2018

区块链

基础理论与研究概况

AMiner 研究报告第三期

清华大学计算机系－中国工程科技知识中心

知识智能联合研究中心（K&I）

2018 年 4 月

目录

1 概述篇.....2

1.1 区块链产生背景.....3

■ 1.1.1 政治法律.....3

■ 1.1.2 经济.....3

■ 1.1.3 社会.....4

■ 1.1.4 科技.....4

1.2 编写方法与全文结构.....4

1.3 术语和缩略语.....5

2 区块链简介.....7

2.1 区块链概念.....8

2.2 区块链发展阶段.....8

■ 2.2.1 区块链 1.0：数字货币.....9

■ 2.2.2 区块链 2.0：智能合约.....10

2.3 区块链特征.....11

3 技术人才篇.....13

3.1 密码学.....14

■ 3.1.1 公钥密码体制.....14

■ 3.1.2 哈希算法.....16

■ 3.1.3 密码学国际研究现状.....18

■ 3.1.4 密码学代表学者.....19

3.2 共识协议.....31

■ 3.2.1 共识机制.....33

■ 3.2.2 共识机制代表学者.....35

3.3 博弈论.....42

■ 3.3.1 博弈论概述.....42

■ 3.3.2 博弈论代表学者.....44

3.4 性能提升办法.....50

■ 3.4.1 Thunder.....50

■ 3.4.2 Celer Network.....50

■ 3.4.3 Lightning Network.....51

■ 3.4.4 Algorand.....51

■ 3.4.5 SPECTRE & PHANTOM.....52

4 应用趋势篇.....54

AMiner

4.1 数字货币.....55
■ 4.1.1 数字货币概述.....55
■ 4.1.2 数字货币分类.....56
■ 4.1.3 最新研究现状.....60
■ 4.1.4 数字货币优点和风险.....66
4.2 区块链其他应用场景.....68
■ 4.2.1 金融服务.....69
■ 4.2.2 智能制造.....70
■ 4.2.3 供应链管理.....70
■ 4.2.4 文化娱乐.....70
■ 4.2.5 社会公益.....71
■ 4.2.6 政府管理.....71
4.3 区块链发展现存障碍.....72
4.4 挑战与未来.....74

AMiner

图表目录

表 1 术语.....5
表 2 缩略语.....6
表 3 区块链的类型及特性.....8
表 4 加解密算法类型.....15
表 5 典型散列算法特点.....17
表 6 共识机制分类.....31
表 7 共识机制及技术水平.....33
表 8 共识机制评价维度.....34

图 1 区块链 1.0 技术架构.....10
图 2 区块链 2.0 技术架构.....11
图 3 密码体制的基本模型.....14
图 4 对称密码体制加密流程.....15
图 5 公钥加密流程.....15
图 6 密码学研究全局热点.....18
图 7 基于点对点网络的 Sybil Attack 原理.....33
图 8 比特币全球学者分布.....61

AMiner

扫码订阅

摘要

全球新一轮产业变革和科技革命持续深入，信息技术引领世界技术竞争新高地。区块链作为密码学、分布式系统、共识机制、博弈论的集大成者，推动多领域学术研究的蓬勃发展，也为相关产业提供诸多机遇。为了总结区块链基础理论研究及概况，我们编写了此份研究报告。其主要内容包括：

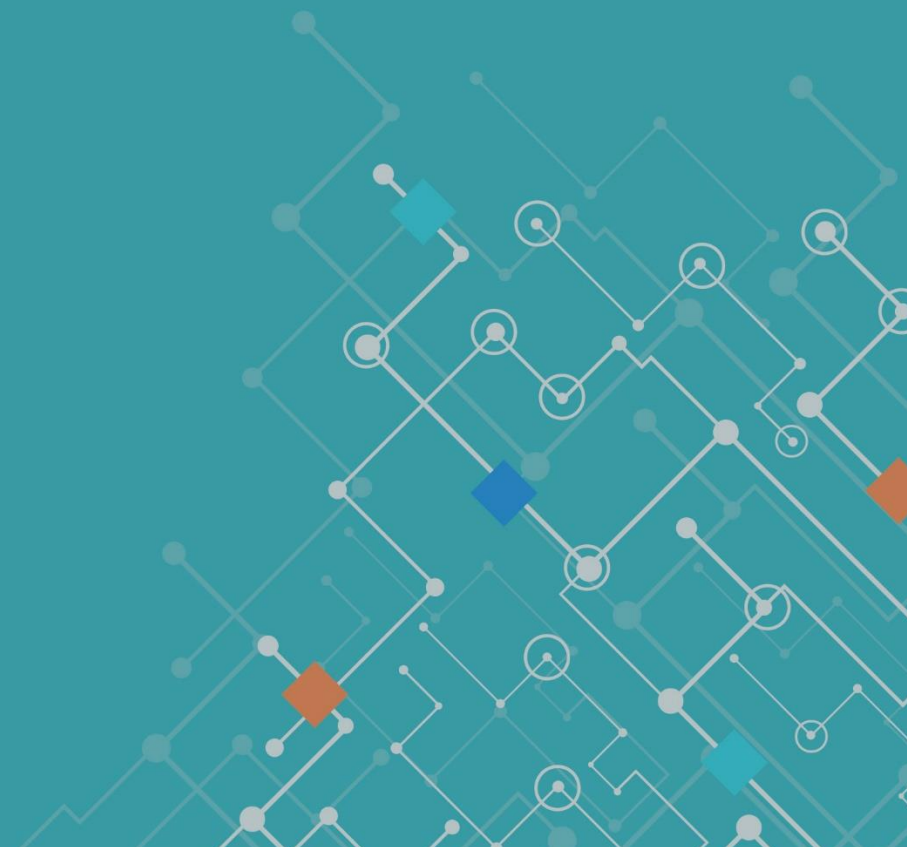
一、区块链基本概念梳理和国内外区块链发展现状分析。首先从政治、经济、社会文化、科学技术 4 个角度整理了区块链技术产生背景，简要概括区块链基本概念和相关术语，分别探讨区块链 1.0 数字货币阶段和区块链 2.0 智能合约阶段的技术架构，总结出区块链技术 6 大特征，并指出区块链技术的理论意义及现实意义。

二、区块链基础理论国内外研究现状分析。通过 AMiner 系统提供的大数据信息，分别整理密码学、分布式系统和博弈论领域的国内外专家学者、研究机构、代表论文、研究热点及热点变化趋势、中外研究情况对比情况，对区块链基础理论研究现状进行全面梳理。

三、区块链典型应用场景及典型应用分析。以比特币为主分析区块链在实际场景中的应用，分别指出区块链在比特币系统中发挥的作用、比特币研究现状和现存问题。此外，本研究还列举了区块链在金融服务、智能制造、供应链管理、文化娱乐、社会公益、政府管理 6 大方面的相对成熟、应用前景广阔或具有潜在应用价值的应用场景，并对区块链应用价值进行展望。

最后，基于对区块链研究现状的分析和研判，围绕区块链下一步理论研究和应用落地方面提出相关建议。

概述 1
concept 1



1.1 区块链产生背景

■ 1.1.1 政治法律

随着区块链逐步应用于金融、供应链、工业制造、公益等领域，各国政府及监管机构在区块链的发展与落地中发挥重要作用。目前，各国政府对与以比特币为代表的数字货币政策褒贬不一，但对于区块链技术，各国政府普遍采取积极支持的态度。2016 年 1 月 19 日，英国政府发布《分布式账本技术：超越区块链》白皮书，积极探索区块链未来在减少金融诈骗、降低交易成本的潜力；2016 年 6 月，新加坡金融管理局推出“沙盒计划”（Sandbox），在可控范围内允许金融科技公司的发展；2017 年 4 月 1 日，日本正式实施《支付服务法案》，承认比特币的合法地位；美国各州政府也采取措施学习与探索区块链技术，并尝试通过区块链提高政府工作的透明度和效率。中国政府同样对区块链技术给予了高度关注。自 2016 年 10 月工业和信息化部发布《中国区块链技术和应用发展白皮书（2016）》及 2016 年 12 月区块链首次被作为战略性前沿技术写入国务院发布的《国务院关于印发“十三五”国家信息化规划的通知》以来，各地政府纷纷出台有关区块链的政策指导意见及通知文件。中国互联网金融协会也成立区块链研究工作组，深入研究区块链技术在金融领域的应用及影响。2017 年 5 月，中国电子技术标准化研究院联合数十家单位发布《中国区块链技术和产业发展论坛标准 CBD-Forum-001-2017》，为区块链落地产业设定标准。

■ 1.1.2 经济

国内外互联网、IT 等领域的大量企业开始涉足区块链行业，着手研发或推出从基础设施到应用案例的一系列解决方案。全球主流金融机构布局区块链，2015 年 10 月，美国纳斯达克推出基于区块链技术的证券交易平台 Linq，进行金融证券市场去中心化的尝试。高盛、摩根大通、瑞银集团等银行业巨头分别各自成立各自的区块链实验室、发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司。此外，区块链初创公司及各类投资机构也纷纷涉足区块链领域，为区块链技术落地提供资金支持。初创公司 Ripple Labs 致力于推动 Ripple 成为世界范围内各大银行通用的标准交易协议，使货币转账能像发电子邮件那样成本低廉、方便快捷；R3CEV 推出的 BaaS（Blockchain as a Service）服务，已与美国银行、花旗银行、招商银行等全球 40 余家大型银行机构签署区块链合作项目，致力于制定银行业的区块链行业标准与协议。从 2016 年开始，招商银行、民生银行等传统金融机构和蚂蚁金服、京东金融、百度金融等金融科技企业先后涉足区块链金融场景应用，众安科技、人寿保险、阳光保险等保险机构也纷纷展开区块链概念证明实验。

1.1.3 社会

随着区块链技术的发展，其在各行业的应用潜力开始受到社会关注。联合国、国际货币基金组织，以及美国、英国、日本等国家都对区块链的发展给予高度关注。同时，国内外先后成立各种类型的区块链产业联盟，协调推进区块链技术和应用发展。R3 区块链联盟于 2015 年 9 月成立，致力于为银行提供探索区块链技术的渠道和区块链概念产品。同年，Linux 基金会成立超级账本（Hyperledger），推进区块链数字技术和交易验证开源项目。中国先后成立中关村区块链产业联盟、中国分布式总账基础协议联盟（China Ledger）、金融区块链合作联盟（金链盟）和区块链微金融产业联盟（微链盟），积极探索推动区块链的应用。

1.1.4 科技

点对点传输、共识机制、加密算法、博弈论等基础技术及理论的发展与完善，为区块链技术取得进展奠定坚实的基础。国内外学者与科研机构对区块链领域的研究成果不断涌现，进一步助力区块链技术的完善与进化。日本经济贸易产业省《区块链技术及相关服务的调查报告（2015）》（Survey on Blockchain Technologies and Related Services FY2015 Report）、英国政府《分布式账本技术：超越区块链》（Distributed Ledger Technology: Beyond Blockchain）、中国工业和信息化部《中国区块链技术和应用发展白皮书（2016）》及京东金融研究院与工信部下属中国信通院云计算和大数据所共同发布的《区块链金融应用白皮书》，均对区块链及技术发展最新动向进行跟踪总结。

1.2 编写方法与全文结构

一是收集国内外区块链最新研究成果和总结报告。本研究收集了主要国家政府和国际政府间组织发布的区块链报告和白皮书，如联合国《数字货币和区块链技术在构建社会团结金融中如何扮演角色》（How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?）、工信部《中国区块链技术和应用发展白皮书（2016）》、KPMG 区块链研究报告《共识—价值互联的不变协议》、iiMedia Research《2017-2018 中国区块链热点专题研究报告》等，从政府、学术研究以及行业发展等角度全面把握区块链技术的发展动向。

二是利用 AMiner 平台整理区块链基础技术国内外研究状况。重点分析了密码学、分布式系统、共识机制、博弈论领域当前世界学者分布、代表学者、学者关系、研究成果、研究趋势和中外研究概况对比，以丰富的图文数据展示区块链基础理论在全球范围内的发展状况

和未来的研究潜力。

三是分析区块链应用的典型案例。通过对比特币、以太坊和传统金融机构的区块链应用案例进行分析，了解区块链采用的底层基础设施、应用架构和应用价值，展现区块链与现实场景结合状况与现存问题，为区块链理论与实践的进一步发展提出展望。

1.3 术语和缩略语

本报告涉及的术语如表 1 所示。

表 1　术语

术语	定义/解释
区块链	在分布式账本中排序及验证交易的方式，是数据存储、点对点传输、共识机制、加密算法等计算机技术的集成应用。
密码学	研究编制密码和破译密码的技术科学。
分布式账本	一个可以在多个站点，不同地理位置或者多个机构组成的网络中分享的资产数据库。其中，资产可以是货币以及法律定义的、实体的或是电子的资产。
共识机制	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。在区块链各个节点之间达到一致的分布式算法
博弈论	博弈论是现代数学的新分支，也是运筹学的重要学科，研究公式化了的激励结构间的相互作用，是研究具有斗争或竞争性质现象的数学理论和方法。
智能合约	一种用计算机语言取代法律语言记录条款的计算机程序。
数字货币	货币的数字化，通过数据交易并发挥交易媒介、记账单位及价值存储的功能。

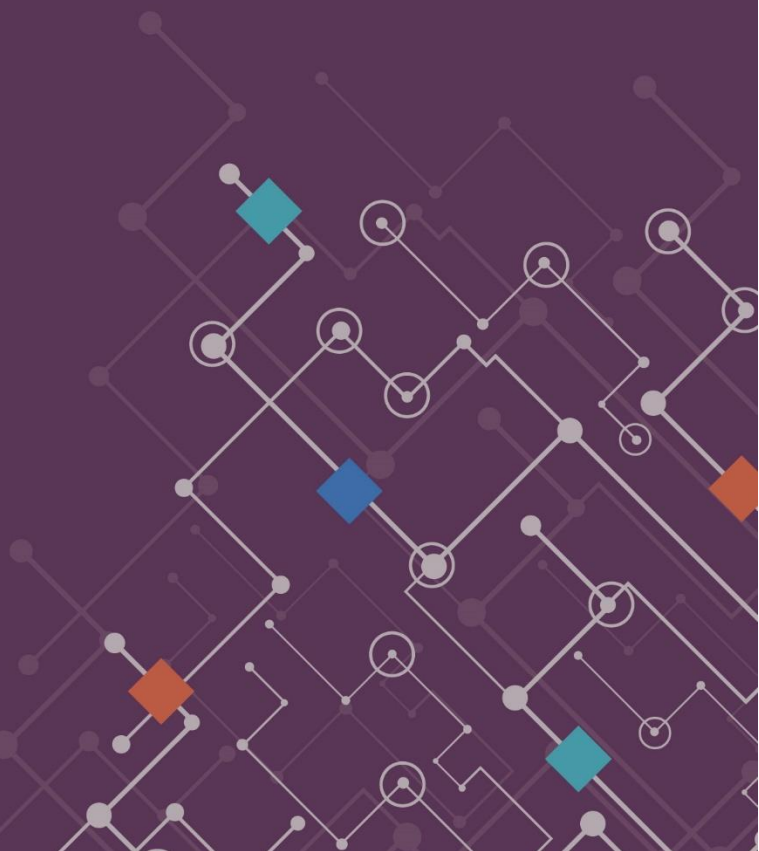
本报告涉及的缩略语如表 2 所示。

表 2　缩略语

缩略语	原始术语
PoW	工作量证明（Proof of Work）
PoS	股权证明（Proof of Stake）
DPoS	股权授权证明（Delegate Proof of Stake）
PBFT	实用拜占庭容错（Practical Byzantine Fault Tolerance）
P2P	点对点（Peer to Peer）
DAPP	分布式应用（Decentralized Application）
RSA	RSA 加密算法（RSA Algorithm）
ECC	椭圆加密算法（Elliptic Curve Cryptography）
KYC	客户识别（Know Your Customer）
AML	反洗钱（Anti Money Laundering）

区块链简介 2

block chain



2.1 区块链概念

区块链本质上是一个去中心化的分布式账本数据库，目的是为了解决交易信任问题。广义来看，区块链技术是利用块链式数据结构验证与存储数据、利用分布式节点共识算法生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用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。狭义来看，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。

区块链技术的最大优势与努力方向是“去中心化”，通过运用密码学、共识机制、博弈论等技术与方法，在网络节点无需相互信任的分布式系统中实现基于去中心化信用的点对点交易。因此，区块链成为以比特币为代表的数字货币体系的核心底层技术。

区块链可分为三类：公有链（Public Blockchain）、联盟链（Consortium Blockchain）、私有链（Private Blockchain）。

表 3　区块链的类型及特性

类型	特性
公有链	世界上任何个体或团体都能发送交易，且交易能获得该区块链的有效确认 任何人均可参与其共识过程。 最早出现、目前应用最广泛的区块链。 现阶段每秒 3—20 次数据写入。
联盟链	某个群体内部指定多个记账节点，每个区块的生成由所有预选节点共同决定。 预选节点参与共识过程，其他接入节点可以参与交易，但不过问记账过程，可满足监管 AML（Anti Money Laundering,反洗钱）/KYC（Know Your Customer,客户识别）。 现阶段每秒 1000 次以上数据写入。
私有链	仅使用区块链总账技术进行记账，某一组织或个人独享写入权限 改善可审计性，不完全解决信任问题。

2.2 区块链发展阶段

2008 年，名为“中本聪”（Satoshi Nakamoto）的学者或组织发表论文《比特币：一种点对点电子现金系统》，这一事件被认为是区块链技术的起源。随着比特币等数字货币的日益

普及，区块链技术的发展引起了政府部门、金融机构、初创企业和研究机构的广泛关注。区块链的研究成果与应用成果呈现几何级数增长的态势，与大数据、物联网、智能制造等场景紧密结合，依托现有技术进行独创性组合创新。

梳理区块链技术发展脉络，区块链演进经历了两个阶段：区块链 1.0，即以可编程数字加密货币体系为主要特征的区块链模式；区块链 2.0，即以可编程金融系统为主要特征的区块链模式。当前，区块链发展已经进入区块链 2.0 模式。但是，区块链模式是平行发展而非质变式演进的，区块链 1.0 模式与 2.0 模式目前同时存在于人类社会，且以数字加密货币为应用代表的 1.0 模式仍在探索之中。区块链的不同发展阶段呈现出相互影响、相互补充的互动态势。

■ 2.2.1 区块链 1.0：数字货币

区块链是利用密码学方法相关联产生的数据块，用于验证信息有效性或防伪，并生成下一个区块。在区块链 1.0 阶段，以比特币为代表的数字货币和支付行为是最典型的应用。继 2008 年中本聪提出比特币设想后，2009 年比特币正式上线运行。随着比特币在世界范围内的普及，人们开始意识到作为比特币底层技术的区块链具有去中心化的优良性质。区块链采用纯数学方法而不是中心机构建立信任关系，使得互不信任或弱信任的参与者之间能够维系不可篡改的账本记录。

具体而言，区块链 1.0 具有如下功能：

- **分布式账本（Distributed Ledger）**：分布式账本是在网络成员之间共享、复制和同步的数据库，记录网络参与者之间的交易，部分国家的银行将分布式账本作为一项节约成本的措施和降低操作风险的方法。
- **块链式数据（Linked Data Storage）**：区块链采用带有时间戳的链式区块结构存储数据，从而为数据增加了时间维度，具有极强的可验证性和可追溯性。
- **梅克尔树（Merkle Trees）**：梅克尔树是区块链的重要数据结构，能够快速归纳和校验区块数据的存在性和完整性。
- **工作量证明（Proof of Work, PoW）**：通过引入分布式节点的算力竞争保证数据一致性和共识的安全性。

图 1　区块链 1.0 技术架构[1]

2.2.2 区块链 2.0：智能合约

区块链 2.0 进入可编程金融阶段。在这一阶段，区块链系统渗入经济、金融与资本市场，形成股票、债券、期货、贷款、抵押、产权、智能财产的智能合约。除了构建货币体系之外，区块链在泛金融领域也有众多应用案例。例如，智能合约的核心是利用程序算法替代人执行合同，这些合约包含三个基本要素：要约、承诺、价值交换，可以实现资产、过程、系统的自动化组合与相互协调。

区块链 2.0 具有如下功能：

- **智能合约（Smart Contract）**：1994 年，Nick Szabo[2]首次提出智能合约概念，即一种旨在以信息化方式传播、验证或执行合同的计算机协议，能够在没有第三方的情况下进行可信交易。智能合约是已编码的、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。
- **虚拟机（Virtual Machine）**：指通过软件模拟的运行在一个完全隔离环境中的完整计算机系统，在区块链技术中，虚拟机用于执行智能合约编译后的代码。
- **去中心化应用（Decentralized Application, DApp）**：去中心化应用是运行在分布式网络上、参与者的信息被安全保护（也可能是匿名的）、通过网络节点进行去中心化操作的应用。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（Ethereum）的去中心化区块链及其原生数字货币以太币（Ether）。

[1] 内容来源：《中国区块链技术和应用发展白皮书（2016）》

[2] Szabo N. Smart contracts[J]. Unpublished manuscript, 1994.

