HZ BOOKS
华章IT

区块链4.0明星项目InterValue创始人兼CEO、CTO携核心团队成员撰写

系统讲解DAG技术的底层原理，深入剖析3大主流DAG区块链项目架构及实现原理

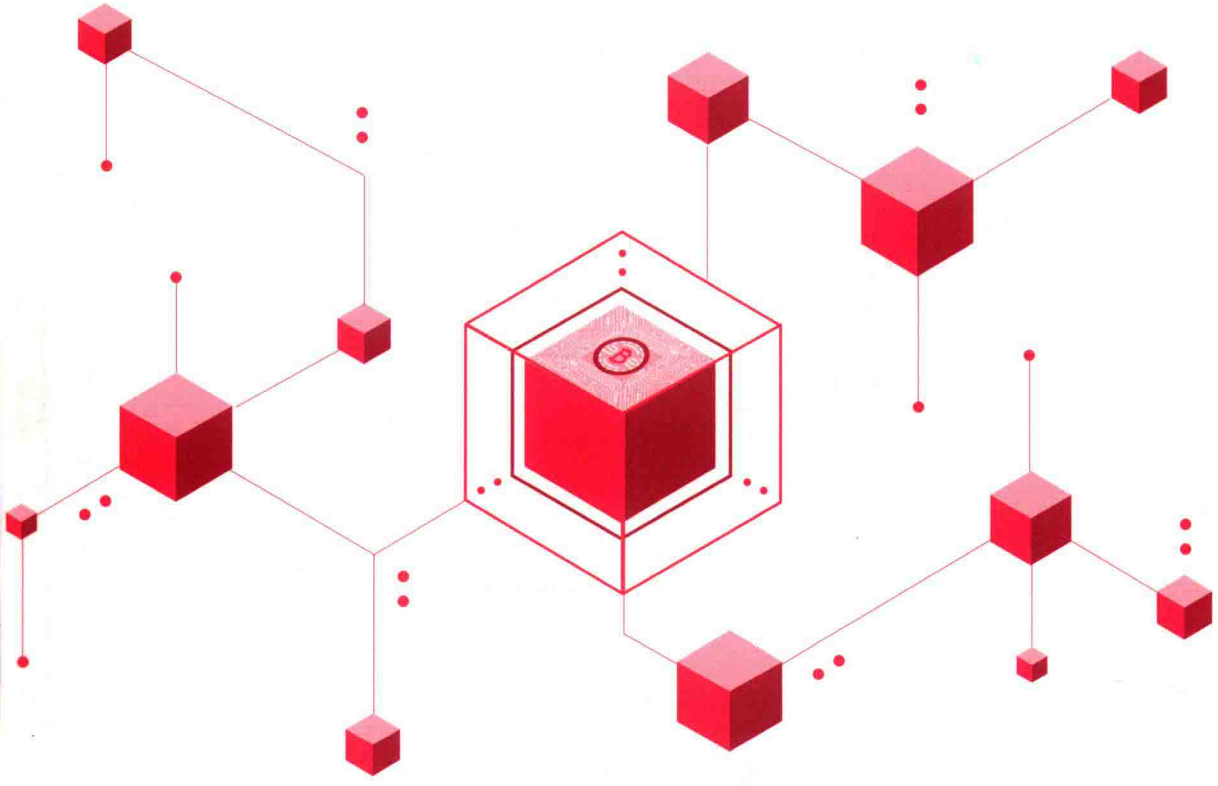
区块链技术丛书

BLOCKCHAIN TECHNOLOGY ON DAG Principle and Practice

DAG区块链技术

原理与实践

曹源 张翀 丁兆云 姜新文◎等著



非外借

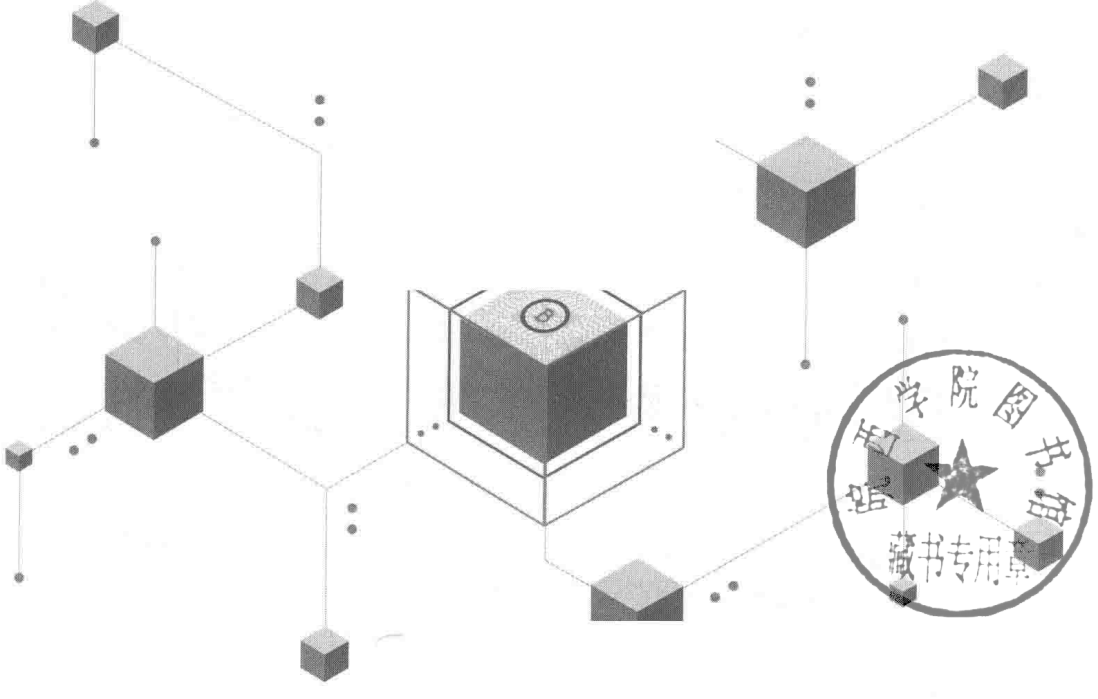
机械工业出版社
China Machine Press

区块链
技术丛书

BLOCKCHAIN TECHNOLOGY
ON DAG Principle and Practice

DAG区块链技术
原理与实践

曹源 张翀 丁兆云 姜新文◎等著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

DAG 区块链技术：原理与实践 / 曹源等著 . —北京：机械工业出版社，2018.10
（区块链技术丛书）

ISBN 978-7-111-61177-6

I. D… II. 曹… III. 电子商务 - 支付方式 - 研究 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 235228 号

DAG 区块链技术：原理与实践

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：张锡鹏 责任校对：殷 虹
