，本书也提供比较典型的区块链解决方案，包括支付和标识登记方面的解决方案。

5）以独特的架构演进对IT发展的影响为切入点，给读者展示一个全新观察整个IT历史的视角，并在这个视角下探讨区块链技术在未来IT发展中的影响和地位。

本书中一些实操的例子和章节，比较适合区块链初学者和程序员，可以成为区块链入门的书；架构剖析和深入分析方面的章节，比较适合IT架构师，以及区块链技术爱好者来深入了解区块链架构特点和技术细节，对设计区块链的解决方案有所帮助；解决方案和常见问题章节有助于区块链从业人员全面了解区块链应用落地方面的情况。最后一章是从架构视角对IT发展的一些观察，仅供喜爱思考的IT从业者参考。

读者对象

·区块链从业者

·IT架构师

·区块链应用开发人员

·对区块链技术感兴趣的人员

如何阅读本书

本书分为三大部分，共11章。

第一部分介绍基础和入门，包括以下2章内容。

第1章　本书的开篇，首先介绍区块链的定义和特点，并简单介绍了区块链的主要类型，然后通过介绍购买、存储和交易比特币等实际使用场景来让读者对区块链有所体验，然后再探讨一些关于区块链的常见问题。

第2章　介绍区块链的基础概念，为后面深入介绍区块链技术做铺垫。

第二部分介绍架构和核心技术，包括以下8章内容：

第3章　详细介绍区块链1.0、2.0、3.0典型架构，同时介绍了互联链的概念和架构。

第4章　详细介绍了区块链涉及的密码学原理和典型的算法。

第5章　介绍了在区块链架构中常用的共识算法。

第6章　提供比特币开发指南，通过实际案例来帮助初学者入门。

第7章　提供以太坊上的智能合约开发指南，帮助初学者掌握智能合约的开发要领。

第8章　详细介绍HyperLedger开源项目及其架构。

第9章　讨论区块链上常见的问题，包括最近出现的The DAO攻击的源码级分析。

第10章　讨论区块链上的典型解决方案，一个是以闪电网络为主的支付方案，另一个是以标识登记为主的开源ODIN解决方案。

第三部分为回顾和展望，即第11章，主要回顾IT架构演进历史并展望未来区块链对IT发展的影响。

勘误和支持

由于笔者的水平有限，编写时间仓促，书中难免会出现一些错误或者不准确的地方，恳请读者批评指正。如果你有更多的宝贵意见，欢迎通过微信或邮件进行讨论。你可以通过微信joezou3986、微博@云中君3986，或者发送邮件到邮箱joezou@openstack.org.cn联系到我，期待能够得到你们的真挚反馈，在技术之路上互勉共进。

致谢

首先感谢我的作者伙伴——张海宁先生、唐屹教授、李磊教授、刘天喜博士、陈晖先生、曲烈博士和郑晓明博士。他们在工作之余，挤出宝贵时间为本书贡献了他们对区块链技术的理解和洞察。特别感谢我的大学同门师弟Henry张海宁先生在关键时刻的出手相助，为本书贡献了很多精力，他不单在内容上积极供稿，也在本书的审定、修改和校正方面下了很多工夫。唐屹教授和李磊教授也在繁忙的教学和学术研究中抽出时间来对一些区块链的基本概念和关键技术（包括密码学和共识算法）做了详尽的阐述。刘天喜博士在本书的框架规划和开篇设计上做了很大贡献。而陈晖先生的比特币开发指南对很多初学者入门有很大的帮助，他的ODIN开源项目也是区块链登记方面的一个典型解决方案。曲烈博士的智能合约开发章节给众多以太坊开发初学者提供一个易懂、易上手的应用指引。郑晓明博士也对主流代币做了比较全面的介绍。

本书作者也得到中关村区块链联盟的大力支持，在此也特别鸣谢中关村区块链产业联盟秘书长王安平先生、副秘书长范金刚先生和林大鹏先生以及联盟发展部张培部长。同时也感谢江源老师、江苑绛博士，他们的鼓励成为我坚持下来的动力。另外在写书过程中也得到澳洲富士通区块链技术架构师董仲利先生、信达证券区块链首席专家曹寅先生、亚投行企业IT项目管理专家Allen邵以及合肥工业大学刘古刘和方辉先生的帮助，在此对他们表示感谢。

另外感谢比特币开源社区、以太坊开源社区，以及巴比特社区的各位技术专家们的博客文章，每次阅读必有所获，本书也多处引用了他们的观点和思想。

非常感谢机械工业出版社华章公司的编辑高婧雅，她的敬业精神和编辑效率令我由衷敬佩，她的反馈、建议、鼓励和帮助引导我们克服诸多困难完成全部书稿。

特别致谢

最后，因为工作和写书，牺牲了很多本该陪伴家人的时间。我要特别感谢我的母亲从小对我的培养，也要感谢我的哥哥姐姐们在儿时营造的和睦互助、求知好学的家庭环境，这对我长大以后形成对新兴技术浓厚的求知欲性格有很大影响，一直以来在我的职业生涯中都受益匪浅。更要感谢我太太Annie长期以来对我的默默支持，以及女儿Beverley，儿子Skyler对我工作的理解。

谨以此书献给我最亲爱的家人，多年以来帮助、支持我的师友们，以及众多热爱区块链技术的朋友们！

我想和作者聊聊

如果你想和本书作者沟通，可以通过以下方式。

1）【欢迎加入罗友书社，微信：15535237487，罗辑思维，得到APP，樊登读书会，喜马拉雅系列海量书籍与您分享】

2）

3）

4）

邹均