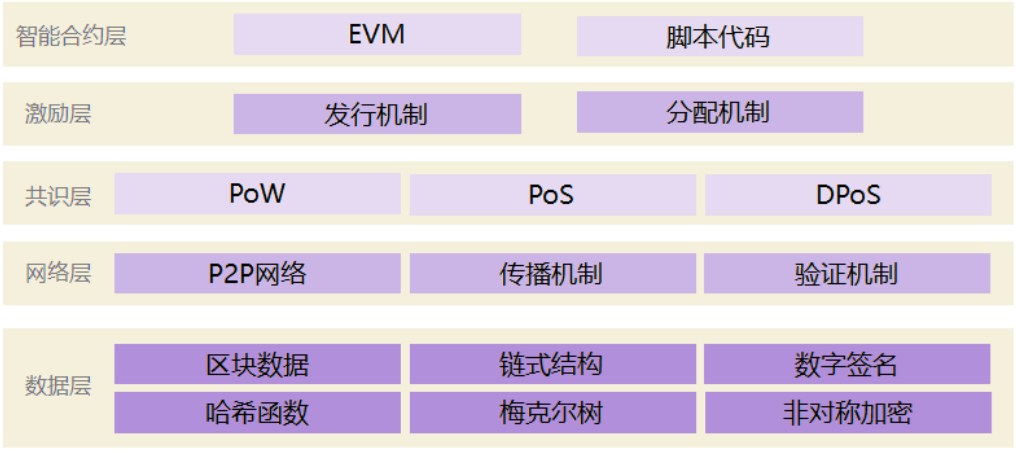


图 2　区块链 2.0 技术架构[3]

2.3 区块链特征

区块链共有五大特征：去中心化、开放性、自治性、信息不可篡改和匿名性。其中，去中心化是指区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。开放性是指区块链的所有数据信息也是公开的，每一笔交易都会通过广播的方式，让所有节点可见。安全可靠是指单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制超过 51%的节点同时修改。自治性是指任何人都可以参与到区块链网络，每个节点都能获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。

- **去中心化**：区块链数据的验证、记账、存储、维护和传输都不是基于中心机构，而是利用数学算法实现。去中心化使网络中的各节点之间能够自由连接，进行数据、资产、信息等的交换。
- **开放性**：区块链具有源代码开源性，即网络中设定的共识机制、规则都可以通过一致的、开源的源代码进行验证。任何人都可以加入（公开链），或者通过受控方式加入（联盟链）。
- **自治性**：区块链技术采用基于协商一致的规范和协议，使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，任何人为的干预不起作用。
- **信息不可篡改**：区块链使用了密码学技术中的哈希函数、非对称加密机制保证区块链上的信息不被篡改。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

[3] 内容来源：《中国区块链技术和应用发展白皮书（2016）》

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。

- **匿名性**：由于节点之间的交换遵循固定的算法，其数据交互是无需信任的，区块链中的程序规则会自行判断活动是否有效，因此，交易对手无须通过公开身份的方式让对方自己产生信任。

核心技术及研究现状

core technology

3

3.1 密码学

早在人类文明初期，密码学就已经开始发展。早期密码学将通俗易懂的明文转换成为普通听众无法理解的密文，并设计特殊规则让合法听众将密文还原为明文。早期简单密码的设计体现在实现方式上，即通过替换、换位方式进行密码变化，如古罗马 Caeser 密码、法国 Vigenere 密码。伴随着信息通信即计算机技术的飞跃式进步，密码学在实现效率和实现方式上均实现了前所未有的系统发展。1949 年，Shannon 发表“保密系统的通信理论”[4]，奠定密码学数学基础。1973 年，IBM 开发 Feistel 分组密码结构[5]，其物理上的对称性和反复性极大降低了对硬件实施中编码量和线路传输的要求，奠定了数据加密标准（Data Encryption Standard, DES）的结构基础。1976 年，Diffie 和 Hellman 提出“密码学新方向”[6]，打破 DES 加密安全性对密钥保密的依赖，开辟公钥密码理论，为密钥协商、数字签名技术提供新解法。当前，中国国家密码局认定的国产商用密码算法包括 SM1、SM2、SM3 及 SM4。其中，SM1 为对称加密算法，SM2 为非对称加密算法，SM3 为哈希算法，SM4 是在国内广泛使用的 WAPI 无线网络标准中使用的加密算法。四种国密算法满足多种密码应用的安全需求，为建设行业网络安全环境提供技术基础。目前，密码学广泛应用于网络信息加解密、身份认证、数字签名，以及关于完整性、安全电子交易（Security Electronic Transaction, SET）等的安全通信标准和网络协议安全性标准中。

■ 3.1.1 公钥密码体制

密码体制分为对称密码体制和非对称密码体制。

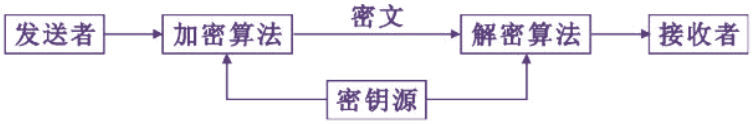


图 3　密码体制的基本模型

消息发送者从密钥源得到密钥，通过加密算法对消息进行加密得到密文；接收者收到密文后，利用从密钥源得到的密钥，通过解密算法对密文进行解密，得到原始消息。

在对称密码体制中，解密算法是加密算法的逆算法。也就是说，加解密过程使用的密钥

[4] Shannon C E. Communication theory of secrecy systems[J]. Bell Labs Technical Journal, 1949, 28(4): 656-715.

[5] Meyer C H. Design considerations for cryptography[C]//Proceedings of the June 4-8, 1973, national computer conference and exposition. ACM, 1973: 603-606.

[6] Diffie W, Hellman M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644-654.

具有唯一性，解密方必须事先知道加密密钥。这使得对称加密体制具有算法公开、加密速度快、加密效率高的优势。另外，随着加密用户增加，密钥数量呈几何级数增长，密钥管理成本高，对称密码体制在分布式网络的应用受到阻碍。目前，广泛应用的对称密码体制有 DES、3DES、国际数据加密算法（International Data Encryption Algorithm, IDEA）、高级数据加密标准（Advanced Encryption Standard, AES）和国内的 SM1、SM4 等。

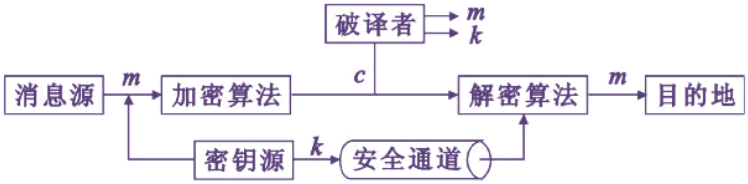


图 4　对称密码体制加密流程

在非对称密码体制中，公钥和私钥的配对使用是明文加解密的关键。公钥用于加密明文，私钥用于解密密文。若发信方（加密者）想发送只有收信方（解密者）才允许解读的信息，发信方必须首先知道收信方公钥，并利用此公钥加密；该份密文用且仅能用收信方的私钥解密。由此可见，非对称密码体制拥有两个秘钥，且由公钥推出私钥在计算上是极为困难的，这也极大提高了数据加密安全性。公钥密码体制的建立，对密码学具有革命性的意义。目前，广泛应用的非对称密码体制有 RSA、椭圆曲线密码（Elliptic Curve Cryptography, ECC）等。

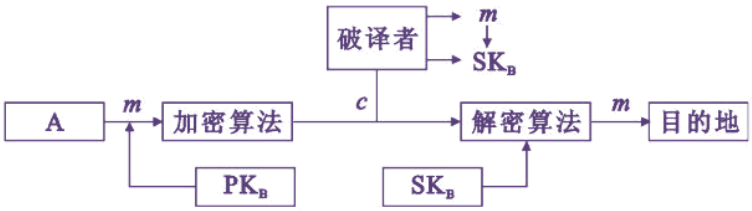


图 5　公钥加密流程

表 4　加解密算法类型

算法类型	特点	优势	缺陷	代表算法
对称加密	加解密的密钥相同	计算效率高，加密强度高	需要提前共享密钥，易泄密	DES、3DES、AES、IDEA
非对称加密	加解密的密钥不相关	无需提前共享密钥	计算效率低，仍存在中间人攻击的可能性	RSA、Elgamal、椭圆曲线系列算法

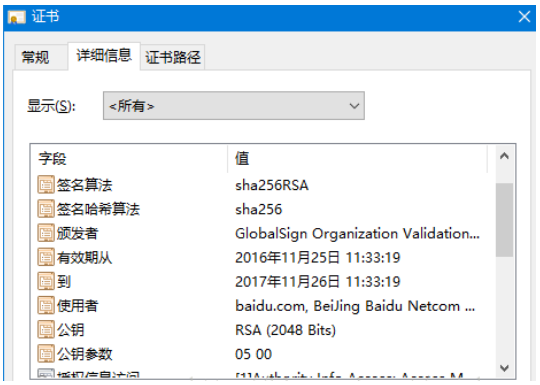
正逐渐发展的数字签名便应用了公钥密码体制，公钥加密系统的加入，保证了数字签名的不可伪造性和不可抵赖性。数字签名跟手写签名的作用实质上是一样的，用来证明某个消

息或者文件是本人发出/认同的。我国在 2005 年就已经施行《电子签名法》，确立了电子签名（包括但不限于数字签名）的法律效力。

常见的签名算法有 RSA，DSA，ECDSA，其中 RSA 是实现数字签名最简单的公钥加密算法。RSA 既可以用公钥加密然后私钥解密，也可以用私钥加密然后公钥解密，这是它的对称性。因为 RSA 中的每一个公钥都有唯一的私钥与之对应，任一公钥只能解开对应私钥加密的内容。

这样，如果你生成了一对 RSA 密钥，你把公钥公布出去，并告诉全世界人这个公钥是你的。之后你只要在发送的消息，比如“abcd”，后面加上用私钥加密过的密文，其他人拿公钥解密，看解密得到的内容是不是“abcd”就可以知道这个“abcd”是不是你发的。其他人没有对应的私钥，没法生成公钥可以解密的密文，所以是不可伪造的。又因为公钥对应的私钥只有一个，所以只要能成功解密，那么发消息的一定是你，不会是其他人，所以是不可抵赖的。

数字签名的用途很多，最常见的用处就是用来认证一个网站的身份，比如百度主页的数字签名证书。



除此之外，代码签名也是其重要的用途。如果 Windows 上的可执行程序来源于正规公司，那么通常它会有代码签名，用于确保其来源可靠且未被篡改。

3.1.2 哈希算法

哈希函数（Hash Function），也称散列函数，是一种在有限合理的时间内，将任意长度消息压缩为固定长度的消息摘要的函数。哈希算法就是在哈希函数基础上构造的、用于实现数据完整性和实体认证的算法。哈希函数的表示形式为：

$$h = H(m)$$

其中，h为固定长度的哈希值，m为任意长度消息，H为哈希函数。

MD5（Message Digest Algorithm 5）是 1991 年由 Rivest 开发出的在计算机领域广泛使用的散列函数[7]，提供将大容量信息在用数字签名软件签署私钥前被压缩成一定长度的十六进制数字串。美国联邦信息处理公开标准文件（FIPS 180-2）定义了四种安全的哈希算法：SHA-1，SHA-256，SHA-384，SHA-512[8]，每种算法都是某种单项哈希函数的迭代过程。这些哈希函数可以处理任意长度的消息输入，形成“消息摘要”（Message Digest）。在我国，由密码学学者王小云和国内其他专家设计的哈希函数算法标准 SM3 于 2010 年 12 月 17 日发布，已被广泛应用于数字签名及验证、消息验证码生成及验证、随机数生成，为超过 6 亿智能电网用户和上亿银行卡提供保护。

表 5　典型散列算法特点

加密算法	安全性	运算速度	输出大小（位）
MD5	低	快	128
SHA1	中	中	160
SHA256	高	比 SHA1 略低	256
SM3	高	比 SHA1 略低	256

具体而言，上述四种算法均包含两个处理阶段：预处理（Preprocessing）和哈希计算（Hash Computation）。预处理进行消息填充、分割已填充消息、设置哈希计算初始化值等工作，而哈希计算则利用预处理消息迭代生成一系列连续哈希值，即消息摘要（Message Digest）。

哈希函数具有如下特性：

- **正向快速**：给定明文和 Hash 算法，在有限时间和有限资源内能计算出 Hash 值；
- **逆向困难**：给定若干 Hash 值，在有限时间内很难（基本不可能）推出明文；
- **输入敏感**：一旦原始输入信息做出一点修改，产生的 Hash 值应有很大不同；
- **冲突避免**：很难找到两段内容不同的明文，使得它们的 Hash 值一致（发生冲突）。

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植等内容打包成一个区块，向全网广播。对原数据的任何改动，都将生成不同的消息摘要，

[7] Rivest R. The MD5 message-digest algorithm[J]. 1992.

[8] FIPS N. 180-2: Secure hash standard (SHS)[J]. US Department of Commerce, National Institute of Standards and Technology (NIST), 2012.

这就使得该算法充分保证原数据的完整性。正是由于上述重要特性，哈希算法被广泛应用于生成和验证数字签名、消息认证码、随机数产生、错误校正与检测等领域。

3.1.3 密码学国际研究现状

密码学作为区块链重要理论基础，具有一个完备而复杂的知识体系，涵盖了庞大的知识图谱，这些学科的发展支撑了现代密码学研究的爆发式增长。数论、线性代数、信息论、通信、近世代数为密码学的发展奠定了基础。而从密码学研究的趋势来看，zero knowledge（零知识）、secure computation（安全计算）、black box（黑箱）、elliptic curve（椭圆曲线）、secret sharing（秘密共享）是近期学者关注的焦点。从全局研究热度看，zero knowledge（零知识）依旧是研究热度最高的话题，紧随其后的热点研究领域则分别是 public key（公钥）、key distribution（密钥分配）和 hash function（哈希函数）。

其中，zero knowledge（零知识）从上世纪八十年代后期就受到了学者高度关注，且在 30 年内话题热度不减。从新世纪开始，public key（公钥）、key distribution（密钥分配）的发展势头日趋强劲，这与比特币的兴起和区块链的落地有着密不可分的关联。由上文所述，公钥体系的建立对密码学具有革命性的意义，是现代密码学投向应用的重要里程碑。同时，我们也能够清晰地看到，在传统热点之下也有许多具有潜力的研究方向逐渐浮出水面，受到各国学者越来越多的关注。可见在密码学蓬勃发展的今天，热点变换之快超出人们的预想。

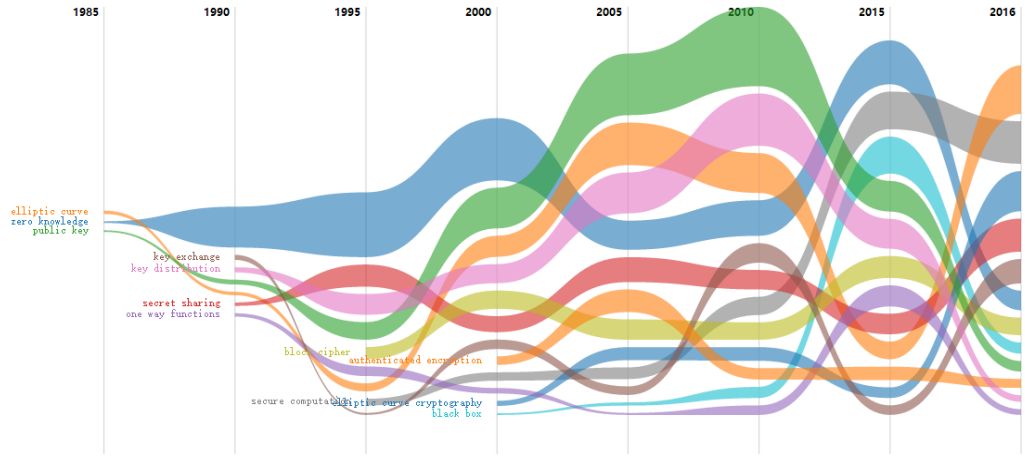


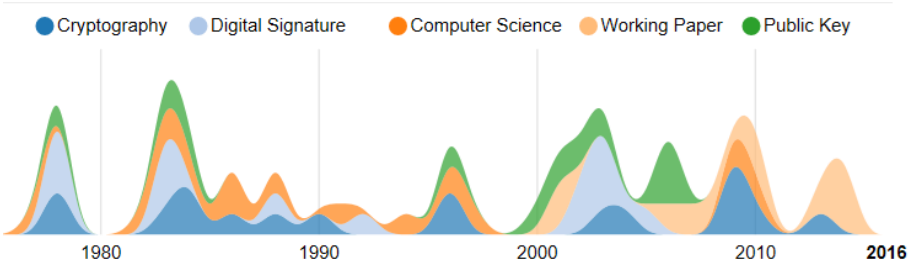
图 6　密码学研究全局热点

目前，人们普遍意识到，计算和通信技术正在以一种超出预想的速度融合。我们正在进入一个高度连接的世界，每个用户都可以看到其他用户的数据。维护信息的隐私和完整性的目前最实用的方法就是进行公钥加密。公钥加密技术已经广泛运用在人类社会中。Microsoft 浏览器和服务器实用公钥加密技术进行客户端或服务器身份验证和密钥管理。信用卡的安全电子交易标准也运用到了公钥密码技术。今天，数以万计的人们通过互联网从事信贷购车业

务，信贷购车网站的数量也在飞速增长，这也与公钥加密技术的使用密切相关。事实上，如果没有公钥加密技术提供的灵活、强大的安全保障，依托于互联网的电子商务交易就很难实现。未来，公钥加密技术将成为各类信息系统中不可分割的重要组成部分。

3.1.4 密码学代表学者

Ronald L. Rivest



Rivest 是麻省理工学院电子和计算机系 Viterbi 讲座教授和计算机与人工智能实验室成员。自 1969 年从耶鲁大学获得数学学士学位、1977 年从斯坦福大学获得计算机博士学位后，Rivest 专注于密码安全和计算机安全算法的研究。他的研究兴趣集中在密码学、数字信号、计算机科学、公钥体系等，从研究方向趋势图可看出，Rivest 从 70 年代开始始终对密码学保持密切的关注。其最重要的贡献在于和另外两位科学家 Adi Shamir 与 Leonard M.Adleman 一起开发了 RSA 算法[9]，获得了信息安全领域的重大突破，三人并凭借该算法获得 2002 年图灵奖。RSA 算法也由三位科学家姓氏的首字母命名。

RSA 算法推动使用公钥加密技术支持计算机安全通讯领域的研究取得重大进展。目前，RSA 系统被广泛应用于电子邮件、Web 浏览器、虚拟私有网络、移动电话及其他许多需要安全交换信息的应用程序。RSA 加密算法的核心是分解最大整数的困难。而分解整数又涉及寻找质数。我们可以将这个过程假设为甲、乙二人想要秘密通信，并保证丙不会窃听内容。为此，甲秘密地选择了两个质数（通常长度为 100 位）并将这两个质数相乘，创建出一个“公

[9] Rivest R L, Shamir A, Adleman L M. Cryptographic communications system and method: U.S. Patent 4,405,829[P]. 1983-9-20.