印 刷：北京诚信伟业印刷有限公司 版 次：2018 年 11 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：18.25
书 号：ISBN 978-7-111-61177-6 定 价：79.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

Forword 序 一

“如果你没有理解我的意思，我没有时间说服你。”

——摘自中本聪语录

近年来，随着区块链这一波发展高潮的来临，业界发现除了与这个新生事物相关的法规及其监管问题突出之外，制约这项伟大发明落地应用推广的桎梏主要有两个方面：一是整个区块链（公链）系统并发运行效率很低，二是共识机制和智能合约甚至整个生态系统的友好性、可用性，特别是安全性能非常不到位。所以本书集中讲解了这两方面的原理与近来国内外对区块链的探索进展。本书是一本理论联系实际的好范本，非常适合涉猎面颇广的大专院校师生和社会上从事区块链相关工作或者对区块链感兴趣的各类读者深入阅读。

本书深入浅出，内容丰富，几乎涵盖了整个区块链相关的基本技术，尤为突出的是DAG在区块链领域的创造性应用。从基本区块链基础概念知识入手，本书比较详尽地介绍了DAG图论常识及其属性、特征以及数学定义，让非计算机和数学专业的读者也能读懂。接着，对DAG区块链的共识机制、DAG区块链的智能合约、DAG区块链中的密码学技术、DAG区块链安全问题，以及目前最有代表性的DAG区块链项目案例等几个方面进行了系统性阐述、分析和建设性展望。本书图文并茂，理实交融，既可用作培训区块链特别是基于DAG的区块链的讲义，又可用作自学教材。

全书主要围绕DAG区块链的共识机制和智能合约以及相关安全问题进行展开。为什么是DAG区块链呢？因为其可以解决当前区块链成块慢、缺乏并发处理机制，以至于无法满足大规模场景应用这个最基本的核心问题。相比图论中的一般图，DAG里的许多问题可以在多项式级甚至线性复杂条件下加以解决。以比特币和以太坊为代表的区块链，由于链式存储机构，导致出块无法并发执行。所以，具有代表性的DAG区块链项目，例如IOTA、Byteball、HashGraph及Intervalue等，都先后提出并采用了所谓“无区块（blockless）”概念。创造性地运用DAG数据结构，让每一笔交易直接参与维护全网的交易顺序。这样交易发起

后就可以跳过区块打包阶段，直接融入全网。这样连打包交易出块的时间都节省了，效率自然也提高了很多。也正是 DAG 没有“区块”的概念，由用户发出的数据单元前后链接构成，每个单元可以有多个父数据单元，因而在这种区块链上实现智能合约功能需要技术创新，充满挑战。因此，早期 DAG 区块链项目 IOTA 并没有支持智能合约，而知名的 Byteball 也仅支持非图灵完备的简单的声明式智能合约。在本书中介绍的最令人振奋的两个 DAG 区块链智能合约进展案例是美国的 Hedera Hashgraph 和中国的 InterValue。简单实用安全可靠，是智能合约成功与否的关键。

本书作者们主要是 DAG 区块链 InterValue 项目的技术领导和骨干人员。我作为这个项目的首席顾问，对整个项目团队执行力和集体的天赋充满信心。所以我在此很高兴地向读者推荐，在读懂本书有关区块链基本原理和 DAG 数据结构算法分析之后，建议重点围绕 InterValue 的 DAG 区块链章节，全面系统地理解 InterValue 项目的目标、愿景、生态体系、关键特征、技术和产品优势等，比如独创的共识机制、技术创新的智能合约设计、更为严密的安全功能的技术实现，以便步步深入并领略基于 DAG 区块链的最新进展和对其未来前景的美好期待与展望。

下面就简要介绍一下 InterValue 的主要特点和优势，抛砖引玉，希望对读者详尽阅读本书各章节有所帮助。

在重点讨论 DAG 区块链 InterValue 项目之前，我们需要特别关注一下目前美国最有代表性的 DAG 区块链项目——Hedera Hashgraph，因为有“标杆”比较，才能更好地鉴别与判断孰优孰劣。首先，从共识机制的技术实现方面看，目前已有的 Hashgraph 共识算法是通过 Gossip 网络和虚拟投票策略达到交易顺序共识的。但实现该共识的前提是网络节点超过 $2n/3$ 的投票能力具有对 famous witness 事件的一致投票结果。其中 n 是全网的当前投票能力的总和，该投票能力通常为节点的持股数量。虽然采用本地投票策略使得 Hashgraph 可以实现较快的交易确认，但此方法也带来了许多问题：由于全网投票能力波动大，可能导致系统长时间无法找到满足 $2n/3$ 投票一致的事件，从而无法达成共识；不同节点处理事件的能力差别较大，可能会造成系统长时间无法达成共识；由于采用 Gossip 邻居交换协议，节点会周期性剔除长时间未更新的邻居，此时若子网规模较小，很容易使恶意节点在同一轮产生两个 famous witness 事件，从而产生双花交易；随着系统规模变得越来越大，节点收到的同步信息也越来越多，以至于系统的吞吐率会随着节点数目的增加而降低。鉴于 Hashgraph 以上种种问题，InterValue 区块链项目提出了自己的共识机制——HashNet。这种共识采用基于双层 Gossip 拓扑的 Hashgraph。上层 Gossip 网络中的节点为全节点（full node），负责维护全网交易一致性。全节点通过 DPOS 的方式选举出来，全节点之间通过 Hashgraph 达成共识，这样有利于保持网络稳定性。每个全节点从下层网络中接收两类数据：下层网络内部节点的交易数据和跨子网交易数据。下层 Gossip 网络中的节点为局部全