钥”在互联网上发布。当乙向甲发布秘密信息时，乙就从互联网上获得甲的公钥，并将自己的密钥输入到 RSA 算法中将他的消息加密。由于只有甲知道自己的公钥是如何创建的，因此只有甲能够破译乙发送过来的信息。尽管丙能够看到加密的信息和甲的公钥，但是并不知道甲的公钥是如何创建的，丙也就无从知晓如何解读乙的信息。在这种情况下，甲和乙之间的对话就是非常机密和安全的了。这就是 RSA 算法的本质。

420

Introduction to algorithms EI

thomas h cormen, clifford stein, **ronald l rivest**, charles e leiserson

Introduction to algorithms (1990)

Cited by 47875 Bibtex http://dx.doi.org/10.1057/jors.1991.155

419

A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYP-TOSYSTEMS

R. L. Rivest, A. Shamir, L. M. Adelman

Communications of The ACM (1977)

Cited by 19244 Bibtex

418

A method for obtaining digital signatures and public-key cryptosystems EI

R. L. Rivest, A. Shamir, L. Adleman

Communications of the ACM - Special 25th Anniversary Issue (1983)

Cited by 17694 Bibtex http://dx.doi.org/10.1145/357980.358017

417

A method for obtaining digital signatures and public-key cryptosystems EI

R. L. Rivest, A. Shamir, L. Adleman

Commun. ACM (1978)

Cited by 12228 Bibtex http://doi.acm.org/10.1145/359340.359342

416

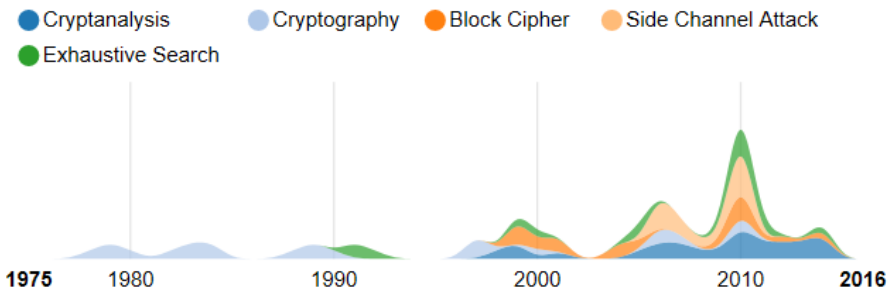
The MD4 Message-Digest Algorithm EI

R. Rivest

RFC (1992)

Cited by 5916 Bibtex https://doi.org/10.17487/RFC1320

Adi Shamir



Adi Shamir 是著名的密码学专家，其研究兴趣包括密码学理论、分组密码、侧通道攻击、穷举搜索等，自 2010 年以来在后三者的研究贡献尤为突出。Shamir 早年在以色列魏茨曼科学研究所获得硕士、博士学位，其博士论文题目为《不动点的递归程序和它们之间的 Agard 微分关系》。1977 至 1980 年在美国麻省理工学院学习后返回以色列，并从 2006 年起受邀担任巴黎高等师范学院教授。

308

A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYP-TOSYSTEMS

R. L. Rivest, **A. Shamir**, L. M. Adelman

Communications of The ACM (1977)

Cited by 19244 Bibtex

307

A method for obtaining digital signatures and public-key cryptosystems EI

R. L. Rivest, **A. Shamir**, L. Adleman

Communications of the ACM - Special 25th Anniversary Issue (1983)

Cited by 17694 Bibtex http://dx.doi.org/10.1145/357980.358017

306

A method for obtaining digital signatures and public-key cryptosystems EI

R. L. Rivest, **A. Shamir**, L. Adleman

Commun. ACM (1978)

Cited by 12228 Bibtex http://doi.acm.org/10.1145/359340.359342

305

How to share a secret EI

Adi Shamir

Commun. ACM (1979)

Cited by 7090 Bibtex http://doi.acm.org/10.1145/359168.359176

304

Identity-based cryptosystems and signature schemes EI

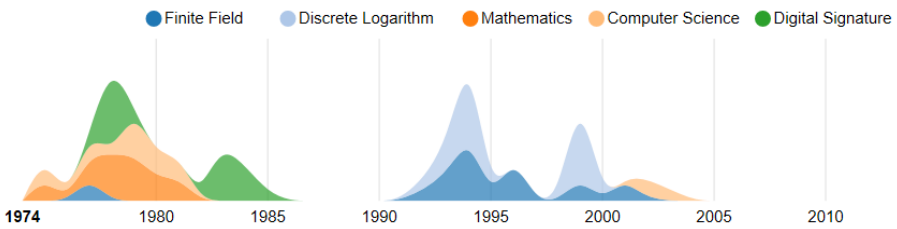
Adi Shamir

CRYPTO (1984)

Cited by 4045 Bibtex https://static.aminer.org/pdf/20170130/pdfs/index.txt

经过多年对密码学领域的探索，Shamir 成为世界公认的密码学领军人物，也收获了一系列奖项，包括美国计算机学院 Kannelakis 奖、以色列数学协会 Erdos 奖、IEEE W.R.G. Baker 奖、UAP 科学奖、梵蒂冈 PUIS XI 金奖以及 IEEE Koji Kobayashi 计算机与通信奖等。除了 RSA 算法之外，Shamir 在密码学领域的建树还包括 Shamir 秘密共享方案、Merkle-Hellman 密码系统的破解、视觉密码以及 TWIRL 和 TWINKLE 因子分解设备。Shamir 同 Eli Biham 一起发现了差分密码分析法——一种用来破解分组密码的一般性方法。

Leonard M. Adleman



RSA 系统的第三位贡献者是加州大学伯克利分校教授 Leonard M. Adleman。Adleman1945 年出生于旧金山，在加州大学伯克利分校获得了数学学士学位和计算机工程博士学位，其后加入麻省理工学院，与 Rivest 和 Shamir 共同开发了 RSA 公钥密码体制。据他的学生回忆，Adleman 有了灵感总要到办公室黑板上演算，并与自己的导师和前辈共同分享自己破解谜题时的喜悦之情，学生们在黑板上演算时，他一边听，一边提出建议和问题。Adleman 在研究上花费了常人难以想象的时间和精力，他每周都会工作 70 小时以上。他狂热的工作风格和常人难以达到的多学科成果，被人们称为“Mad Scientist”。

99

A method for obtaining digital signatures and public-key cryptosystems EI

R. L. Rivest, A. Shamir, **L. Adleman**

Communications of the ACM - Special 25th Anniversary Issue (1983)

Cited by 17694 Bibtex http://dx.doi.org/10.1145/357980.358017

98

A method for obtaining digital signatures and public-key cryptosystems EI

R. L. Rivest, A. Shamir, **L. Adleman**

Commun. ACM (1978)

Cited by 12228 Bibtex http://doi.acm.org/10.1145/359340.359342

97

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems (Reprint) EI

Ronald L. Rivest, Adi Shamir, **Leonard M. Adleman**

Commun. ACM (1983)

Cited by 1842 Bibtex http://doi.acm.org/10.1145/357980.358017

96

On data banks and privacy homomorphisms

R. Rivest, **L. Adleman**, M. Dertouzos

(1978)

Cited by 1490 Bibtex

95

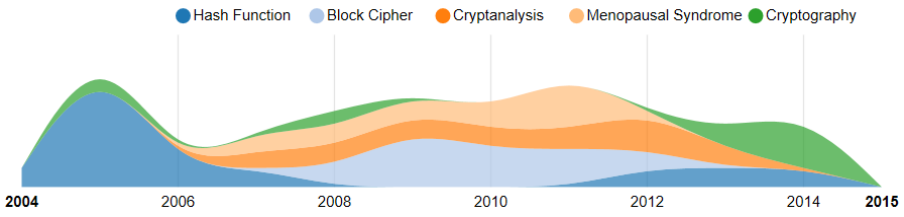
Solution of a 20-Variable 3-SAT Problem on a DNA Computer SCIENCE WOS

Ravinderjit S. Braich, Nickolas Chelyapov, Cliff Johnson, Paul W. K. Rothemund, **Leonard Adleman**

science (2002)

Cited by 674 Bibtex http://www.sciencemag.org/content/296/5567/499.abstract

王小云

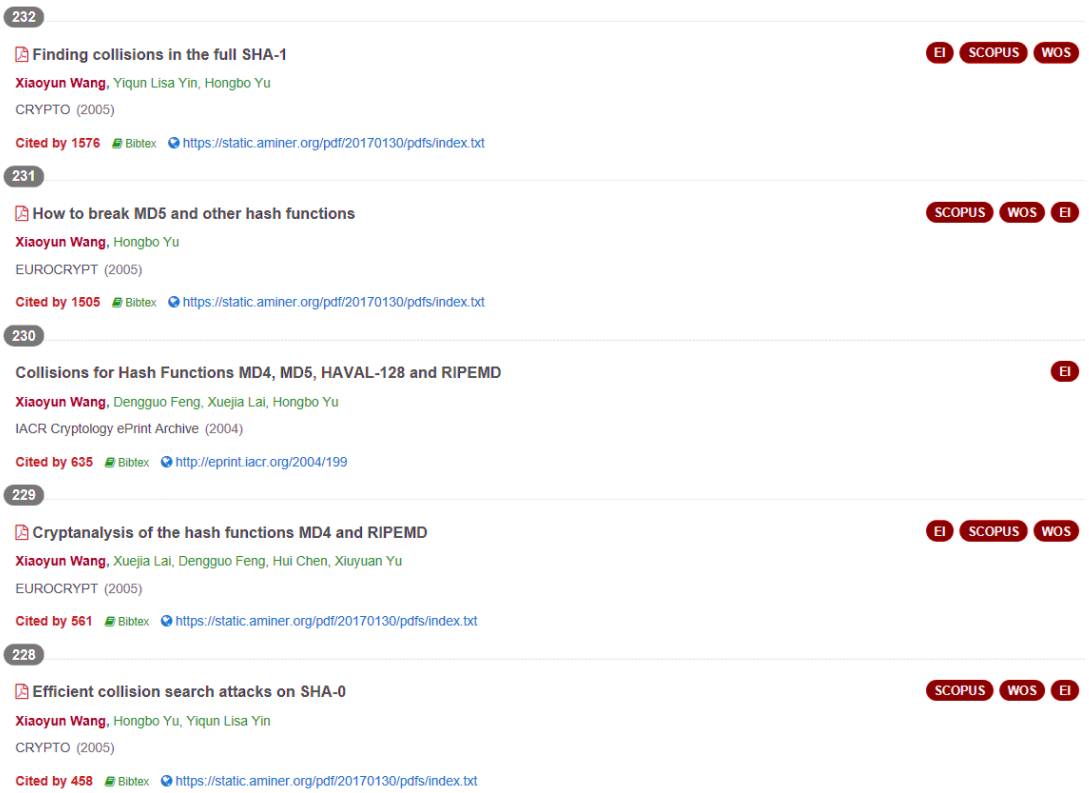


王小云是国内密码学的杰出学者，在国际上也享有极高的声誉。她 1983—1993 就读于山东大学数学系，先后获得学士、硕士与博士学位。1993 年在山东大学数学系任教，现任清华大学教授，2017 年 11 月当选中国科学院院士。王小云致力于密码理论及相关数学问题的研究，提出了密码哈希函数的碰撞攻击理论，即模差分比特分析法，破解了包括 MD5、SHA-1 在内的 5 个国际通用哈希函数算法，给出了系列消息认证码 MD5-MAC 等的子密钥回复共计和 HMAC-MD5 的区分攻击；提出了格最短向量求解的启发式算法二重筛法；设计了

中国哈希函数标准 SM3，该算法在金融、国际电网、交通等重要社会经济领域广泛使用。

1987 年，王小云进入山东大学数学系攻读研究生，并于 1990 年师从数学家潘承洞教授进行数论与密码学研究。博士毕业后，王小云选择继续在科研道路上深入，从那时起，破解哈希函数理论分析技术的思想就已经在她的脑海中涌动。

美国标准及数据（NIST）颁布的基于哈希函数的 MD5 和 SHA-1 多年来被公认为是最先进、最安全的算法。这两种算法对输入信息做出的任何微小更改（如反转一个二进制位）都会导致输出的不可区分性改变（输出的每一个二进制位均有 50%的概率反转），即产生雪崩效应（avalanche effect）。按照常规方法，破解 MD5 和 SHA-1 是不可能或几乎行不通的，这也在一定程度上确保了电子签名的安全。但是，王小云的“横空出世”却对这两大算法产生了前所未有的冲击。2004 年 8 月 17 日，王小云在美国加州圣巴巴拉召开的国际密码学会议（Crypto’2004）上首次宣布她和她的研究小组对 MD5、HAVAL-128、MD4 和 RIPEMD 四种密码算法的破译结果，对曾经被认为是“不可破解”的世界通行密码标准 MD5 宣告攻破。会议总结报告这样写道：“我们该怎么办？MD5 被重创了，它即将从应用中淘汰；SHA-1 还活着，但也见到了他它的末日”。果不其然，2005 年 2 月的 RSA 年会，SHA-1 也由王小云宣告破解。在她的算法下，普通计算机只需几分钟就能够找到 MD5 的“碰撞信息对”，这意味着现行的基于哈希函数的密码系统及应用都面临被攻击的风险。

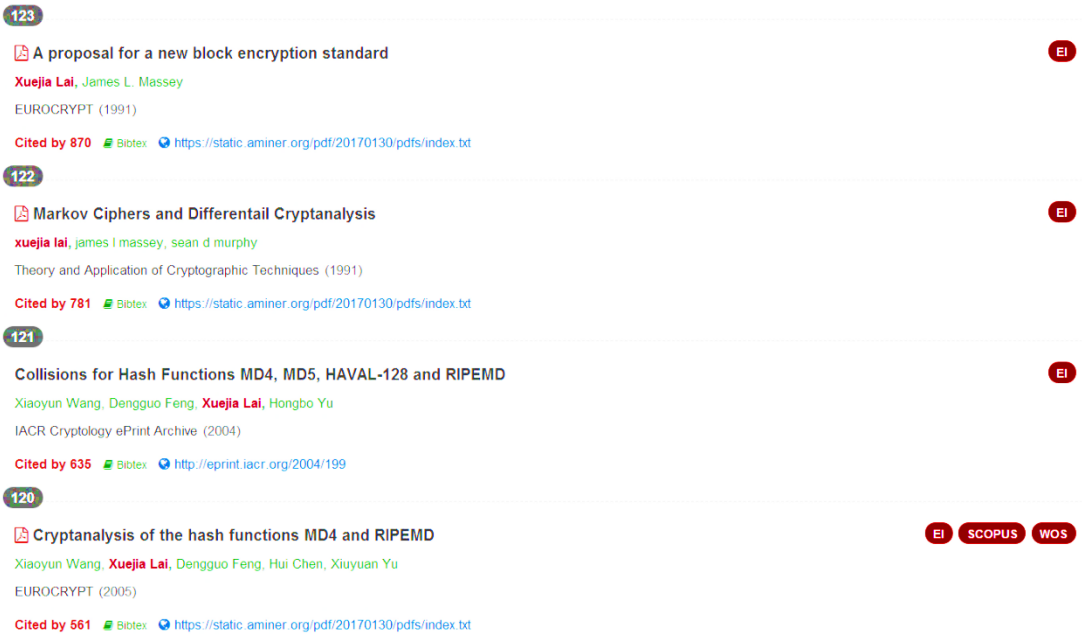


在两大加密算法受到巨大冲击后，美国政府宣布不再使用 SHA-1 并面向世界范围内的专家征集更安全的国际标准算法。然而王小云放弃了参与设计国际标准的团队，投身于建立国内标准密码算法的工作中。2005 年，王小云与国内其他专家共同设计的 SM3 哈希函数算法标准正式发布，目前已为国内众多应用的安全保驾护航。“一般黑客会选择攻击非标准化的密码系统或者没有部署密码技术的网络通信系统。随着国家对密码学和现代信息安全问题越来越重视，从事密码学研究的人越来越多，他们不断完善各行业信息安全上的密码系统，这会进一步压缩黑客的生存空间”。

在王小云的眼中，密码学就像“设谜”与“猜谜”的过程，一般人看来复杂而枯燥的密码学对她而言具有无穷的魅力：“那么繁琐复杂的万物运行，就蕴藏在简介的数与形里。真正沉下心去理解这些符号，层层剥笋由浅入深，由简单到复杂，一层比一层更接近本质，很是奇妙。”

来学嘉

来学嘉自 2004 年起担任上海交通大学教授，在过去的 20 年里，他的工作主要集中在密码学和 PKI 领域，特别是在设计和分析实用的密码系统（包括块密码和流密码）、分组密码的微分密码分析、分析和哈希函数等方面。1994 年，来学嘉加入 R3 安全工程公司，自 2001 年起担任瑞士 S.W.I.S.集团高级顾问和技术总监，参与欧洲银行使用的欧洲芯片的算法设计，参与制定 3ISO 安全标准。来学嘉曾出版著作《关于块加密密码的设计和安全性》和 40 多篇论文，也一直在评估、分析和改进几个国际公司和组织的密码，参与 KRISIS、ICE-CAR 和 PKI 项目，并同时担任中国科学技术大学研究生院名誉教授，西南交通大学顾问教授，中国密码学学会常务理事。其代表学术成果集中于哈希方程、分组密码、信息安全工程、密码学等领域的研究：

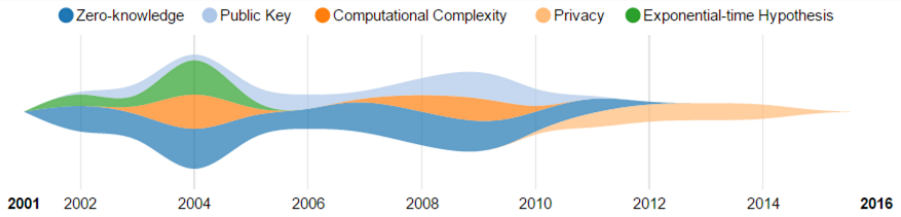


[10]在来学嘉教授回国后的最初几年，适逢中国信息安全发展的黄金时期，安全产业风起云涌，信息安全人才涌现，行业、产品都取得了非常多的成果，但是唯独理论方面尚有欠缺。是时，很多人都在探讨信息安全究竟是什么，也有很多人问他这个问题，就是这个看似很简单，看似已有定论的概念，他用了很长时间去考虑。其实在国际上，对于信息安全的定义和概念，以及它的研究对象等问题的探讨也从来没有停止。作为国际知名的密码学家，密码学是来学嘉教授的主要研究领域，但是密码学是否就可以等同于信息安全？

在其研究越来越深入后，来学嘉教授也认识到，虽然自己做的最多的是密码，但是很多时候不可避免地涉及到信息安全。密码与信息安全殊途同归，其实二者在本质上是相同的，说到底都是单向性——好用、难破，但是信息安全的需求却比密码研究更为迫切。来学嘉将信息安全定义为“研究有敌手参与的信息系统”。面对信息威胁构建动态的应对体系，这是信息安全存在的意义。从政府、银行、企业到个人，追求信息安全的呼声越来越高。来学嘉教授也表示，未来需要更多信息安全专门人才参与系统设计，将安全性和可用性更好地结合。

[10]白洁.信息安全与通信保密二三事——专访著名密码学者来学嘉教授[J].信息安全与通信保密,2009(10):14-17.