节点（local full node），负责维护子网内部交易的一致性。与全节点不同，局部全节点的选举需要综合考量其 Token 数量、处理能力、带宽、在线时长等因素，局部全节点之间通过 Hashgraph 达成子网交易共识。这样 HashNet 共识有效地避免了 Hashgraph 共识中很多的问题与不足，可以说是“青出于蓝而胜于蓝”。并且，随着 InterValue 项目不断深入发展，基于 HashNet 的增强 DAG 共识和用于 witness（公证人）选择的 BF-VRF 共识机制相结合的双层共识机制将日臻完善，不断优化更新，以满足大规模化场景应用的需求。

另外，DAG 区块链 Byteball 及 Hashgraph 在智能合约及其安全性能方面，DAG 区块链通过了非图灵完备智能合约实现成功案例或者正在开发出实用性的图灵完备智能合约。但 Byteball 智能合约虽简单可用，却无法满足复杂应用场景需求。而图灵完备智能合约逻辑复杂，虽然支持应用范围广泛，但合约内容需要具备专业知识的程序员编写，难以满足广大普通用户的实际需要，并且智能合约出现安全漏洞的风险很高。因此，在 DAG 区块链上实现安全性能高的图灵完备智能合约是目前业界迫切期待的创新点。如果能将在 DAG 区块链上实现简练实用的非图灵完备智能合约和比较友好、安全、可用并且功能强大的图灵完备智能合约的共生同存统一于平台之中，将使得两类智能合约优势互补，特别有利于区块链平台上建构各类应用生态，从而极大地促进整个区块链行业的繁荣发展。作为区块链 4.0 的典型代表，InterValue 项目的智能合约正着力实现这两类智能合约于同一平台友好共存，本人力荐广大读者重点阅读本书有关 InterValue 的章节。除此之外，抗量子攻击级别加密算法技术、密码技术、新型智能合约语言等也十分值得一读，相信真正喜欢区块链或对区块链感兴趣的读者，一定会从本书中不断理解区块链特别是基于 DAG 区块链的魅力和其相应的“价值链接”——也就是项目名称 InterValue 所赋予的丰富内涵。

展望区块链发展趋势，公链平台如 InterValue 和 Byteball 等项目，将有机整合撒手锏大规模应用以及数字经济包括交易功能在内的 Token 经济共同体形成三位一体的社会经济体系，应该说这是区块链行业带动整个社会发展的大趋势。公链基础设施势必会不断创新和完善，保证大规模并发的处理能力，智能合约完备友好，整个公链体系安全可靠。区块链金融一定是真正点对点分布式的，交易所仅仅是典型公链的一个功能。而基于庞大区块链社区用户的 Token 经济共同体生态的核心应用场景，将是推动公链发展壮大的真正动力。期待 DAG 区块链能引领区块链时代创新发展滚滚向前的大潮，实现人类史上又一次生产力（公链技术）和生产关系（各类 Token 经济共同体生态的场景应用）变革与飞跃。

原阿里巴巴集团产品技术委员会主要负责人之一
Higgs Accelerator 创新创研加速器创始人、计算机科学家
Allen Wu（吴载午）
加州湾区硅谷

序　二 *Forword*

“区块链 +” 时代

我与曹博士

我的一个投资界的朋友很早就参与了区块链领域的投资。2017 年临近年底的一天，他给我特别介绍了 InterValue 和这个项目的创始人曹博士。这样我就很快与曹博士见了面。曹博士对 DAG 的深入研究以及 InterValue 在性能和安全方面取得的重大突破，给我留下了非常深刻的印象。

我的区块链创业

我一直是区块链的拥趸者。2015 年，我从京东 SVP 的职位上退下来，开始了我的区块链创业，创办了磁云科技。2016 年磁云科技成功孵化了唐泉金服项目。这是一个“区块链 + 金融”项目，该项目基于区块链技术，在商业银行间实现了基于智能合约的跨行调款。目前该系统已经在几百家商业银行中正式运行。

也正是在唐泉金服这个项目中，磁云成立了区块链研究院，立足于建立自主知识产权、国产、高性能的联盟区块链平台——磁云 M0。据权威机构测试，磁云 M0 的 TPS 超过 30 万。磁云 M0 之所以能取得这样的高性能，一个关键的突破是采用了分层 + 跨链共识。这也是 DAG 技术要突破的核心问题。

2018 年，磁云又将 M0 技术运用于应收账款等债权债务流转领域，以期推动中国供应链金融的深化，破局三角债难题和中小企业融资难、融资贵的问题，并取得重大突破。这就是磁云唐票的由来。磁云唐票已经在银行开展供应链金融、核心企业发展虚拟财务公司、开展自金融和产业集群供应链金融三个方面成功应用。对这个项目有兴趣的读者，可以到磁云官网进一步了解。

区块链的三个特性

我最关注的区块链特性有三个：

第一，区块链可以防篡改。通过数学加解密算法和博弈论的运用，区块链建立了一个防止数据被篡改的机制，它被称为可以“创造信任的机器”。

第二，Token。这个词当前争议比较大，一是这个词怎么翻译，二是没有 Token 的区块链是否还是区块链。我个人认为 Token 很重要。如果 Token 能够对应到现实世界的资产，那么它的可切分、可转让、可流通这三个特点可以创造前所未有的流动性。而流动性的本质是什么？是交易成本的下降和交易效率的提升。

第三，重构商业模式。区块链在存证、共享账本、智能合约、共享经济、数字资产这五个方面大有可为。可以说，你现在看到的所有互联网平台，都可以用区块链重新做一遍。

当前区块链的问题

业界普遍认为：当前区块链技术还不够成熟，特别是区块链的性能问题一直被诟病。我们知道的比特币系统只有个位数的 TPS，而以太坊也非常拥堵，据称 TPS 不超过 100。通常了解到的区块链，TPS 一般都不超过 10 000。这严重限制了区块链落地到现实的应用场景。

我在 2016 年就提出“去链结网”的思想。区块链最早是一种“链式”数据结构。凡是链，都会因为某个节点带来的延迟或被破坏，造成整个链出现严重问题。引申开来，在互联网时代，我们的链式思维也要变成“网”的思维，如供应链要变成“供应价值网”，产业链要变成“产业互联网”等。

对区块链的第一个改造就是“去链”。DAG 又被称为“有向无环图”，用“图”来替代原来的“链”，并在此基础上设计新的共识算法，成为当前提升区块链性能的重点突破方向。

我对 DAG 的认识

DAG 的核心思想是“分层分片”。这好比我们的财务记账，最底层是明细账，然后是汇总后的分类账，最后是总账。分层之后，对每一层又可以进行分片。这样共识就可以分为“片内共识”和“跨片共识”。把最早区块链的“串联”变成“并联”的存储结构和共识算法，大幅提升区块链的 TPS 性能指标，这就是 DAG 追求的主要目标。

DAG 数据结构没有“区块”的概念，其是由用户发出的数据单元前后链接构成，每个数据单元可以有多个父数据单元，因而在 DAG 区块链这种全新数据结构上实现智能合约功能是一个充满挑战和令人期待的事情。

有人说 DAG 特别适合物联网。事实上，DAG 的确为物联网应用发展在海量接入、海量存储以及高并发上提出了许多切实有效的解决方案。

本书对 DAG 应用的场景生态进行了深度分析和探索，如分布式社交、分歧合约、分布式文件存储、金融和泛金融领域等，几乎没看到边界。

科技引领的未来

这是一个伟大的时代。人工智能、物联网和区块链，分别对应生产力、生产资料和生产关系，这三种新技术对人类社会将产生深远的影响。当前中国正在进行的产业升级，本质上是产业 + 新科技、金融 + 新科技和产业 + 新金融三位一体的总体提升。我们要尤其关注区块链带给我们的新机会。