赵运磊



赵运磊现任复旦大学计算机学院教授、博士生导师。中国密码学会安全协议专委会委员，上海信息安全专委会委员。先后以负责人承担 973 课题、3 项国家自然科学基金、中央机要局十一五、十二五国家密码发展基金（重点项目，保密项目）。先后入选上海市人事局“浦江”人才计划（特殊急需人才计划）、上海市科委“科技启明星”人才计划，微软亚洲学者、复旦大学优秀博士论文，复旦大学优秀博士后等荣誉称号。

72

A new framework for RFID privacy SCOPUS WOS EI

Robert H. Deng, Yingjiu Li, Moti Yung, **Yunlei Zhao**

IACR Cryptology ePrint Archive (2010)

Cited by 120 Bibtex http://eprint.iacr.org/2010/059

71

Generic construction of chosen ciphertext secure proxy re-encryption EI SCOPUS WOS

Goichiro Hanaoka, Yutaka Kawai, Noboru Kunihiro, Takahiro Matsuda, Jian Weng, Rui Zhang, **Yunlei Zhao**

CT-RSA (2012)

Cited by 52 Bibtex http://dx.doi.org/10.1007/978-3-642-27954-6_22

70

On the security of a bidirectional proxy re-encryption scheme from PKC 2010 SCOPUS WOS EI

Jian Weng, **Yunlei Zhao**, Goichiro Hanaoka

IACR Cryptology ePrint Archive (2011)

Cited by 35 Bibtex http://eprint.iacr.org/2010/319

68

Analysis of differentially expressed genes in genic male sterility cotton (Gossypium hirsutum L.) using cDNA-AFLP. SCOPUS EI WOS

Xiaoding Ma, Chaozhu Xing, Liping Guo, Yangcang Gong, Hailin Wang, **Yunlei Zhao**, Jianyong Wu

Journal of genetics and genomics = Yi chuan xue bao (2007)

Cited by 27 Bibtex http://www.ncbi.nlm.nih.gov/pubmed/17601613?report=xml&format=text

67

Efficient public key cryptosystem resilient to key leakage chosen ciphertext attacks SCOPUS WOS EI

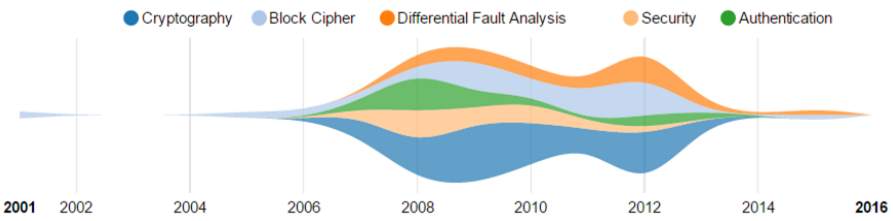
Shengli Liu, Jian Weng, **Yunlei Zhao**

CT-RSA (2013)

Cited by 25 Bibtex http://dx.doi.org/10.1007/978-3-642-36095-4_6

赵运磊教授研究注重成果的体系化、系统化，并注重理论联系实际、产学研相结合。他的研究涵盖密码学理论及应用两个方面：其一，密码核心基础理论：伪随机、零知识、知识证明、non-malleability 上获得系统性的创新，获得基于复杂性理论的可证明安全性新理论框架等系统性和基础性的重要突破。其二，在密码应用上，在创新理论框架的指导下设计研发高度应用的密码协议，发展创新的网络安全核心密码协议新技术和重要技术革新，获得一系列自主知识产权，积极推动或参与若干网络安全核心密码协议国际标准的更新换代或改进提高，服务于国家知识经济的发展和（信息安全）核心技术的自主创新。赵运磊教授的密码学理论及应用研究两个特点：国内极少数密码研究成果被计算机科学理论、密码学、信息安全三个领域的一区会议均引用的学者之一；国内极少数以第一或通讯作者在密码学与信息安全一区会议均发表论文的学者之一。

谷大武



谷大武，上海交通大学长江特聘教授、博士生导师、国家二级教授，计算机系密码安全团队负责人，密码与计算机安全实验室（LoCCS）主任。主要研究兴趣包括密码学、软件与系统安全、硬件与系统分析、大数据和云安全和金融安全技术等。谷大武 1988-1998 就读于西安电子科技大学，先后获应用数学学士、密码学硕士和密码学博士学位，目前已有学术论文 120 篇，发明专利 20 项，主要成果发表在 CRYPTO、CHES、FSE、TCC、CCS、ACSAC、RAID、SANER、ESORICS、ACM Computing Surveys、IEEE TDSC、IEEE TIFS、IEEE TCAD、中国科学等期刊和会议上，担任 E-Forensics2010、CASC2011、CryptoIC2013、ChinaCrypt2015 等大会主席或程序委员会主席，30 余次担任 ASIACRYPT、ASIACCS、ACNS、ISC、ISPEC、ICICS、Globecom、IEEE TrustCom 等国际会议 PC。

308

Differential and linear cryptanalysis using mixed-integer linear programming SCOPUS WOS EI

Nicky Mouha, Qingju Wang, **Dawu Gu**, Bart Preneel

Inscrypt (2011)

Cited by 97 Bibtex http://dx.doi.org/10.1007/978-3-642-34704-7_5

307

Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis WOS EI

Delvaux, J., Dawu Gu, Schellekens, D., Verbauwhede, I.

IEEE Trans. on CAD of Integrated Circuits and Systems (2014)

Cited by 49 Bibtex http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=6965637

306

Differential fault analysis on the ARIA algorithm SCOPUS WOS EI

Wei Li, **Dawu Gu**, Juanru Li

Inf. Sci. (2008)

Cited by 47 Bibtex http://dx.doi.org/10.1016/j.ins.2008.05.031

305

Impossible differential attacks on reduced-round LBlock SCOPUS WOS EI

Ya Liu, **Dawu Gu**, Zhiqiang Liu, Wei Li

ISPEC (2012)

Cited by 44 Bibtex http://dx.doi.org/10.1007/978-3-642-29101-2_7

304

A Survey on Lightweight Entity Authentication with Strong PUFs EI

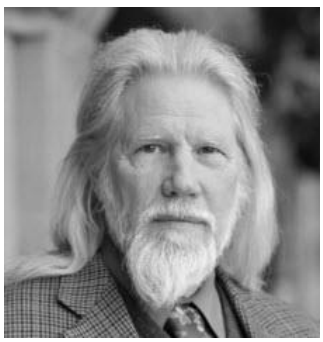
Jeroen Delvaux, Roel Peeters, Dawu Gu, Ingrid Verbauwhede

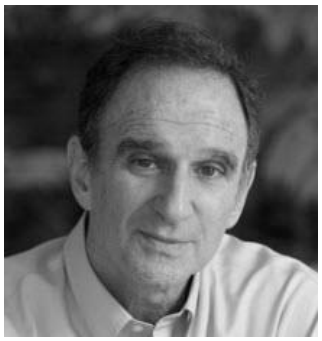
ACM Computing Surveys (2015)

Cited by 41 Bibtex http://doi.acm.org/10.1145/2818186

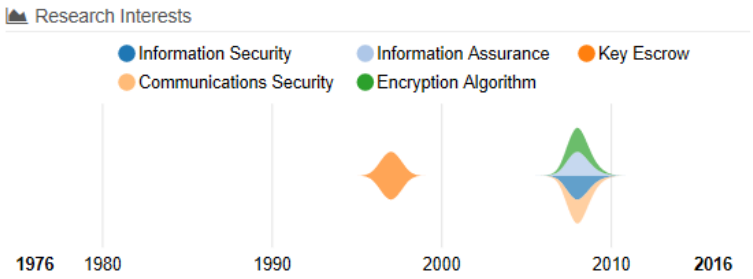
2018 年 1 月 8 日，2017 年国际科学技术奖在北京人民大会堂揭晓。谷大武团队的科研成果《密码芯片系统的攻防关键技术研究及应用》获得国家科技进步二等奖。上海交通大学官方网站对谷大武的学术成就给予了高度评价：“密码芯片系统是网络与信息安全呢的基础和支撑，该项目立足自主研发与开放创新，突破了密码芯片攻防的系列关键技术。谷大武等人提出了密码芯片分析的先进模型、算法和实现方法，研制出领先的攻击检测平台；设计了一系列芯片防护新方法，研制出 7 类核心芯片，实现了国产芯片在民生、工业领域的大规模应用并辐射海外，防护技术用于国内主流企业的芯片设计。谷大武等人带头研制的金融卡芯片防护水平跻身国际一流，智能电表和智能电网安全芯片实现了电力行业自主密码芯片从无到有的突破。”

Bailey Whitfield Diffie & Martin Edward Hellman

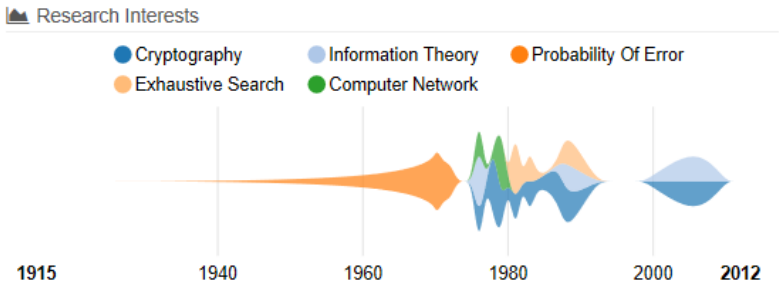




Bailey Whitfield Diffie，著名密码学学者，2015 年图灵奖得主。1965 年在麻省理工学院取得博士学位，现斯坦福大学学者。



Martin Edward Hellman，1969 年在斯坦福大学取得博士学位，密码学者，对公开密钥加密技术有重要贡献。



1976 年，Diffie 与 Hellman 共同发表论文《密码学的新方向》（New Directions in Cryptography），他们在此论文中提出 Deffie-Hellman 密钥交换，并由此获 2015 年图灵奖。获奖理由是“他们对现代密码学的重要贡献，他们的论文介绍了公钥密码学和数字签名的思想，这是当今互联网上最常用的安全协议的基础。”

Diffie 还与 Hellman 一起获得了 Golden Jubilee Award for Technological Innovation from the IEEE Information Theory Society、NIST/NSA National Computer Systems Security Award、Franklin Institute’s Levy Medal、IEEE Kobayashi Award 等奖项。

Deffie-Hellman 密钥交换协议

Deffie-Hellman 密钥交换协议是密码学领域内最早付诸实践的密钥交换方法之一。它可以让双方在完全缺乏对方（私有）信息的前提条件下通过不安全的信道达成一个共享的密钥。此密钥用于对后续信息交换进行对称加密。

Deffie-Hellman 算法原理：Diffie-Hellman 加密算法的有效性依赖于计算离散对数的难度。简言之，可以如下定义离散对数：首先定义一个素数 p 的原根，为其各次幂产生从 1 到 p-1 的所有整数根，也就是说，如果 a 是素数 p 的一个原根，那么数值 a mod p,a2 mod p,⋯,ap-

1 mod p 是各不相同的整数，并且以某种排列方式组成了从 1 到 p-1 的所有整数。对于一个整数 b 和素数 p 的一个原根 a，可以找到惟一的指数 i，使得 b=ai mod p 其中 0≤i≤ (p-1) 指数 i 称为 b 的以 a 为基数的模 p 的离散对数或者指数，该值被记为 inda，p(b)。

Diffie-Hellman 算法具有两个吸引力的特征：

1、仅当需要时才生成密钥，减小了将密钥存储很长一段时间而致使遭受攻击的机会。

2、除对全局参数的约定外，密钥交换不需要事先存在的基础结构。

3.2 共识协议

共识协议或共识平台是分布式账本技术的核心。分布式账本能在点对点（Peer to Peer, P2P）网络中的不同节点之间相互复制，且各项交易均由私钥签署。区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。如何在分布式系统中高效地达成共识，是分布式计算领域的重要研究问题。决策权越分散，系统达成共识的效率越低，但系统稳定性和满意度越高；与此相对，决策权越集中，系统更易达成共识，但同时更易出现独裁。区块链的分布式存储的独特性体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据；二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，数据节点可以是不同的物理机器，也可以是云端不同的实例。区块链解决的核心问题之一，就是通过决策权高度分散的“去中心化”系统提升稳定性和满意度，使各节点针对区块数据的有效性达成共识。

表 6　共识机制分类

应用条件	共识机制
没有节点作恶	Paxos、Raft、ZooKeeper、ViewTimestamp Replication
有节点作恶	PBFT、PoW、PoS、DPoS、Algorand、Sleepycat、SnowWhite

共识协议要解决的核心问题是在网络中有节点作恶时如何能够达成共识。要解决这个困难，首先需要了解“拜占庭将军问题”。1982 年，Leslie Lamport、Robert Shostak 和 Marshall Pease 发表论文《拜占庭将军问题》[11]，提出一项思维实验：假设一组将军分别统领拜占庭军队的一部分，共同围困一座城市。这些将军只能通过信使将自己的策略相互传递。但是，这组将军中有一人或多人可能已经叛变，并试图传递错误信息以破坏作战计划。该实验的问题就在于，这只军队最多允许存在多少名叛变的将军，使得作战仍然可以

[11] Lamport L, Shostak R, Pease M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.

顺利完成？数字货币运行机制可类比于拜占庭将军问题场景。在分布式账本中，各参与者节点可近似看作将军。此问题即转化为，分布式系统可容许多少作恶节点，使得交易仍可正常进行，且不损害整体系统的可靠性？Lamport 本人已经给出了达到拜占庭容错的架构[12]，但算法复杂，难以投入应用。此后，Miguel Castro 和 Barbara Liskov 于 1999 年提出实用拜占庭容错算法（PBFT）[13]，此系统能够提供高性能的运算，可以每秒处理成千的请求。比特币系统则用“挖矿”的方式以解决拜占庭将军问题，利用去中心化的点对点加密协议运行区块链，实现了无需信任单个节点即可达成共识和建立互信。

除了拜占庭问题外，Sybil 攻击也是共识机制解决的重要问题之一。Sybil 攻击，又称女巫攻击，是指社交网络中的少数节点通过控制多个虚假身份来影响网络中的正常节点。具体来说，这些少数节点可能会对一个点对点网络呈现多个身份，且以不同节点的功能进行活动。因此，这些节点可能在网络上获得不成比例的控制权，随后做出恶意行为，如影响投票结果、降低点对点网络节点查找效率、破坏网络文件共享安全、消耗节点链接资源等。Sybil 攻击最早由 Douceur 在点对点网络环境中提出[14]，他指出这种攻击方式将破坏分布式存储系统中的冗余机制。此后，Karlof 和 Newsome 发现 Sybil 攻击对传感器网络的路由机制同样存在威胁[15][16]。Sybil 攻击能够对网络产生多大程度的影响，取决于攻击节点能够以多低成本产生虚假身份。Sybil 攻击只能控制单个节点，对全网的影响相对较小；但是，在 Sybil 攻击的基础上产生的 Eclipse 攻击和 DDoS 攻击，则会使部分节点脱离点对点网络，甚至占用大量受害节点资源，对全网造成致命打击。

---

[12] Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults[J]. Journal of the ACM (JACM), 1980, 27(2): 228-234.

[13] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI. 1999, 99: 173-186.

[14] Douceur J R. The sybil attack[C]//International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002: 251-260.

[15] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures[J]. Ad hoc networks, 2003, 1(2-3): 293-315.

[16] Newsome J, Shi E, Song D, et al. The sybil attack in sensor networks: analysis & defenses[C]//Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004: 259-268.

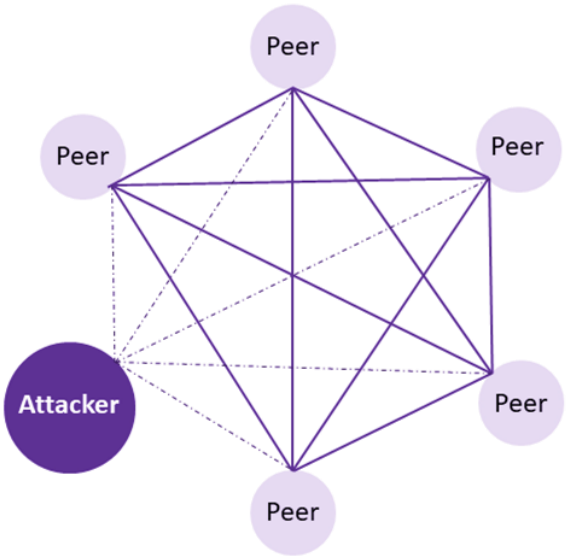


图 7　基于点对点网络的 Sybil Attack 原理

Sybil 攻击产生影响的方式主要为破坏信任、控制资源和低成本地加入网络。因此，防御 Sybil 攻击，也可以从信任认证、资源测试、提高节点加入网络代价三方面入手。工作量证明（Proof of Work, PoW）是抵御 Sybil 攻击的有效方式。PoW 机制能够实现区块链的一致性，由于网络中每个节点完成工作量的证明由其拥有的计算资源决定，因此攻击节点不能通过创建多个虚假身份提高自身完成工作量证明的概率，也就有效抵御了 Sybil 攻击。

3.2.1 共识机制

在分布式账本之中，共识机制使大部分（或全部）网络成员就某条数据或拟定交易的价值达成一致，并就此对账本进行更新的机制。换言之，共识机制是在参与节点之间管理一系列连贯实施的规则的程序。

共识算法允许关联机器连接起来进行工作，并在某些成员失效的情况下，工作仍能正常进行。这种容错能力是区块链与分布式账本的另一主要优势，并有内置冗余余量以作备用。

用以建立共识的算法多种多样，并建立基于性能、可扩展性、一致性、数据容量、治理、安全性和失效冗余等方面的要求。目前，广泛应用的共识机制包括 PoW、PoS、DPoS、PBFT 等。

表 7　共识机制及技术水平

共识机制	技术水平
PoW	依赖机器进行数学运算获取记账权，资源消耗相比其他共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网 50%节点出错。

PoS	主要思想是节点记账权的获得难度与节点持有的权益成反比。相对于PoW，一定程度上减少了数学运算带来的资源消耗，性能也得到相应提升但依然基于哈希运算竞争获取记账权的方式，可监管性弱，允许全网50%节点出错。
DPoS	与PoS主要区别在于节点选举若干代理人，由代理人验证和记账，其合规监管、性能、资源消耗和容错性与PoS相似。
PBFT	采用许可投票、少数服从多数来选举领导者进行记账，但该共识机制允许拜占庭容错，允许强监管节点参与，具备权限分级能力，性能更高，耗能更低。该算法每轮记账都会由全网节点共同选举领导者，允许33%的节点作恶，容错性为33%。

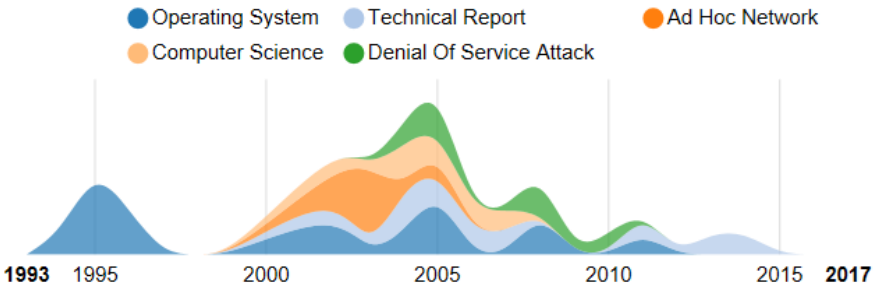
不同的共识机制会对区块链系统整体性能产生不同影响。因此，评价共识机制技术水平，通常从安全性、扩展性、性能效率和资源消耗四个方面入手。

表 8　共识机制评价维度

评价维度	含义
安全性	即是否可以防止二次支付、自私挖矿等攻击，是否有良好的容错能力。自私挖矿通过采用适当的策略发布自己产生的区块，获得更高的相对收益，是一种威胁比特币系统安全性和公平性的理论攻击方法。
扩展性	即是否支持网络节点扩展。扩展性是区块链设计要考虑的关键因素之一。根据对象不同，扩展性又分为系统成员数量的增加和待确认交易数量的增加两部分。扩展性主要考虑当系统成员数量、待确认交易数量增加时，随之带来的系统负载和网络通信量的变化，通常以网络吞吐量来衡量。
性能效率	即从交易达成共识被记录在区块链中至被最终确认的时间延迟，也可以理解为系统每秒可处理确认的交易数量。区块链技术通过共识机制达成一致，因此其性能效率问题一直是研究的关注点。
资源消耗	即在达成共识的过程中，系统所要耗费的计算资源大小，包括CPU、内存等。以比特币系统为例，基于工作量证明机制的共识需要消耗大量计算资源进行挖矿，提供信任证明完成共识。

3.2.2 共识机制代表学者

Emin Gün Sirer



Emin Gün Sirer 是康奈尔大学计算机科学副教授，研究兴趣包括分布式系统、加密货币和大规模服务的软件基础设施，尤其在操作系统、阻断服务攻击、计算机科学领域有较高的影响。

87

Extensibility safety and performance in the SPIN operating system EI

Brian N. Bershad, Stefan Savage, Przemysław Pardyak, **Emin Gün Sirer**, Marc E. Fiuczynski, David Becker, Craig Chambers, Susan J. Eggers

SOSP (1995)

Cited by 1373 Bibtex https://static.aminer.org/pdf/20170130/pdfs/index.txt

86

Meridian: a lightweight network location service without virtual coordinates EI

Bernard Wong, Aleksandrs Slivkins, **Emin Gün Sirer**

SIGCOMM (2005)

Cited by 533 Bibtex http://dx.doi.org/10.1145/1080091.1080103

85

Karma: A se-cure economic framework for p2p resource sharing

V. Vishnumurthy, S. Chandrakumar, **E. G. Sirer**

(2003)

Cited by 496 Bibtex

84

Majority Is Not Enough: Bitcoin Mining Is Vulnerable. EI

Ittay Eyal, **Emin Gün Sirer**

Financial Cryptography (2014)

Cited by 390 Bibtex http://arxiv.org/abs/1311.0243

83

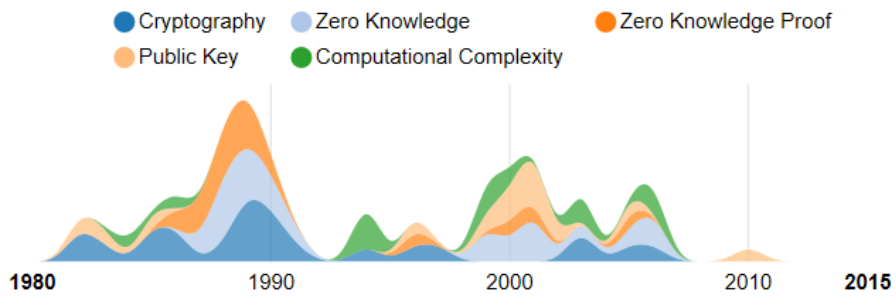
The design and implementation of a next generation name service for the internet EI