区块链要发挥效力，必须与实际应用场景相结合。与金融的结合、与产业的结合、与商业的结合，都是可以大放异彩的领域。未来的杀手级 DApp 一定会出现在这些领域中。

区块链是对大数据的一次重构。而且这次重构打破了大数据垄断，实现了用户主权和全社会大数据价值分享。

当前，一些基于 DAG 技术的区块链已经在 TPS 性能上取得了重大突破，如 InterValue 已经达到了百万级，这也为区块链真正杀手级应用的出现打开了一扇门。

磁云科技创始人
京东终身荣誉技术顾问
李大学
北京

Forword 序　三

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，区块链是一种将数据区块按时间顺序相连以组合成的块链式数据结构，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。区块链本身具备的分布式、去中心化、不可篡改和可编程特性，提供了不需要信任累积的信用建立范式，使得区块链技术成为全球关注的焦点。区块链技术被认为是继蒸汽机、电力、信息、互联网之后，第五种最有潜力引发生产关系颠覆性革命的技术。如果说，互联网带给我们的是信息自由传递，那么区块链将引领人类社会走进价值互联的全新时代。

如今的区块链技术已经发生了数次更新换代。

首先是区块链1.0——数字货币。2009年年初，比特币网络正式上线运行。作为一种虚拟货币系统，比特币的总量由网络共识协议限定，任何个人及机构都不能随意修改其中的供应量及交易记录。支撑比特币运行的区块链技术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。

紧接着是区块链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应用价值，并开始创建可共用的技术平台并向开发者提供BaaS（Blockchain as a Service）服务，从而极大地提高了交易速度，大大地降低了资源消耗。此时的区块链支持PoW、PoS和DPoS等多种共识算法。

再后来是区块链3.0——区块链应用延伸。由于块链式结构的固有缺陷，2015年后，以Byteball和IOTA等为代表的基于DAG数据结构的区块链技术兴起。区块链系统较之前更加高效，可扩展性以及互通性更强，并具有更好的用户体验。区块链应用也进一步延伸到医疗

健康、IP 版权、教育、物联网、共享经济、通信、社会管理、慈善公益、文化娱乐等更为广泛的领域。

再后来是区块链 4.0——完善生态体系。基于 HashNet 数据结构的区块链 4.0 技术逐步受到业界的关注。

然而，至今为止区块链技术距离大规模应用的要求还有较大差距，尤其是区块链底层技术还没有获得突破，还存在许多技术难题亟待攻克。目前开展的各类区块链场景应用很大程度上根基不稳，难以发挥实际作用，因此迫切需要开展区块链底层基础设施研究，从而为各类区块链应用提供可靠支撑，推动区块链技术在各个行业的应用落地。

在这种背景下，以提供价值互联网基础设施为目标的 InterValue 应运而生。该项目全面解决了现有区块链基础设施普遍存在的交易拥堵、交易费用高、交易确认迟缓、交易匿名保护、跨链通信和多链融合能力弱、存储空间耗费巨大，以及抗量子攻击能力差等问题，权威实测达到百万量级 TPS，达到世界顶尖水平，为区块链技术实用化和涌现现象级应用带来希望。

本书由 InterValue 核心团队成员在总结自己的实践和认识的基础上完成。本书围绕 DAG 区块链技术，从原理到实践展开。首先介绍了区块链基础以及 DAG 区块链入门知识；然后逐一介绍 DAG 区块链采用的共识机制、智能合约、密码学技术，逐个解析 DAG 区块链的成功案例，这些案例包括 IOTA、Byteball 和 InterValue；最后，对 DAG 区块链安全、DAG 区块链生态进行了讨论，对于 DAG 区块链的未来做了展望。

InterValue 项目基于 DAG 数据结构。由于本书全体作者的工作背景都是长期与区块链和数字货币研究实战相关，本书又是作者们自己在成功推出权威实测达到百万量级 TPS、达到全球顶尖水平的区块链基础设施的基础上，总结自己的实践写就的著作，所以一定能带给读者非同寻常的价值，可以为读者自己实战 DAG 引路护航。

国防科技大学计算机学院教授，湘潭大学信息工程学院教授

姜新文

Foreword 序　四

DAG 对于区块链公链的价值，值得每一个从业人员关注，无论我们是不是从事技术工作。今天我们都知道区块链技术如何伟大，对人类的影响会如何深远，但我们也都知道行业还处于什么阶段，许多看似美好的商业应用都是空中楼阁难以落地，主要的原因就是基于块链结构区块链底层公链的性能太差。而 DAG 这个方向的发展，给公链性能带来的改变不是优化，而是指数级别的变化和质的飞跃。关于这一点，本书从技术角度有清晰的论述。从本书中介绍的公链核心性能和特点的对比中，我们非技术的从业者可以更好地理解区块链底层技术发展的趋势。中本聪的比特币改变世界从技术白皮书开始，从块链结构到 DAG，本书虽然着重讲技术，但我相信它的影响力会大大超出技术领域。

曹博士其人在我眼中，四个字形容他最为贴切——静水流深。他为人不事张扬，态度柔和，胸中实有万千丘壑，却宁静而优雅，洞悉区块链领域各种前沿技术，坚持价值观不被欲望绑架，拥有真正的自由和快乐。在当今浮躁的行业中，他是难得的一股清流，我相信这样的人可以成为，也应该成为这个行业的脊梁。也希望这样的人写的这样的一本书，可以帮助一批又一批的技术人才更快成长。只有这样，区块链这个行业才会迎来真正的繁荣。

起源资本创始人

冉立之

前　言 Preface

为什么要写这本书

十余年前，攻读硕士期间在做 P2P 应用系统时，分布式的内容分发和文件共享均相对较容易实现，但却一直为 P2P 节点的信誉机制和信任体系的建立绞尽脑汁而不可得。博士阶段研究方向转为网络安全，在寻找研究方向时，因长期以来对网络对抗、密码学的研究有兴趣，机缘巧合，在 2008 年年底恰逢中本聪、哈尔芬尼等人在密码学邮件组讨论比特币设计并在讨论组里发布了比特币的原始论文，自此，开始了我的区块链研究生涯。

区块链行业近年来发展迅速，作为行业较早的从业者，我一直和行业一起成长，并实际参与了区块链行业，进行了诸多工程实践。人们基于块链式结构的分布式账本技术设计了很好的经济模型，解决了分布式环境下达成一致性之后的节点激励问题，但现有块链式结构的设计因需要将单笔交易的全部阶段作为原子操作来完成，所以先天性难以并行出块，存在难以提高系统吞吐量等问题。人们在如何提高块链式分布式账本的 TPS 上做了很多工作，典型的如闪电网络等，但由于块链式数据结构本身的限制，始终难以实现彻底的性能提升。

在数学和计算机科学的诸多领域，图（网）这种数据结构在解决诸多复杂应用问题时相较于链表结构具备先天性的优势，这在诸多科学问题和实际应用领域中已经得到证明。在区块链或者说分布式账本技术领域，我认为该规律依然适用。2013 年，在 bitcointalk.org 论坛上关于 NXT 的讨论帖中，就有用户提出以有向无环图（Directed Acyclic Graph，DAG）作为区块链的底层数据结构以提高系统整体性能，此时提出的 DAG 底层依然用区块，但把区块的链式存储结构改成 DAG 存储，即变成区块 DAG。此时人们的思路还停留在侧链的思路上，不同类型的交易并行在不同链上进行，即 DAG 和区块结合使用。但 DAG 区块仍受限于出块速度这个指标，因此 2015 年人们提出 Blockless DAG 的概念，

此时的DAG把区块和交易进行了融合，交易发起后没有产生区块的阶段，而是直接对交易进行全网交易排序。后续人们逐渐在DAG技术路线上进行了探索，出现了IOTA、ByteBall、XDAG、Hedra Hashgraph、InterValue等项目，DAG几乎在每个维度上都能显露出比区块链更优的特性，在效率、确定性、避免中心化、能耗等方面尤为明显，但如何设计安全、高效的基于DAG的共识机制以实现对交易全网排序并确保排序的唯一性和一致性是个技术难点。上述项目在DAG共识机制上做了迭代性的探索，尤其是InterValue项目在共识机制设计上，创新性地提出的分层分片的Gossip共识机制HashNet。HashNet有望较好地平衡“不可能三角”，即平衡区块链基础设施的去中心化、性能和安全性。