Venugopalan Ramasubramanian, **Emin Gün Sirer**

SIGCOMM (2004)

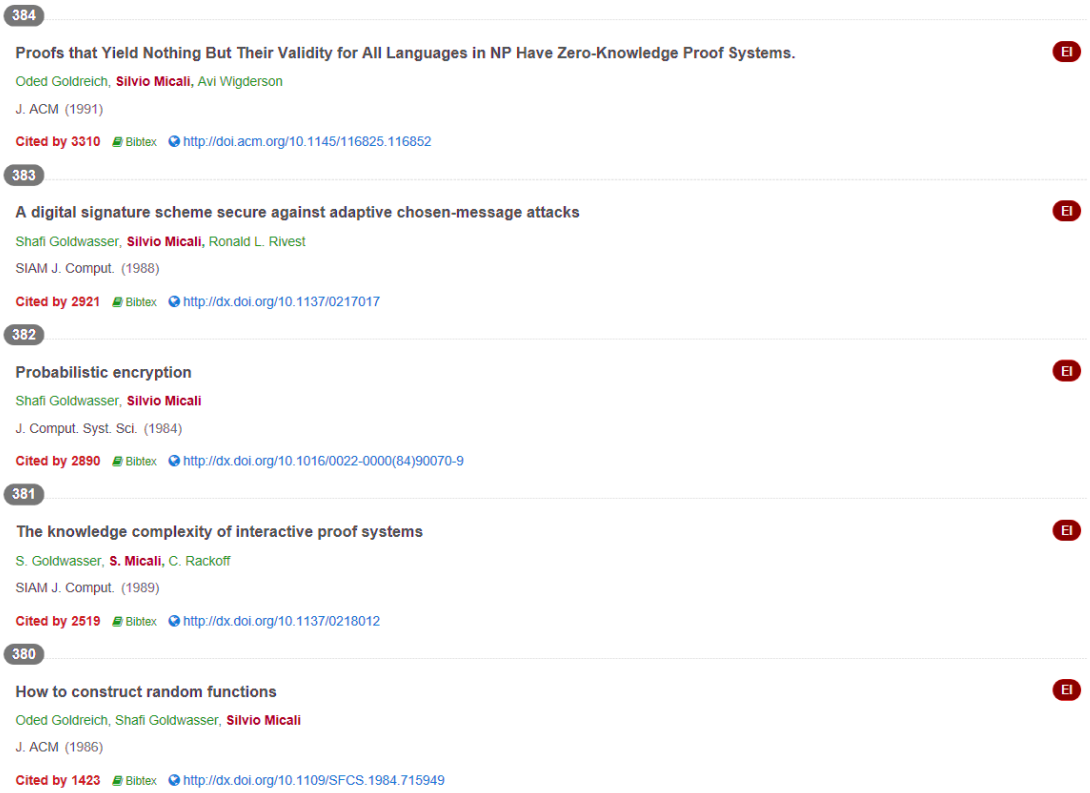
Cited by 386 Bibtex http://dx.doi.org/10.1145/1030194.1015504

Silvio Micali



Silvio Micali 于 1954 年出生在西西里的巴勒莫。他在罗马接受了本科教育，并于 1978 年从 Sapienza 大学获得数学学位，成为 Corrado Bohm 教授最聪明的学生之一。1982 年，他在加州大学伯克利分校攻读博士学位。在多伦多的博士后职位之后，他于 1983 年 7 月加入麻省理工学院，此后一直在那里工作。

Silvio Micali 是一个有远见的人，他的工作贡献了密码学的数学基础，并提出了计算理论。他的非传统思维已经从根本上改变了我们对一些基本概念的理解，如随机性、秘密、证据、知识、共谋和隐私。这项基础性工作是计算机安全产业发展的关键组成部分，由他的专利和创业公司推动。他的工作也对计算机科学和数学的其他研究领域产生了巨大的影响。

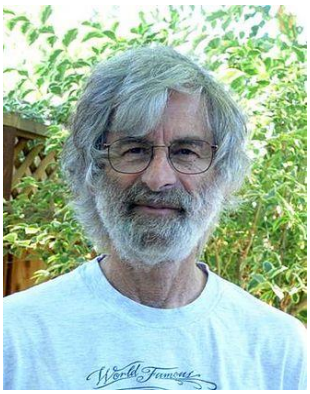


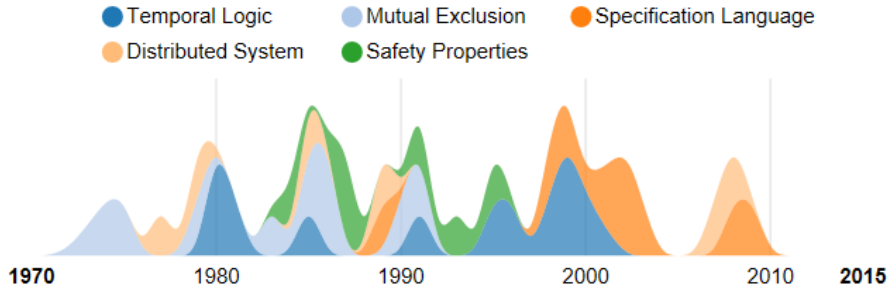
Micali 与 Goldwasser 的合作使得密码学成为一门精确的科学。他们的第一篇论文是在研究生时写的，其主题是“概率加密”，是计算机科学史上最有影响力的论文之一。它为成千上万的研究人员奠定了基础。另一个具有深刻影响的学术贡献来自 Micali 与 Goldwasser 和 Rackoff 的联合论文中，这篇论文关注了“交互式证明”领域，通过允许相互作用、随机化和容错极大地丰富了交互式证明的效用。在过去的几年里，Micali 把注意力转向了博弈论，尤其是致力于开发一种更强大的、考虑到串谋和信息安全在内的机制。

Micali 一项突出贡献在于设计了 Algorand 算法。能够扩展的共识算法是区块链获得成功关键要素之一，Micali 设计的 Algorand 算法则是共识算法中的重要创新。Algorand 算法是 PoS 的一种变形，PoS 使用了密码技术来随机选择那些负责将下一个区块（或交易）添加到区块链中的参与者，而 Algorand 算法利用了被 Micali 称为“加密抽签”的方法来选择参与者来创建和验证区块。通过加密抽签，Algorand 算法在理论上可以扩展需求，同时提升安全性和计算速度，以期实现“所有人都拥有相同网络访问权限”[17]的愿景。

[17] http://www.8btc.com/scalable-blockchain-consensus-turing-award-winner

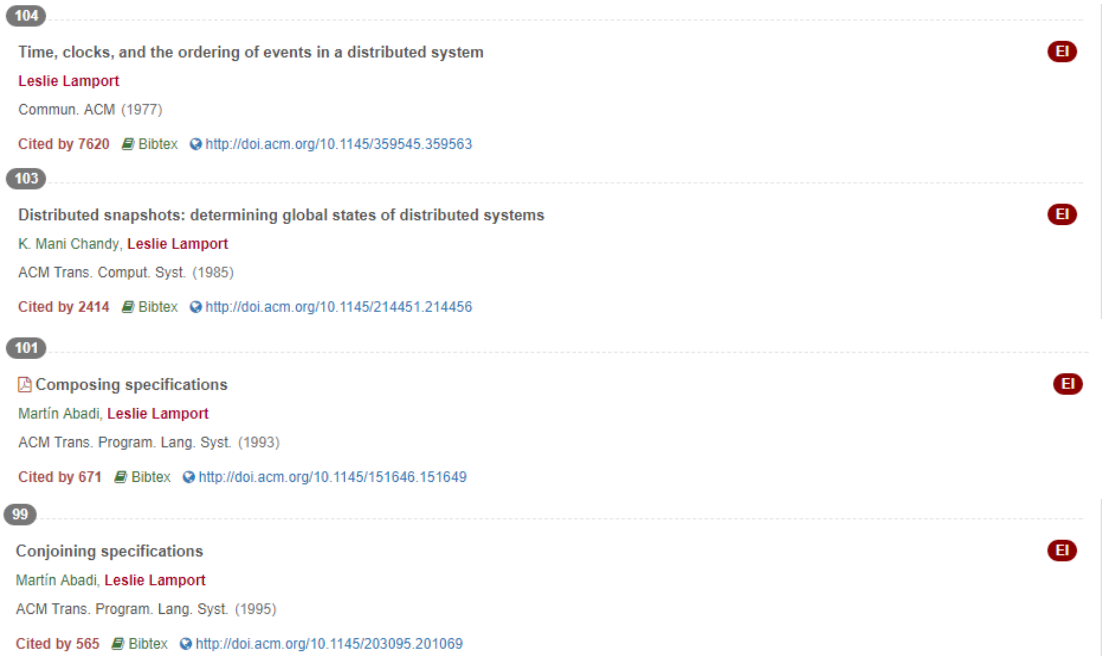
Leslie B. Lamport





Leslie B. Lamport 出生于 1941 年 2 月 7 日，美国计算机科学家，2013 年图灵奖得主。Lamport“对分布式和并发系统的理论和实践做出了重要贡献，尤其是在因果关系、逻辑时钟、安全与活力、复制状态机和顺序一致性等方面”。他设计并开发了正式的建模和验证协议，以提高真正的分布式系统的质量和计算机系统的正确性、可靠性。

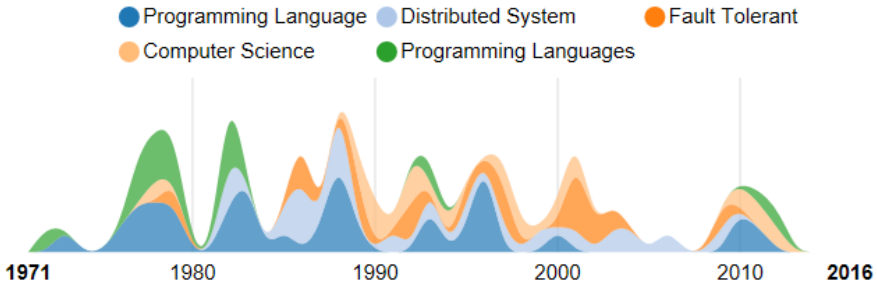
计算机领域科学家及行业领军人物对 Lamport 的工作做出了极高的评价。微软创始人比尔·盖茨说道：“作为一名伟大的科学家，图灵奖的荣誉 Lamport 当之无愧。作为一名带头人，他界定了分布式计算的许多关键概念，并让今天执行关键任务的计算机系统成为可能，莱斯利的伟大不仅局限于计算机科学领域，而且还体现在努力让世界变得更加安全。世界各地无数人受益于他的工作，却从未听说过他的名字。在我看来，这个奖项也是对微软研究院非凡工作的认可，这里已经成为立志克服业内最难挑战的科学家和工程师们的理想家园。当我们鼓励全球最强大脑都来超越未知的可能时会发生什么？Lamport 就是一个很好的例子。”微软新英格兰研究院技术院士、1992 年图灵奖得主 Butler Lampson 同样指出：“Lamport 对并发系统理论和实践在质量、范围和重要性上的贡献都是难以超越的。它们完全可以和 Dijkstra、Hoare、Milner 和 Pneuli 等所有前辈图灵奖得主的成就相提并论。虽然他能像这些前辈一样做好理论研究，但他最大的优点是作为一名应用数学家，十分了解如何利用数学工具来解决具有非凡现实意义的问题。



Lamport 毕业于布朗克斯高等科学学院，在高中时期他与同伴四处搜寻废弃真空管搭建电路，显现出了对计算机科学的浓厚兴趣。这种对计算机科学的热情在他的科研生涯中始终不曾泯灭。1960 年，Lamport 获得麻省理工学院的数学学士学位，1963 年和 1972 年分别从布兰迪斯大学获得数学硕士和数学博士学位。他在 1978 年发表的论文《分布式系统内的时间、时钟事件顺序（Time, Clocks, and the Ordering of Events in a Distributed System）》成为计算机科学史上被引用最多的文献。他为“并发系统的规范与验证”研究贡献了核心原理。Lamport 提出的分布式计算机系统理论为这个学科未来的发展奠定了坚实的基础。

Lamport 的著作包括《时间、时钟和分布式系统中的事件排序》《复制数据库的维护》《Dijkstra 并行编程问题新解》《拜占庭将军问题》等。2000 年，他凭借《时间、时钟和分布式系统中的事件排序》论文获得 ACM 分布式计算原理研讨会首届有影响力论文奖，2004 年凭借与计算机科学有关的信息处理领域突出贡献荣获 IEEE Emanuel R. Piore 奖。他曾三次获得 ACM SIGOPS 荣誉大奖。该奖项旨在表彰发表至少 10 年、在操作系统领域最有影响力的论文。同时，他在 2008 年荣获 IEEE 计算机科学逻辑研讨会（LICS）最经得起时间考验奖。该奖项每年颁发一次，旨在表彰 20 年以前发表并经得住时间考验的 LICS 论文。

Barbara Liskov



Barbara Liskov 是美国具有影响力的女性科学家之一。她 1939 年 11 月 7 日出生于加利福尼亚洛杉矶，现任麻省理工学院教授与福特工程学院电气工程和计算机科学系工程学教授。她的突出贡献在于开发 Liskov 替代原则，是美国最早获得计算机科学博士学位的女性之一，也是 2008 年图灵奖的获得者。

1961 年，Liskov 在加州大学伯克利分校攻读数学专业，获得数学学士学位。在校期间，她是数学专业仅有的两名女生之一。从伯克利毕业后，她继续申请伯克利和普林斯顿的研究生数学课程。由于当时普林斯顿大学并不接受女生学习数学专业，她最终没有继续数学研究，而是搬到波士顿，开始在 Mitre 公司工作。正是在那里，她对计算机和编程产生了兴趣。之后，她决定重返校园，再次申请伯克利分校，同时也申请了斯坦福大学和哈佛大学。1968 年，她获得了斯坦福大学的学位，成为美国第一批获得计算机科学系博士学位的女性。在斯坦福大学，她和约翰·麦卡锡一起工作，并在人工智能领域进行初步探索。

328

Practical byzantine fault-tolerance

miguel castro, barbara liskov,

OSDI (2000)

Cited by 1337 Bibtex http://doi.acm.org/10.1145/296806.296824

327

A behavioral notion of subtyping

Barbara H. Liskov, Jeannette M. Wing

ACM Trans. Program. Lang. Syst. (1994)

Cited by 1116 Bibtex http://doi.acm.org/10.1145/197320.197383

326

Practical byzantine fault tolerance and proactive recovery

Miguel Castro, **Barbara Liskov**

ACM Trans. Comput. Syst. (2002)

Cited by 1020 Bibtex http://doi.acm.org/10.1145/571637.571640

325

Abstraction mechanisms in CLU

B. Liskov, A. Snyder, R. Atkinson, C. Schaffert

Commun. ACM (1977)

Cited by 812 Bibtex http://doi.acm.org/10.1145/359763.359789

324

Abstraction mechanisms in CLU

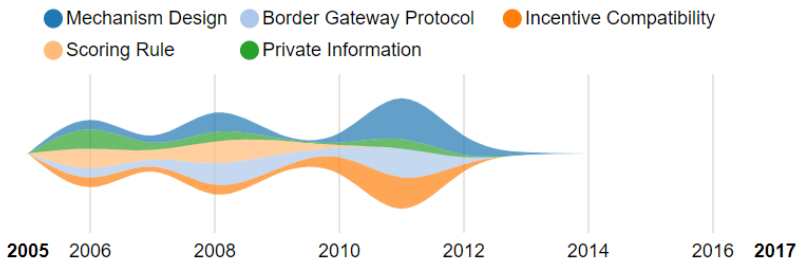
Barbara Liskov, Alan Snyder, Russell Atkinson, Craig Schaffert

Proceedings of an ACM conference on Language design for reliable software (1977)

Cited by 812 Bibtex http://dx.doi.org/10.1145/800022.808322

Liskov 领导了许多重要的项目，包括金星操作系统（Venus Operating System）：一个小型的、低成本的、交互式的分时系统。在 Jeannette Wing 的帮助下，她开发了一种特殊的亚型定义，即 Liskov 替代原则。她领导着麻省理工学院的编程方法论小组，其目前的研究重点是拜占庭容错和分布式计算以及实用拜占庭容错（PBFT）。2004 年，Liskov 因“对编程语言、编程方法和分布式系统的基本贡献”获得了约翰·冯·诺伊曼奖章。Liskov 也是 2008 年图灵奖的获得者，ACM 表彰了她对“编程语言和系统设计，特别是与数据抽象、容错和分布式计算相关”的实际和理论基础的贡献。2012 年，她入选国家发明家名人堂。

Aviv Zohar



Aviv Zohar 是希伯来大学工程与计算机科学学院的副教授，QED-it 的首席科学家。2013 年 12 月，他与 Yonatan Sompolinsky 共同发表的论文中，提出了（GHOST）协议。其中介绍了使用 GHOST 协议的 BlockDAG 结构——从本质上将比特币区块链架构变成了树结构，继而提高了安全性和交易时间。2018 年 2 月基于 SPECTRE 项目提出了新的扩容协议 PHANTOM。以上三项协议对区块链行业影响重大。

60

Secure High-Rate Transaction Processing in Bitcoin. EI

Yonatan Sompolinsky, **Aviv Zohar**

Financial Cryptography (2015)

Cited by 230 Bibtex http://dx.doi.org/10.1007/978-3-662-47854-7_32

59

On bitcoin and red balloons EI

Moshe Babaioff, Shahar Dobzinski, Sigal Oren, **Aviv Zohar**

Proceedings of the 13th ACM Conference on Electronic Commerce (2012)

Cited by 179 Bibtex http://arxiv.org/abs/1111.2626

58

Eclipse Attacks on Bitcoin's Peer-to-Peer Network. EI

Ethan Heilman, Alison Kendler, Aviv Zohar, Sharon Goldberg

IACR Cryptology ePrint Archive (2015)

Cited by 142 Bibtex http://dl.acm.org/citation.cfm?id=2831152&preflayout=flat

57

Complexity of strategic behavior in multi-winner elections EI

Reshef Meir, Ariel D. Procaccia, Jeffrey S. Rosenschein, **Aviv Zohar**

J. Artif. Intell. Res. (JAIR) (2008)

Cited by 133 Bibtex http://dx.doi.org/10.1613/jair.2566

3.3 博弈论

■ 3.3.1 博弈论概述

博弈论，也称为“对策论”“赛局理论”，是研究决策主体行为发生直接相互作用的时候的决策以及这种决策的均衡问题，具有斗争或竞争性现象的数学理论和方法。博弈论考虑游戏中的个体的预测行为和实际行为，并研究它们的优化策略。

不同历史时期、不同地区的国家对博弈论的理解有较大差异。最初，博弈被视为与“赌博”相关，而后成为数学的分支学科，博弈论被用于分析经济现象，随后又被理解为策略互动、思维方式和研究工具。法国博弈论专家克里斯汀·蒙特（Christian Montet）和丹尼尔·塞拉（Daniel Serra）在《博弈论与经济学》专著中这样定义：“博弈”这个词应理解为明智的、

理性的个人或群体间冲突与合作的情形[18]；1994 年诺贝尔经济学奖获得者豪尔绍尼（John C. Harsanyi）在获奖辞中给出这样的解释：“博弈论是关于策略相互作用的理论，就是说，它是关于社会形势中理性行为的理论，其中每个局中人对自己行为的选择必须以他对其他局中人将如何反应的判断为基础”。2005 年诺贝尔经济学奖获得者罗伯特·奥曼（Robert J. Aumann）将“博弈”定义为策略性的互动决策[19]。

近代对于博弈论的研究，开始于冯·诺伊曼（Von Neumann）。1928 年，冯·诺依曼证明了博弈论的基本原理，从而宣告了博弈论的正式诞生。1944 年，冯·诺依曼和摩根斯坦共著的划时代巨著《博弈论与经济行为》将二人博弈推广到 n 人博弈结构并将博弈论系统的应用于经济领域，从而奠定了这一学科的基础和理论体系。1950 至 1951 年，纳什利用不动点定理证明了均衡点的存在，为博弈论的一般化奠定了坚实的基础，其开创性论文《n 人博弈的均衡点》（1950）[20]，《非合作博弈》（1951）[21]，给出了纳什均衡的概念和均衡存在定理。

此外，提到博弈论，就不能绕开纳什与纳什均衡（Nash Equilibrium）。所谓纳什均衡，指的是在策略组合上，任何参与人单独改变策略都不会得到好处；也就是说，如果在一个策略组合上，当所有其他人都不改变策略时，没有人会改变自己的策略，则该策略组合就是一个纳什均衡。纳什均衡的重要性体现在两方面：其一，纳什均衡是其他所有均衡概念的基础，博弈逻辑的核心就是寻求纳什均衡；其二，纳什均衡描述了参与者为了达到自身利益的最大化，必须采用合作来达到一直稳定最大收益函数，每个参与人的策略是对其他参与人策略的最优反应。纳什均衡策略比冯·诺依曼的标准更加一般化，开启了非合作博弈的里程碑。

今天，博弈论已发展成一门较完善的学科。博弈论提供了一种计算各种可能决策所产生效益的数学方法，该理论为在各种竞赛性场合做出最佳决定建立了一套具体的数学公式。正如经济学家赫伯特·金迪斯（Herbert Gintis）所说，博弈论是我们“研究世界的一种工具”。但它不仅仅是一种工具，“它不仅研究人们如何合作，而且研究人们如何竞争”。同时，“博弈论还研究行为方式的产生、转变、散播和稳定”。

博弈论的研究价值及现状诺贝尔经济学奖获得者保罗·萨缪尔森（Paul Samuelson）曾说过：“要想在现代社会做一个有文化的人，你必须对博弈论有一个大致了解”。我国最权威的

[18] Montet C, Serra D. Game theory and economics[M]. New York: Palgrave macmillan, 2003.

[19] Aumann R J. Game theory[J]. The New Palgrave Dictionary of Economics, 2017: 1-40.

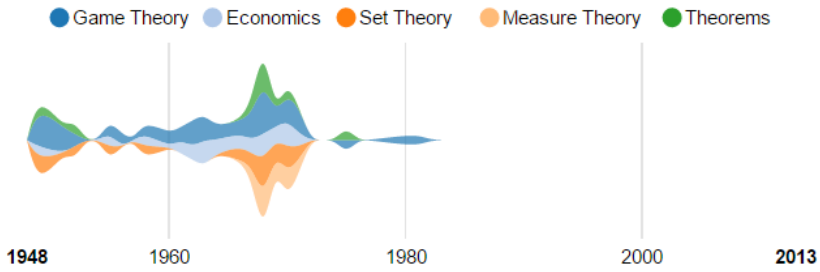
[20] Nash J F. Equilibrium points in n-person games[J]. Proceedings of the national academy of sciences, 1950, 36(1): 48-49.

[21] Nash J. Non-cooperative games[J]. Annals of mathematics, 1951: 286-295.

博弈论专家、北京大学张维迎教授这样描述博弈论的研究价值:“如果对博弈论不了解的话，那么我们在经济学、法学、社会学、政治学等学科上都很难对前沿问题进行研究。”

■ 3.3.2 博弈论代表学者

Lloyd S. Shapley



Sharpley 是美国著名数学家、经济学家。2012 年，他凭借“稳定分配理论和市场设计实践”与哈佛大学教授 Alvin E. Roth 共同分享当年的诺贝尔经济学奖。其主要贡献包括 Shapley 价值、随机对策理论、Bondareva-Shapley 规则、Shapley-Shubik 权力指数等。Shapley 毕业于普林斯顿大学和哈佛大学，任加州大学洛杉矶分校数学与经济学名誉教授，对数理经济学，特别是博弈论理论，作出了突出贡献。他早期与 R.N.Snow 和 Samuel Karlin 在矩阵对策上的研究如此彻底，以至于此后该理论几乎未有补充。他在功用理论发展上扮演关键角色，为冯·诺依曼—摩根斯坦稳定集（Von Neumann-Morgenstern Stability Set）存在问题的解决奠定了基础，在冯·诺依曼和摩根斯坦之后，Shapley 被认为是博弈论领域最出色的学者。80 多岁高龄时，Shapley 依旧笔耕不辍，提出多人效用、权力分配理论。

98

Potential Games EI

Dov Monderer, **Lloyd S. Shapley**

Games and Economic Behavior (1996)

Cited by 3025 Bibtex http://dx.doi.org/10.1006/game.1996.0044

97

On market games EI

Lloyd S Shapley, Martin Shubik

Journal of Economic Theory (1969)

Cited by 484 Bibtex http://dx.doi.org/10.1016/0022-0531(69)90008-8

96

The Shapley value : essays in honor of Lloyd S. Shapley

alvin e roth, **lloyd s shapley**

The Economic Journal (2005)

Cited by 457 Bibtex

95

Cores of convex games

Lloyd S. Shapley

International Journal of Game Theory (1971)

Cited by 410 Bibtex http://link.springer.com/article/10.1007/BF01753431

94

Fictitious Play Property for Games with Identical Interests EI

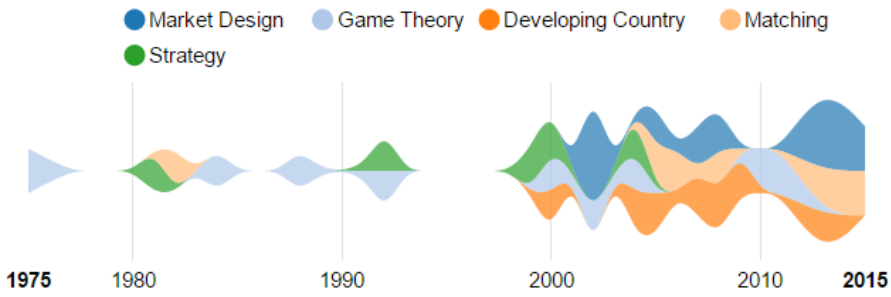
Dov Monderer, **Lloyd S. Shapley**

Journal of Economic Theory (1996)

Cited by 397 Bibtex http://dx.doi.org/10.1006/jeth.1996.0014

谈起 Shapley，除了他在博弈论理论上的突出贡献，还有他深厚的中国情结。1943 年，作为哈佛大学数学系的一名本科生，Shapley 应征入伍成为一名空军中士，并很快奔赴中国成都战区，与中国军民并肩抗击过日本侵略军。Shapley 发挥他天才的数学才能，破解气象密码，获得铜星奖章（Bronze Star）。战争结束后，Shapley 回到哈佛大学继续念书。2002 年 8 月 14 日到 17 日，Shapley 因为参加青岛大学承办的“2002 国际数学家大会‘对策论及其应用’卫星会议”再次来到中国。青岛大学的高红伟教授作为会议组织者，至今还留着一份为 Shapley 办理入境签证时青岛市政府出具的邀请函原件，“Shapley 被誉为博弈论的无冕之王，精通博弈理论，但却不太喜欢现代的信息技术，不喜欢使用电子邮件与别人进行沟通”，高红伟教授说，昔日的英武少年已成为一个科学老顽童。青岛之行，Shapley 再次讲述起他与中国将近 70 年的那段渊源时，依然激动。

Alvin E. Roth



Roth 是美国经济学家，1971 年毕业于哥伦比亚大学运筹学专业，1988 年赴哈佛大学任教，在博弈论、市场设计和实验经济学领域做出了突出贡献。

1951 年，Roth 出生在美国一个犹太裔家庭，这个以教育和勤奋为代表性格的民族文化，令他从小便得到熏陶，并显现出在数学、逻辑等方面的过人之处。但令人惊愕的是，他其实是一个高三从纽约皇后区退学的孩子。在解释自己的退学原因时，Roth 表示自己厌倦了课程内容，“我那时缺乏动力”。此后，他来到哥伦比亚大学在进行了短期的周末工程班学习后，Roth 听从教授的建议考上大学开始本科生涯。1971 年，Roth 从哥伦比亚大学本科毕业，获得工程学学士学位。在大学校园，他对运筹学这门当时并不是“显学”的年轻学科产生了浓厚兴趣，为了在运筹学领域进行深入探索，他来到斯坦福大学，于 1973 年和 1974 年先后获得运筹学硕士、博士学位，此时，Roth 只有 23 岁。离开斯坦福之后直到 1982 年，Roth 一直在伊利诺斯大学任教。此后他在匹兹堡大学担任安德鲁-梅隆经济学教授直到 1998 年，之后他加入哈佛大学并在此工作至今。

336

The handbook of experimental economics

John H. Kagel, **Alvin E. Roth**

(1995)

Cited by 3080 Bibtex http://dx.doi.org/10.2307/1243316

335

Two-sided matching

alvin e roth, marilda sotomayor

(1992)

Cited by 2829 Bibtex

334

Predicting How People Play Games: Reinforcement Learning in Experimental Games with Unique, Mixed Strategy Equilibria

ido erev, **alvin e roth**

The American Economic Review (1998)

Cited by 1881 Bibtex

333

Learning in extensive-form games: Experimental data and simple dynamic models in the intermediate term EI

Alvin E. Roth, Ido Erev

Games and Economic Behavior (1995)

Cited by 1716 Bibtex http://dx.doi.org/10.1016/S0899-8256(05)80020-X

332

Bargaining and Market Behavior in Jerusalem, Ljubljana, Pittsburgh, and Tokyo: An Experimental Study

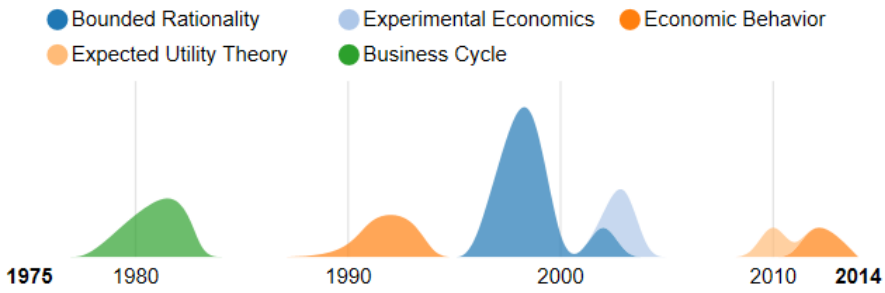
ALVIN E. ROTH, VESNA PRASNIKAR, MASAHIRO OKUNO-FUJIWARA, SHMUEL ZAMIR

Econometrica (1995)

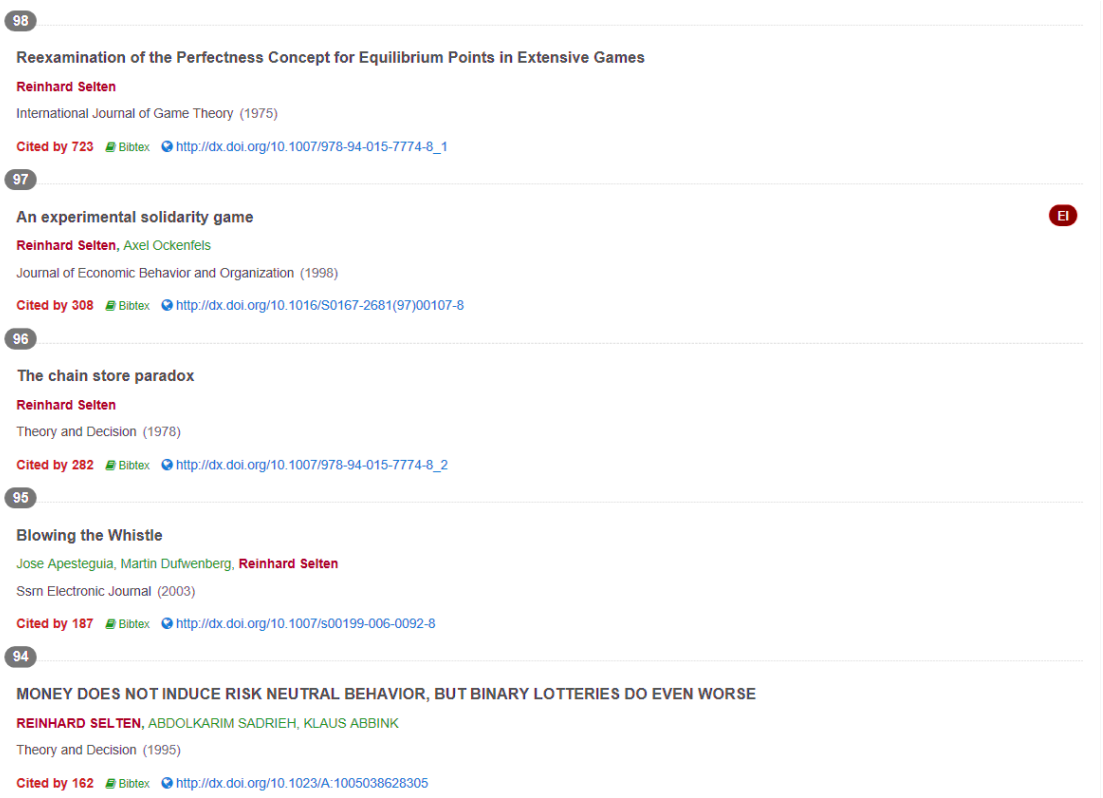
Cited by 1590 Bibtex

Roth 在经济学领域的突出贡献不仅在于丰富了理论体系，更在于运用到现实生活中解决实际问题。Roth 最令人关注的贡献包括医学院毕业生住院培训分配系统设计、纽约市高中匹配系统设计等。他利用递延接受算法（deferred acceptance algorithm）重新设计这些系统，每年帮助超过 20000 名医生匹配到心仪的医院作为职业生涯的起点和 90000 名高中生顺利选择到向往的学校。Roth 表示，“有些人觉得经济学领域有各种优秀的工具和技巧，唯独缺乏有趣的问题。但我却发现，既不失趣味又有现实意义的重要问题遍地都是，我们应当努力利用现有的工具解决它们。”

Reinhard Selten

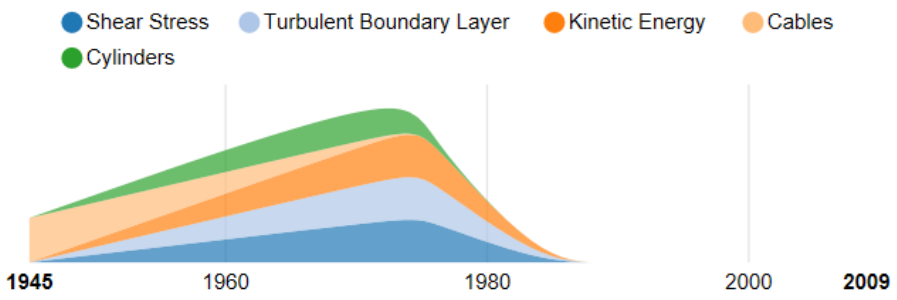


Selten 是 1994 年诺贝尔经济学奖得主，子博弈精炼纳什均衡创立者，代表著作有《价格制定者厂商的一般均衡》（1974）、《博弈论均衡选择的一般理论》（1988）等。1951 年，Selten 进入德国法兰克福大学攻读数学，在 1957 年硕士毕业后从事博弈论及其应用、实验经济学等博弈论的学术研究。



60 年代早期，Selten 进行了寡头博弈实验。Selten 在实验中发现了一个自然均衡，但同时发现这个博弈有许多其他的均衡。为了描述他的发现，Selten 定义了子博弈精炼（sub-game perfectness）的概念，并于 1965 年发表了他最著名的博弈论论文《一个具有需求惯性的寡头博弈模型》。Selten 当时并没有想到他的这篇文章后来会被广泛引用，并成为了子博弈精炼均衡（sub-game perfect Nash equilibrium）的正式定义，同时为后来获得诺贝尔经济学奖奠定了基础。1975 年，Selten 发表论文《扩展式博弈精炼均衡概念的重新考察》。在论文中，Selten 提出了著名的“颤抖手均衡”（trembling hand equilibrium）概念。在与生物学家的交流中，Selten 意识到博弈论能应用于生产学的研究。在一些年轻的数学家的帮助下，Selten 熟悉了进化稳定（evolutionary stability）的概念和含义，对生物博弈理论产生了极大的兴趣，并对扩展式博弈形式下进化稳定进行了考察，写出一系列的论文。Selten 认为，与不同领域的具有较少数学训练的科学家的合作是很有意义的，他也积极地尝试着与不同学科的学者开展交叉研究。Selten 与政治学家研究了国际冲突的博弈论模型，并发现政治学家能根据经验事实作出正确的判断，而不受数学模型的制约；他还与植物学家研究了蜜蜂传花粉过程的理论模型。尽管 Selten 非常喜欢比勒菲尔德大学的学术交流气氛，但他想建立一个实验经济学研究的计算机实验室，而波恩大学愿意为此提供更好的物质条件，于是 Selten 于 1984 年来到波恩大学，一直工作至今。

John F. Nash



提起纳什，人们自然会想到电影《美丽心灵》中记录的他的传奇一生。纳什生于 1928 年，从事博弈论、微分几何与偏微分方程领域的研究，是纳什均衡创始人。1950 年，22 岁的纳什以非合作博弈（Non-cooperative Games）为题写出 27 页博士论文毕业，但令人未曾想到的是，他在那篇仅仅 27 页的博士论文中提出的一个重要概念，也就是后来被称为“纳什均衡”的博弈理论，成为他今后的一系列成就的基石。

10

Unsteady Turbulent Boundary Layers in Two-Dimensional, Incompressible Flow

John F. Nash, Lawrence W. Carr, Robert E. Singleton

Aiaa Journal (1975)

Cited by 3 Bibtex http://dx.doi.org/10.2514/3.49657

9

Method for Calculating Unsteady Turbulent Boundary Layers in Two-and Army Three-Dimensional Flows

Robert E. Singleton, **John F. Nash**

Aiaa Journal (1974)

Cited by 2 Bibtex http://dx.doi.org/10.2514/3.49303

8

Turbulent-Boundary-Layer Behaviour and the Auxiliary Equation

John F. Nash

Cited by 1 Bibtex

1958 年，纳什开始显露出精神失常的症状，继而产生严重的幻听与幻觉，不得不接受反复的治疗。纳什的精神状况使得他与 Fields 奖和诺贝尔经济学奖失之交臂，也渐渐淡出了学术界的视野。这样的状态持续了将近 30 年，直至 80 年代末期，纳什的症状渐渐减轻，才迎来了他生命中最重要的褒奖。纳什均衡开始走进人们的视野，成为各类期刊、教材与论文的关注对象，非合作博弈均衡的影响力越来越大。由于在非合作博弈均衡上的突出贡献，纳

什在 1994 年与另两位经济学家 Selten 与 Harsanyi 共同获得诺贝尔经济学奖。此时，年届 66 岁的纳什重新开始了他的学术生涯，在他的自传中，纳什写道：“从统计学上看，没有任何一个已经 66 岁的数学家或科学家能通过持续的研究工作，在他或她以前的成就基础上更进一步。但是，我仍然继续努力尝试。由于出现了长达 25 年部分不真实的思维，相当于提供了某种假期，我的情况可能并不符合常规。因此，我希望通过至 1997 年的研究成果或以后出现的任何新鲜想法，取得一些有价值的成果”。

3.4 性能提升办法

■ 3.4.1 Thunder

Thunder 是一个完全去中心化，EVM 兼容的区块链，同时它具有中心化的高性能优势。Thunder 是 Elaine Shi 和 Rafael Pass 教授搭建的下一代高速、低延时的区块链应用开发平台，该平台彻底解决了第一代第二代系统存在的性能瓶颈和功能扩展问题。

Thunder 是一个新的区块链，能够实现高吞吐量及快速确认时间（两秒内即时确认），可承受高达 50%的攻击，直接支持 EVM 智能合约。也就是说现有基于以太坊的 DApps，几乎不需要修改就能使用 Thunder 主链，理论上来说较为安全可靠。

Thunder 使用新范式大规模分布式协议。它的共识协议结合了（1）慢速链：可以是任何标准区块链，如以太坊，或权益证明区块链；（2）高速链：由利益相关者委员会和称为“加速器”组成的特殊社群执行投票。几乎所有的交易都可以在高速链上立即确认，而无需等待慢速链缓慢地增长。万一高速链失效时，有一个可验证的安全机制可以回退到慢速链，从那里启动并回到高速链。加速器的唯一工作是加速交易的确认，即使是恶意的加速器也不会损害区块链的安全性或分散性。Thunder 是现有的比较安全的区块链解决方案。

■ 3.4.2 Celer Network

Celer Network 是一种连贯的技术和经济架构，可通过链外扩展技术实现互联网规模的公共区块链。它可以扩展到每秒数十亿次交易。通过成为第一个具有互联网级可扩展性的非连锁运营网络，Celer Network 可能成为分布式账本领域最具可扩展性的连锁商。