由于区块链行业尚处于早期阶段，尤其是在技术方向的探索上，诸多项目依然在进行块链式区块链的研究，行业内尚未在能支持大规模分布式应用（DApp）的区块链基础设施应该走什么样的技术路径这个问题上达成共识，基于我对DAG技术的理解和应用实践，我认为非常有必要撰写一本关于DAG技术原理与工程实践的图书：首先让区块链爱好者对DAG这条技术路径的发展历程、现状和趋势有深度了解；其次让区块链从业者在从事区块链相关研究和开发过程中掌握DAG的技术原理并能够将该技术用于工程实践；最后希望能够将各类区块链行业大规模应用和基础设施研发团队的技术路径引到DAG技术路径上来，通过各团队的努力，在实用化区块链基础设施研发和基于实用化区块链基础设施构建的用户量级达到千万级以上的分布式应用研发上，尽早取得里程碑式的成果，实现现象级区块链基础设施和现象级区块链应用的落地。

读者对象

- 区块链技术爱好者
- DAG相关项目的用户
- DAG技术爱好者
- DAG项目实际开发者
- DAG相关应用开发者
- 开设区块链相关课程的大专院校的学生

如何阅读本书

本书可归纳为三大部分。

第一部分为基础原理（第 1 章～第 5 章），依次对 DAG 技术原理，包括数据结构、共识机制、智能合约、密码学技术进行了介绍，帮助读者掌握 DAG 的原理性知识。

第二部分为工程实践（第 6 章～第 9 章），着重讲解 DAG 技术工程实践中的三个具有代表性的项目，即 IOTA、ByteBall 和 InterValue，尤其是对 InterValue 项目进行了详细介绍，并对 DAG 技术安全原理和实践进行了探讨。

第三部分为展望（第 10 章～第 11 章），对 DAG 的生态建设和发展趋势进行了探讨。

希望本书能够为读者提供原理性指导和工程实践参考。

勘误和支持

除封面署名的作者外，参加本书编写工作的还有张晓斌、康来、荀长庆、何速、龙军、张子文、刘晓铖、徐浩、彭磊、左晓亮、刘星、邢志、陈政、张硕云、甘卫、文冉、邓长青等。由于作者的水平有限，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。书中的全部源文件可以从华章网站[⊖]下载，我会将相应的功能更新并及时发布出来。如果你有更多的宝贵意见，也欢迎发送邮件至邮箱 caoyuan@nudt.edu.cn，期待能够得到你们的真挚反馈。

致谢

感谢比特币之父中本聪，他开创了一款影响我整个人生的软件。

感谢国防科技大学十数年的教育，我在这里度过了学生生涯并留校任教数年，让我有幸在我感兴趣的技术领域开展研究。

感谢公司的所有小伙伴——邵炳春、郭乐、钟磊、向妍、杨祝建、陈丽沙、李海平、于存威、张文政、叶永学、彭韬、刘轶、张超、杜玺麟、施雨良、丁继刚、郭芳琪、高迪、胡慧、阳昕丽、黄召戎、文德英、克雷蒙、康纯、张静、李爱军、贺文军、余增辉、李旭、刘欣如、熊季、彭毓妍、曹恒、邱颖、彭飞、李进、杨坚、张航、李帅、张小苗、代祥、金多多、万舸、徐斯洁、肖春宇，以及名单之外的更多朋友，感谢你们长期对公司的支持和贡献。

感谢机械工业出版社华章公司的杨福川老师，在这半年多的时间中始终支持我的写作，你的鼓励和帮助引导我能顺利完成全部书稿。

⊖ 参见华章网站 www.hzbook.com——编辑注。

最后感谢我的父母及亲人，感谢你们将我培养成人，并时时刻刻为我灌输着信心和力量！

谨以此书献给我最亲爱的家人，以及众多热爱区块链尤其是 DAG 技术的朋友们！

湖南宸瀚信息科技有限公司董事长
哈希奈特（北京）科技股份有限公司董事长
四川宸瀚科技有限公司董事长
曹源
写于湖南长沙

目　录 Contents