Celer Network 使用分层架构来确保稳定性和可扩展性。虽然技术性很强，但它可支持 DApp 状态的转换。它不仅超越了传统的简单支付概念，同时还提供许多新功能。在可扩展性方面，Celer Network 的目标是实现 15 倍于当前最先进解决方案的吞吐量。一些项目旨在每秒处理超过 100 万次传输，但现在实现这一目标还是很有难度的，如果成功的话，Celer

Network 将会产生较大的影响。（第一次可证明的最优状态路由算法，其传输吞吐量比现有技术的解决方案高 15 倍）

Celer Network 是一个脱链的操作系统，简化了各种平台上脱链应用程序的开发和使用。此外，Celer Network 提出了原则性的链外加密经济学设计，以实现可扩展性平衡而做出权衡。

■ 3.4.3 Lightning Network

在不进行区块扩容的前提下，比特币借助名为 Lightning Network 技术来进行链下扩容，以此突破区块容量的上限。Lightning Network 是一个链下服务方案，它不发送任何货币，而是在第二层级中进行账本的变更并随后在第一层级中完成结算，从而避免数千次的、实际的资金转移。通过将资金发送到由多方掌管密钥的多重签名地址，Lightning Network 构建起一个支付渠道。

收付双方之间的交易在链下完成，无论这个交易渠道关闭时的余额是多少，这些余额都会被如数发回用户的钱包，这就是双向支付渠道的工作原理。Lightning Network 是一个典型的双向支付渠道网络。通过这个网络，用户可以与自己的承包商进行定期支付或每月结算。

虽然 Lightning Network 这个链下扩容方案独具创意，但它也因为固有的缺陷而遭到了批判。首先，用户必须支付费用才能开通一个支付渠道（类似于账户）。并且，由于在链下交易之前必须完成对多重签名地址的链上交易，因此用户在使用交易渠道之前还要等上一段时间。再者，在没有连接到最终收款方的情况下，支付路径有可能会出现问题。而如果其它人的连接情况不佳，支付就会失败。使用 Lightning Network 所面临的最大的一个问题是，用户的资金可能会被 Lightning Network 的节点窃取。另一个更大的风险是，Lightning Network 的钱包必须保持在线，以便接收资金。在用户脱机的情况下，支付可能就会出现问题，而一旦 Lightning Network 的节点下线，就会造成灾难性的后果。

■ 3.4.4 Algorand

Algorand 是 MIT 机械工程与计算机科学系 Silvio Micali 教授与其合作者（主要是纽约大学石溪分校陈静副教授）于 2016 年提出的一个区块链协议。Algorand 由 algorithm（算法）和 random（随机）两个词合成，意思是基于随机算法的公共账本协议（public ledger）。Algorand 针对比特币区块链系统的几个核心缺陷进行了改进。

Algorand 的目标是：

1.能耗低，不管系统中有多用户，大约每 1500 名用户中只有 1 名会被系统挑中执行长

达几秒钟的计算。

2.民主化，不会出现类似比特币区块链系统的“矿工”群体。

3.出现分叉的概率低于一兆分之一（即 10-18）。假设 Algorand 中平均每分钟产生一个区块（后文会给出有关测试数据），这个概率意味着平均每 190 万年出现一次分叉。

4.可拓展性好，交易的吞吐量和交易的速度都有着明显的提升。

Algorand 是一个公有链系统。用户（或者节点）加入 Algorand 不需要事先申请，可以随时加入。Algorand 对用户数量也没有任何限制。每个用户持有多个公钥。每个公钥均是一个电子签名机制的一部分，也就是有一个与之对应的私钥。每个公钥对应着一定数量的货币。每笔交易实际上是一个电子签名，该电子签名将一定数量的货币从某一个公钥转移给另一个公钥，并用前一个公钥对应的私钥进行加密。不难看出，Algorand 的这些设计，与比特币是一样的。Algorand 要求系统中 2/3 的货币由诚实用户掌握。诚实用户的含义是其行为遵守有关指引（主要指拜占庭共识协议，见下文），并且能完美地发送和接收消息。诚实用户以外的被称为恶意用户，恶意用户的行为可以任意偏离有关指引。对恶意用户，Algorand 假设他们由一个“敌对者”（adversary）控制，“敌对者”能发起强大攻击。

同时，这里介绍一篇最新的论文。

- **Scaling Nakamoto Consensus to Thousands of Transactions per Second**

  Chenxing Li,Peilun Li,Wei Xu，Fan Long,Andrew Chi-chih Yao

文章提出了一种快速、可扩展、分散的区块链系统 Conflux，它可以很好地处理块，而不会丢弃任何一部分。Conflux consensus protocol 将块之间的关系表示为直接无环图，并对块的总顺序达成一致。然后，Conflux 从 block order 中决定性地得出了一个交易总订单作为区块链分类帐。作者评估了在 Amazon EC2 集群上的 Con- flux，最多有 20k 个完整节点。Conflux 实现了 5.76GB/h 的吞吐量，同时在 4.5-7.4 分钟内确认交易。对于典型的比特币交易，吞吐量相当于每秒 6400 个事务。实验结果还表明，当运行 Conflux 时，吞吐量的瓶颈不再是写上一致协议，而是单个节点的处理能力。

3.4.5 SPECTRE & PHANTOM

SPECTRE 和 PHANTOM 两大协议是由 Aviv Zohar 和 Yonatan Sompolinsky 共同提出的。两项协议均是基于 DAG 区块链的协议。SPECTRE 协议的提出要稍早于 PHANTOM,扩容协议 PHAMTOM 于 2018 年 2 月被公布了技术细节。PHAMTOM 作为新的区块链可伸缩性协议，该协议旨在提供网络能够在任何情况下确定其安全保障——包括智能合约在内的交易。

PHANTOM 该协议是建立在 SPECTRE 项目的基础上的，它偏离了比特币的通用块链结构，具有可伸缩行的“非循环块链”（BlockDAGs）。这项技术被协议该研发团队描述为“Satoshi 链的泛化，它更适合快速或大型块链的设置。”但与 SPECTER 协议不同的是，“PHANTOM”在 BlockDAG 协议上使用的是一种所谓“贪婪算法”，通过“区分通过诚实节点开采证券的区块和通过偏离 DAG 挖矿协议的非协作节点开采出来的区块”，来创建出一套更线性的区块结构。

区块链应用场景

application 4

4.1 数字货币

■ 4.1.1 数字货币概述

2013 年基于区块链技术的数字货币受到了各国央行的重视，可以说数字货币是迄今为止最成功的区块链应用场景，其中，比特币、以太坊、瑞波币、比特币现金和莱特币是数字货币及其交易平台的典型代表。数字货币不是凭空出现的，它源自于电子支付，由电子货币、虚拟货币演化而来，并逐渐与电子货币和虚拟货币分离。数字货币的出现是多方面因素共同作用的结果。首先，用数字货币代替纸币，交易快捷方便；其次，利用区块链技术挖矿方式解决数字货币滥发问题，保证货币币值的稳定；最后，数字货币可以实现跨界的统一使用，实现世界范围内的货币通用。

从本质上来说，数字货币并不具有价值，它是一种财富价值的序列符号，可以说，数字货币的发展并未脱离信用货币的范畴，作为一种信用货币，它仍然是是货币符号。数字货币要想了解数字货币就必须了解数字货币背后的锚定原理，数字货币作为信用货币的一种，没有实际价值，存在着容易超发的问题，因此数字货币发行的锚定物问题就相对重要起来，信息技术容量成为新时代数字货币较好的锚定物，数字货币基于区块链技术，以信息技术容量为限，采用技术锚定解决数字货币发行量问题。依据数字货币的设计规则，用户通过“挖矿”来获得数字货币，数字货币的价值则由“挖矿”消耗的计算处理能量转化而来，这样就实现了数字货币的发行量与网络技术处理能力挂钩。挖矿（Mining）就是指产生新区块并计算随机数的过程。具体而言，比特币挖矿分为六步。第一，计算机根据之前产生的最后一个主区块链的内容为基础，计算一个哈希值；第二，计算机在接受广播来的交易单并逐笔校验交易的准确性后，将没有被列入之前区块的交易进行组合，产生一个新区块；第三，计算机生成一个任意随机数；第四，计算机将前三部得出的哈希值和随机数作为输入，放入 SHA256 哈希函数中，计算得到长度为 256 的一个二进制数；第五，检查该二进制数前 n 位是否符合要求；最后，若该二进制数前 n 位符合要求，则本轮挖矿结束，计算机会把新区块连同该随机数广播给网络上其他计算机，其他计算机以同样方式对随机数和新区块进行校验。若结果无误，则全网接受该新区块，将它连同之前的主区块链一起保存。若产生的随机数不符合要求，则回到第二步重新开始寻找随机数，直到成功经过校验。

目前，金融发展的趋势是“去中心化”和金融脱媒。去中心化是互联网发展中信息传递效率提高而形成的扁平化社会关系形态，区块链技术创新使“去中心化”的数字货币发行机制得以实现。但是，去中心化在依然存在很多问题，具体包括：一是市场垄断问题，目前货

币市场状况尚不符合私有货币理论自由竞争的前提；二是风险监管问题，货币体系需要及时的监管和调控来防范风险；三是数字货币如何公平有效的发行；四是技术革命对数字货币币值的影响。因此，去中心化的风险及监管问题还需进一步研究探讨。同时数字货币的设计理念还实现了三方模式到两方模式的突破。三方模式是传统货币体系的典型，借方和贷方通过银行这一中介方连接，借贷双方各自通过银行进行资金结算完成债权债务的转移。但在数字货币时代，Nakamoto 提出了两方模式，完全通过 p2p 实现的电子现金系统。数字货币在区块链技术创新的支持下具有基于账户和不基于账户两种。

但是早期的数字货币系统安全性得不到保障，需要解决两个问题，避免货币伪造和避免双重支付。2008 年 Nakamoto 提出了比特币的概念，比特币的核心支撑技术就是区块链，区块链技术为比特币系统解决了数字加密货币领域的一大难题：双重支付问题。双重支付问题，即利用数字货币的特性两次或多次使用“同一笔钱”进行支付。对双重支付问题的解决与比特币防伪技术紧密相关。比特币通过三方面努力解决双重支付问题。第一，比特币所有交易全网公开，每个账号中的比特币数量不是由一个数据表示的，而是根据历史交易得出的，并且，历史交易是经过全网公认的，这样保证了交易信息不被造假；第二，利用时间戳给交易赋予先后顺序，比特币系统中的每一笔交易都是根据上一笔交易生成的，时间顺序避免了双重支付的产生；第三，投入计算资源对交易进行确认，引入 PoW 投入算力打包交易，使得篡改或伪造信息在数学上无法或几乎不可能实现。在这种分布式节点验证和工作量证明的保障下，比特币在信息传输的过程中完成了价值转移，有效避免双重支付问题。

■ 4.1.2 数字货币分类

■ 纯数字货币

比特币（Bitcoin, BTC）

比特币是一种点对点（P2P）形式的数字货币，利用 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。P2P 传输使其具有去中心化的特点，每个节点中都保存着一份区块链账本数据，理论上，矿工可以从任意区块开始向下挖掘新的区块，同时，P2P 去中心化特征和算法可以确保无法通过大量制造比特币来人为控制币值。比特币采用工作量证明和最长链机制两种共识来决定货币分配并保证区块链是有效的。比特币是自带安全属性的数字货币，被称之为“密码学货币”，该币采用非对称曲线加密算法和哈希算法两种。“非对称密码”是当代密码学最核心的突破，保证了比特币加密和解密采用两种密码，也就是“公钥-私钥”密码不同，私钥可推出公钥，而反之则不能。哈希算法的引入解决了双重花费的问

题，避免了僵尸节点对不合格交易的随意确认。

比特币依靠特定算法并通过大量计算产生，但去中心化特征和算法本身使得比特币数量被永久限制在 2100 万个。因此比特币具有极强的稀缺性，也就蕴藏着巨大的升值空间

比特币的技术特点也带来一些缺陷：交易时间长，每笔交易需要六次区块链确认才能不可逆，不能满足小额交易需要；比特币的匿名性导致丢失和被盗都难以找回。

比特币现金（Bitcoin Cash, BCH）

比特币现金作为比特币的硬分叉币种，遵循比特币创始人提出的通过链上扩容实现全球普及的路线图，区块大小最高支持提升到 8M，删除了隔离验证（SegWit）。相比比特币，比特币现金每个区块可以容纳更多的交易，在一定程度上降低了交易拥堵性。

BCH 采用新的签名哈希类型，提供了重放攻击保护、改善硬件钱包安全性，也解决了二次哈希问题。BCH 还采用新的难度调整算法（DAA），响应式的 POW 难度调整允许矿工按其意愿从旧的比特币链迁移至新链，同时提供保护以抑制算力过度波动。

比特币现金诞生之日曾面临巨大的争议，是比特币的新分支还是另外一种“山寨币”，业内论调不一，但这并不妨碍其在投资者中地位的攀升，市值一度升至数字货币第三位。

比特币现金并非是首个硬分叉币种，以太坊经典也属于硬分叉货币。在数字货币领域，开发者意见分歧可能导致区块链分裂，而比特币现金和以太坊经典的成功催生出更多的分叉货币。2017 年 11 月 SegWit2x 分叉计划取消后诞生了比特币黄金、比特币钻石、闪电比特币、超级比特币。2018 年 4 月 XMR 修改核心共识算法分裂出 XMR 及 XMC 两条区块链。

门罗币（Monero, XMR）

门罗币是基于 CryptoNote 协议的加密数字货币，着重于隐私、去中心化和可扩展性。CryptoNote 协议可以通过数字环签名提供更好的匿名性，并在区块链模糊化方面有显著的算法差异。

环签名（One-time Ring Signature）技术将签名者的公钥和另外一个公钥集合进行混合，然后再对消息进行签名，这样对于签名验证者来说，无法区分哪个公钥对应的是真正的签名者，实现了不可追踪性，从而为用户的交易信息提供了很好的隐私性。

门罗币采用了隐蔽地址（Stealth Addresses），每次发起一次交易都会先用接收者的公钥随机计算出一个临时中间地址，网络上的其它用户包括矿工都无法确认地址归属，从而保证了不可链接性。不过，这种做法导致公私钥长度变为原来的两倍，再加上环签名技术，签名的产生和验证过程复杂度都明显增加。

瑞波币（Ripple）

Ripple 是世界上第一个开放的支付网络，通过这个支付网络可以任意转账一种货币，包括美元、欧元、日元或者比特币。瑞波币是 Ripple 系统中唯一的通用货币，其不同于 Ripple 系统中的其他货币，其他货币比如 CNY、USD 不能跨网关提现的，换句话说，A 网关发行的 CNY 只能在 A 网关提现，若想在 B 网关提现，必须通过 Ripple 系统的挂单功能转化为 B 网关的 CNY 才可以到 B 网关提现。而瑞波币完全没有这方面的限制，它在 Ripple 系统内是通用的。

同比特币一样，Ripple 也是一种可共享的公共数据库，同时它也是全球性的收支总账，这个总账本分布在所有网络节点中并时刻保持同步。瑞波币提出一种共识算法，使一组节点能够基于特殊节点列表表达共识。允许 Ripple 网络中的所有计算机在几秒钟内自动接受对总账信息的更新，而无需经由中央数据交换中心。这意味着 Ripple 的交易确认时间仅为 3 至 5 秒，而比特币则需要 40 分钟。因此，瑞波币能让小型企业在几秒钟内就能收到客户的汇款，这种迅速到款的特性对管理企业的每日现金流有很大帮助。全球三大转账服务公司 UAE Exchange、MoneyGram 和 Western Union 都已经和 Ripple 建立合作探索基于 Ripple 区块链技术的支付项目。瑞波币是 Ripple 网络的基础货币，它可以在整个 Ripple 网络中流通，总量为 1000 亿，并随着交易的增多而逐渐减少。

莱特币（Litecoin, LTC）

莱特币在技术上与比特币具有相同的实现原理，但也做出一些改进。莱特币在工作量证明算法中使用了由 Colin Percival 首次提出的 Scrypt 加密算法，从而相比比特币更容易挖掘，交易速度提高，达到每 2.5 分钟就可以出来一个区块；同时为 Scrypt 算法开发出 FPGA（可编程逻辑门阵列）和 ASIC（专用集成电路），相比比特币的 sha256 更为昂贵；莱特币总产量为 8400 万个，是比特币网络发行货币量的四倍之多。

莱特币与比特币的技术相似性使其具有后者的弱点，包括交易可锻性、区块扩容问题等，为此，莱特币已经在 2017 年成功应用隔离见证技术（SegWit），像 Lightning Network、MAST、机密交易、Schnorr 签名等这些技术一样最初的对象都是比特币。

■ 支持智能合约的货币

以太坊（Ethereum, ETH）

以太坊是一个开源的具有智能合约功能的公共区块链平台，是区块链 2.0 的典型代表，由其专用货币以太币提供去中心化的虚拟机（Ethereum Virtual Machine）来处理点对点合约。以太坊虚拟机（EVM），是以太坊的核心，EVM 可以执行任意算法复杂度的代码，以太坊虚

拟机（EVM）使用了 256 比特长度的机器码，是一种基于堆栈的虚拟机，用于执行以太坊智能合约。

以太坊使用混合型的共识协议，前期使用 PoW 挖矿算法，后续将逐步切换为 PoS 机制。PoS 基于矿工拥有的数字货币数量和持有时间进行分配，相比 PoW 能源成本更低，网络更高效，PoS 网络的安全由用户在网络上持有 token 来保证，而不是用户提供算力来保证 PoW 网络的安全。PoS 机制下，拥有更多财富的个人比拥有较少财富的个人获得创建区块和交易费用的机会更大，这意味着将加大财富差距。

以太坊采用区块链的原理，允许在区块链上创建智能合约，这是其最大的特点。智能合约是一种应用，能够存储数据、封装代码、执行计算任务。目前以太坊支持 Solidity、Serpent 和 LLL 三种语言编写的智能合约，可以根据的习惯选择不同的高级语言，其中，Solidity 最为流行。

以太坊总量不设上限，据 stateofthedapps 网站 2018 年 3 月的统计，目前在全球已有 1252 个以太坊应用诞生，随着时间的推移将会有越来越多的项目在以太坊平台上构建。不过，以太坊每秒只能处理 20 个交易，而所有应用都只能共用一条主链，从而导致网络拥堵效率低，扩展性也不足。

以太经典（Ethereum Classic, ETC）

以太坊经典来自于以太坊的一次硬分叉，相比 ETH 无上限增发，ETC 坚持去中心化、不可逆转、不受第三方审查干扰的原则。ETC 从 2017 年 12 月起每 500 万个区块链减产 20%，最终总量固定在 2.1 亿至 2.3 亿之间。

ETC 采用 POW 共识算法，任何动态组网接入的节点都有利可图，ETH 则将改用 POS 共识算法。ETC 已经将 EVM（以太坊虚拟机）替换为速度更快的 SputnikVM，以适合开发物联网应用。以太坊经典目标是成为去中心化的物联网基础设施。另外，ETC 采用的侧链技术具有交易免费的特点，普通的个人设备也可以享受这种服务。

达世币（Dash）

达世币原名暗黑币，于 2014 年推出，是一款支持即时交易、以保护用户隐私为目的的数字货币，总量约 2200 万。相比其它数字货币减半，该币每年的供应按照 7%的速度减产。

达世币采用广泛使用的链接运算“X11 哈希算法”，减少专门为数字货币挖矿涉及的 ASIC 使用的概率。达世币采用独创的“服务量证明”机制，引入 two-tier 激励模型，也就是主节点网络技术，而非单层激励模型，使得添加更多类型服务成为可能；该币所应用的 Darksend（匿名发送）技术除了具有 CoinJoin（提供匿名技术的软件）核心理念，还具有去中心化、

使用链接实现强匿名、相同面值和被动先进的混币技术。

零币（Zcash, ZEC）

零币是基于比特币 0.11.1 版本代码基础上进行修改的分支，保留了比特币原有的模式，总量 2100 万个。与比特币的区别在于，零币使用了先进密码学技术自动隐藏了交易信息，只有持有私钥的人才有权限查看交易信息。

零币首个实施零币协议的数字货币。零币协议使用零知识证明来实现完全的金融隐私。零知识证明是一种密码学方法，其中一方可以向另外一方证明某个给定的声明是正确的，除了该声明确实是正确的意外，无需传达其它的信息。零币协议允许很多匿名设置，使其在金融隐私方面相比其它协议更有效。

零币采用的工作量证明机制引入了卢森堡两位博士提出的 equihash 理论，削弱了专业矿机的显卡设备优势，强化内存带宽为 PoW 的瓶颈，为大众挖矿打下基础。

■ 4.1.3 最新研究现状

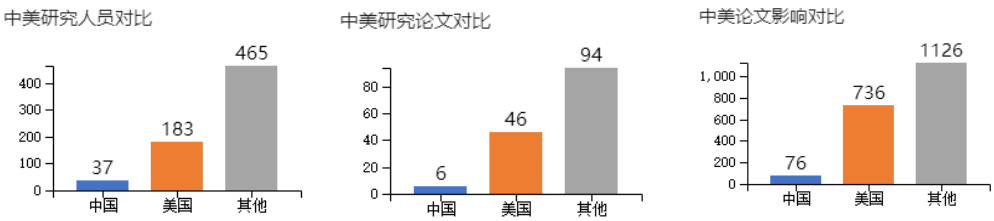
比特币对传统金融体系的颠覆式创新引起全球学者的高度关注，比特币的研究成果今年持续爆发。学者对比特币的研究主要集中在比特币的本质属性、比特币经济性、数字货币法律问题和未来发展方向四个方面。

学者分布

从世界范围看，比特币研究专家集中于美国和欧洲。此外，中国、日本、澳大利亚也有部分学者涌现。少量学者出现于非洲与东南亚地区。比特币研究专家分布与比特币的产业需求和成熟程度是相对应的。相较而言，欧美各国政府对比特币交易和持有态度较为宽松，进行积极监管，但比特币在亚洲与非洲的发展多受到法律限制。政府态度的不同是影响比特币研究的重要因素之一。

图 8　比特币全球学者分布

中美研究概况对比



与美国相比，中国比特币研究起步较晚，在研究人员、研究论文数量与论文影响都存在较大差距。这与不同国家对比特币的态度、比特币发展状况有很大关联。未来，中国在比特币研究领域仍存在很大的发展空间。

最新论文

近期，国际上关于比特币和区块链的研究集中于提出新的、更易于编程和验证的加密货币和智能合同解决方案，探索具有更高安全性能的证明机制以满足行业对效率和可靠性的要求，设计高保障、高性能的存储和处理高值加密货币和机密交易的系统，以及解决现存共识机制在资源浪费等方面的问题。随着区块链研究的深入和数字货币交易的普及，区块链领域的研究也从总结规律、发现问题逐渐向提出解决方案、设计实用机制过渡，研究成果也更多地被应用在经济、金融、信息安全领域。

■ **The Miner's Dilemma.**

I. Eyal.

IEEE S&P, 2015.

一个开放的分布式系统可以通过要求参与者提供工作证明并奖励他们参与来获得。比特币数字货币引入了这种机制，几乎所有的现代数字货币和相关服务都采用了这种机制。一个

自然的过程引导这些系统的参与者形成池，成员聚集他们的力量并分享奖励。比特币的经验表明，最大的资金池往往是开放的，允许任何人加入。长期以来，一个成员可以通过看似加入的方式来破坏一个开放的游泳池，但却从不分享自己的工作证明。该池与攻击者共享其收益，因此每个参与者的收益都更少。

作者通过一个游戏详细阐述了“矿工窘境”的内涵。在这个游戏中，矿池使用一些参与者来渗透到其他矿池中从而对其他矿池进行攻击。对于任意数量的矿池，矿池之间都不相互攻击并不是纳什均衡。但是，一旦任意两个或两个以上的矿池为了争夺资源而相互攻击，它们都会比没有攻击的情况下得到的收益更少，这就是一个典型的“公地悲剧”现象。对于任意两个池子而言，决定是否攻击是矿工的困境，这是迭代囚徒困境的一个实例。这样的例子每天在比特币交易中都会发生。如果矿池之间没有攻击的平衡被打破，开放池的收益可能会减少，它们对参与者吸引力也会随之降低。

■ **Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions.**

A. Miller, A. Kosba, J. Katz, E. Shi.

ACM CCS 2015.

比特币奖励结构的一个隐含目标是减少网络对个体参与者多样化、分散化的影响。事实上，比特币的安全机制依赖于没有一个实体拥有足够大的网络整体计算能力的假设。然而，大多数比特币矿工并没有独立参与挖矿，而是加入了所谓的“矿池”联盟，在这个联盟中，中央池管理人员主要指挥池的活动，导致权力的巩固。这也导致了最大的矿池占了网络总开采能力的一半以上。与此相关的是，“托管矿业”服务提供商为客户提供了规模经济效益，诱使他们远离独立参与。比特币的证明机制具有与生俱来的局限性。这篇论文的主要目的在于定义比特币的局限性，并尝试提出可行的解决机制，通过基准测试结果验证机制的实用性。

■ **On Scaling Decentralized Blockchains (A Position Paper).**

K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer.

BITCOIN 2016.

基于区块链的加密货币越来越受欢迎，这使得可伸缩性成为首要和紧迫的问题。此篇论文分析了比特币的瓶颈如何限制了它对点对点网络覆盖网络的能力，以支持更高的吞吐量和更低的延迟。研究结果表明，对区块大小和间隔的重新参数化应该被看作是实现下一代的高

负载区块链协议的第一步，而且主要的进展还需要对技术方法进行基本的重新思考。该研究为这种方法提供了一个结构化的设计空间。更进一步的扩展将在更长的时间内需要基本的协议重新设计。通过对区块链协议的结构化展示，该研究展示了各种可能成功的方法来进行这种扩展。

■ **Bitcoin-NG: A Scalable Blockchain Protocol.**

I. Eyal, A. E. Gencer, E. G. Sirer and R. V. Renesse.

NSDI, 2016.

以比特币为基础并以比特币为主导的加密货币，已经显示出了以匿名在线支付、廉价汇款、可靠的数字资产交换和建立智能合约等方面的潜能。然而，比特币派生的区块链协议具有固有的可伸缩性限制，这必然会削弱区块链在吞吐量与延时任意一方面的能力。为了解决这一个弊端，四位学者提出一种用于扩展的区块链新共识协议：下一代区块链协议（A Next-generation Blockchain Protocol, Bitcoin-NG）。基于比特币的区块链协议，Bitcoin-NG 是一种更为复杂的容错机制，具有拜占庭容错，能够应对更为极端的情况。除了提出 Bitcoin-NG 共识机制，学者们还引入了一些新的度量标准，用于量化类似于比特币区块链协议的安全性和效率。

■ **Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge..**

F. Tramer, F. Zhang, H. Lin, J.P. Hubaux, A. Juels and E. Shi.

IEEE Euro S&P, 2017.

可信硬件系统，如英特尔 SGX 指令集架构扩展，旨在为应用程序提供强大的机密性和完整性保证。然而，人们也逐渐发展 SGX 的种种弱点，对这种系统对侧道攻击的脆弱性表示担忧。该研究团队提出了被称为 Sealed-Glass Proof（SGP）的密码原语，能够在孤立的执行环境中以“无边界泄露”（unbounded leakage）形式进行计算，并由此能够抵御强大的侧向通道攻击。SGP 可以为一段代码的正确执行提供证明，但是证明过程是其透明的，这意味着一台电脑上应用程序的状态可以在同一主机上的其他进程中可见。SGP 不仅具有严谨的理论模型，也体现了宽泛的实际应用范围。该研究团队利用智能合约和基于 SGX 的 SGP 建立了一个端到端的平台，这个平台能够促进公平交易，防止违约行为，排斥失信卖家和恶意攻击。在论文中，研究团队放松了对 SGP 模型的假设，允许黑盒模块实例化最小的、侧通道的可防御原语，从而产生更广泛的应用程序。

■ **PieceWork: Generalized Outsourcing Control for Proofs of Work.**

P. Daian, I. Eyal, A. Juels, and G. Sirer.

BITCOIN, 2017.

大多数加密货币都利用 PoW 来保护它们的运行，然而 PoW 却有两个弱点。首先，PoW 会造成大量的资源浪费；其次，由于比特币已经吸引全球大部分算力，其他再利用 PoW 共识机制的区块链很难获得相同的算力以保障自身安全，导致在少数“矿池”中存在不平等的权力集中。四位学者构建 PoW 的通用方法，即分段处理（Piece of Work），解决了这两个问题。从本质上讲，分段工作允许将 PoW 计算的可配置部分外包给矿工，使得资源能够被重复利用并能够完成额外的工作，如预防垃圾邮件和减少占用磁盘空间，从而减少了 PoW 的资源浪费。同时，分段处理方法能够避免过度外包，长时期的过度外包可能会导致挖矿操作成本明显升高。

■ **REM: Resource-Efficient Mining for Blockchains.**

F. Zhang, I. Eyal, R. Escriva, A. Juels and R. V. Renesse.

USENIX Security, 2017.

区块链具有成为未来金融交易系统基础设施的潜力。然而，今天区块链的安全依赖于工作证明（PoW），但 PoW 会浪费参与者的计算资源。在这篇论文中，三位作者介绍了一个使用受信任硬件（Intel SGX）[22]的新的区块链挖掘框架——资源高效挖掘（Resource-Efficient-Mining, REM）。REM 实现了类似于 PoW 的安全保证，但利用了 SGX 中固有的部分分散的信任模型，一定程度上解决了 PoW 对计算机资源的浪费。REM 的核心机制是有用工作量证明（Proof-of-Useful-Work, PoUW）。REM 机制具有更强的灵活性，允许任何实体创建有用的工作负载，通过一种具有独立利益的分级认证方案确保了这些工作负载的可信赖性。为了解决被入侵的 SGX CPUs 的风险，三位作者共同开发了一个基于统计数据和其他受信任硬件机制（如英特尔的运行时间证明（Proof-of-Elapsed-Time, PoET））的正式安全框架。三位作者将 REM 作为一个示例应用程序应用于比特币核心共识层，首次全面实现基于 SGX 的区块链运行。

---

[22] Intel Software Guard Extension, SGX 是对英特尔体系（IA）的一个扩展，用于增强软件的安全性。这种方式并不是识别和隔离平台上的所有恶意软件，而是将合法软件的安全操作封装在一起，保护其不受恶意软件的攻击。

引用自 https://blog.csdn.net/u010071291/article/details/52750372

■ **Smart Contracts for Bribing Miners.**

P. McCorry, A. Hicks, S. Meiklejohn.

BITCOIN, 2018.

三位作者提出了三种允许贿赂者公平地向“矿工”行贿的智能合约，使得贿赂者可以从矿工的采矿活动中受益。第一种合约称为审查合约（CensorshipCon），审查合同关注重点在于以太的叔块（uncle block）奖励政策可以直接补贴贿赂矿工的费用；第二类合约为历史修正合同（HistoryRevisionCon），通过一笔频带内付款（in-band payment）[23]的方式来奖励矿工，以扭转交易或强制执行另一项合同的新状态。第三类合约为金手指合约（GoldfingerCon），是指用一种加密货币奖励矿工，以减少另一种加密货币的效用。该论文的目的在于评估拥有智能合约的区块链是否会对中本模式共识机制（Nakamoto-style consensus）产生影响。

■ **Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance**

Sarah Azouvi, Mary Maller, and Sarah Meiklejohn

BITCOIN, 2018.

在去中心化的系统中，分类账户信息输入由节点控制。理论上每个节点都拥有与计算能力相对应的投票权，而节点输入数据是否有效也就是节点的诚实性是决定去中心化和透明性有效的前提。在本篇论文中，三位作者对全球市值最大的两种数字货币比特币和以太坊现有治理结构的去中心化进行了定量研究。作者对每种数字货币都考察了两个不同的指标：对代码库每个文件有贡献的开发者数量和参与每个平台 GitHub 数据库相关部分讨论的人员数量，结果发现对代码库有贡献的人分布是完全不同的，而在讨论问题上，通常少数人贡献了大部分。三位作者还通过调查改进建议的提出者和评论者来评估比特币和以太坊的决策模式，发现以太坊相比比特币在代码库改进建议方面更加中心化，而在讨论环节更加去中心化。此外，通过比较比特币和比特币现金、以太坊和以太坊经典团队发现，初始货币和分裂币团队几乎没有交集。

■ **Paralysis Proofs: Safe Access-Structure Updates for Cryptocurrencies and More**

[23] In-band（频内）网络架构，指那些数据控制已经被固定的网络协议，In-band 控制的控制数据通常和主要的传输数据公用用同样的连接链路（以太网通道），属于应用层管理。Out-band（频外）架构，又被称为熄灯（Lights out Management, LOM）管理，指数据传输信道独立于正常的网络传输，被管理设备即使在关机状态甚至故障的状态下，都可以进行修复重开机或是日志监控等管理作业。

引用自 https://blog.csdn.net/u010558281/article/details/52750730

Fan Zhang, Philip Daian, Iddo Bentov, and Ari Juels

BITCOIN, 2018.

密钥管理是普遍存在的安全问题，凸显了安全和便利性之间的矛盾，在依赖密钥进行授权交易的数字货币领域表现的尤为明显，放大了数字货币的一些独有特点。密钥的高频使用意味着易受攻击，意外的删除或损坏也是灾难性的，数字货币的去中心化意味着凭证直接恢复是不可能的。为此，本篇论文提出一种创新技术——Paralysis Proof System 来解决安全的两难问题。该系统支持安全的有条件的从一种访问结构向另一种转移，访问结构可以随意增加，管理转移的策略非常灵活。建立该系统大众版所使用的主要工具包括公认可靠的硬件——Intel SGX 和区块链。该系统能够相对容易的通过智能合约在以太坊实现，甚至对硬件的要求可以降低。而在比特币中，即便是 SGX 这样的可信硬件与比特币区块链安全的同步也存在困难。总体上，Paralysis Proof System 概念简单，同时借助 SGX 和区块链提供了一种能够广泛实现的强大新能力。该系统提供了多种访问结构变化选项，使其应用并不仅限于数字货币。

■ **A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution**

Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, Dawn Song

Cornell University Library,2018

智能合约是一种能够在区块链上执行的应用。如今智能合约管理着无处不在的区块链部署价值数十亿美元的交易。尽管智能合约继承了区块链的可用性和安全性，但也受累于区块链缺乏保密性和性能不佳的缺点。作者提出一种新的系统——Ekiden，通过将区块链和可信执行环境（TEEs）结合来解决这些缺点。Ekiden 能够在任何期望的区块链上运行，使得智能合约可以在 TSS 支持的计算节点内同步脱链执行，并具有高性能、低成本和敏感数据保密的特点。目前，Ekiden 支持 Rust 和以太虚拟机（EVM）智能合约。

■ 4.1.4 数字货币优点和风险

数字货币有着其他货币无可比拟的优点。首先，数字货币可以有效降低银行经营成本，无论是发行还是交易都有着低成本高效率的特点。从发行环节来看，数字货币不会产生实体货币发行所需要的成本费用，从交易环节来看，数字货币不需要建立和维护个人账户，而是

完全使用电子记账的方式，并且数字货币的交易账簿唯一也不需要货币清算，节省了交易成本。其次，数字货币推动了共享金融的发展，数字货币的交易基本不需要金融中介机构的介入，同时与物联网等现代科技紧密结合。其次，数字货币可以有效解决互联网金融领域监管困难、信息不对等等问题，简化数据处理流程，更进一步推动了互联网金融的发展。除此之外，数字货币的核心技术区块链更是在金融、物流等领域得到了广泛的应用。

数字货币同时也存在着不可不说的风险，下面以其典型代表比特币为例进行说明。比特币自诞生以来，常有剧烈的价格波动，使一些人望而却步。各国对比特币的政策仍在逐步明确的过程中，以及比特币自身的价格波动，让许多人对比特币持保守态度。随着比特币通过挖矿不断产生，比特币价格也在供需平衡的变化过程中动态变化。

在货币形态演进过程中，取得稳定的价值来源与可靠的信用保证，是任何形式的货币必须回答的两大核心问题。以比特币为代表的数字货币作为历史发展的必然结果，同样需要具备解决价值来源于信用保证问题的能力。由于货币本身没有价值而承担价值尺度职能，因此不论在人类社会哪个发展阶段，货币均要求有价值锚定，即使进入数字货币阶段，价值锚定属性仍需得到继承。因此，选择具有稳健价值的锚定物，是货币获得稳定价值的关键。作为私人发行的数字货币，比特币的价值来源为个人投机，价值不稳，公信力不强，可接受范围有限，容易产生较大负外部性。一方面，从比特币产生机制上看，在去中心化的比特币系统中，任何人都可下载运行比特币软件并参与比特币生产，只要创建一个区块，便可拥有该区块中包含的比特币，但是，由于比特币总量固定，相当于不可再生资源，因此，参与“挖矿”的人数越多，算法越复杂，“挖矿”的成本也越高，开发新比特币的难度就越大。另一方面，从比特币交易模式来看，比特币发行和交易集中于“私人小圈子”，交易流程灵活化、个性化，却缺乏强大机制保证其不会违约。由于比特币是虚拟商品，不产生实际经济价值，一旦违约，持有者将没有任何担保或索赔权。由比特币价格走势可见，随着比特币存量不断减少，剩余比特币价值迅速上升，具有很大的投机性质。因此，比特币在自身稳定价值和稳定投资者信心的机制建设上仍然不够完善。

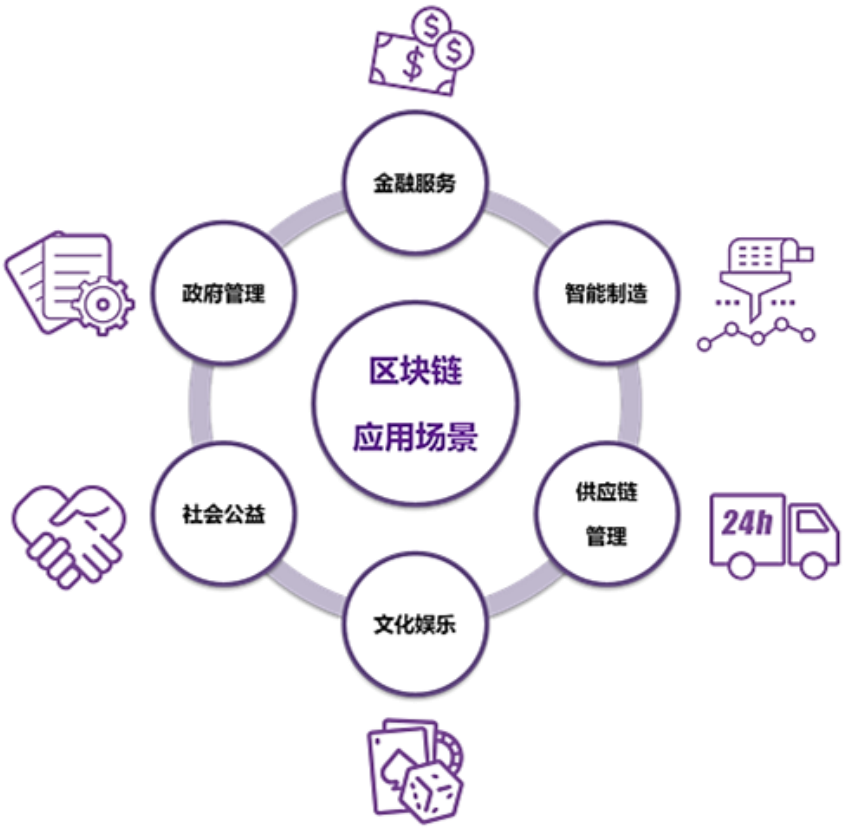
图 9　比特币币值走势图

上图是截止到 2018.7.2 比特币币值行情走势图。

比特币交易提升了社会创新能力，但由于比特币缺乏法律监管，2017 年 9 月 30 日，比特币中国关闭所有交易功能，标志着比特币交易在国内已被全面禁止。比特币拉动了一系列新兴产业的发展，如比特币交易所、第三方支付平台、比特币投资行业、“挖矿”行业，但这些新兴产业基本处于监管的“灰色地带”，没有统一的交易机制进行约束，因此，坐地起价、违约现象时有发生，难以追踪打击，也容易诱发投机行为、金融欺诈和道德风险。事实上，早在 2013 年 12 月 5 日，中国人民银行联合五部委发布《中国人民银行工业部和信息化部 中国银行业监督管理委员会 中国证券监督管理委员会 中国保险监督管理委员会关于防范比特币风险的通知》，明晰了比特币的属性是“特定的虚拟商品”，禁止各金融机构和支付机构开展比特币相关业务，加强比特币网站管理，防范比特币潜在洗钱风险，并加强对社会公众货币知识的教育及投资风险提示。

4.2 区块链其他应用场景

区块链系统具有分布式高冗余储存、时序数据且不可篡改和伪造、去中心化信用、自动执行的智能合约、安全和隐私保护等显著特点，因此，区块链不仅可以应用于数字加密货币领域，同时在金融服务、供应链管理、文化娱乐、社会公益和政府管理等 6 个领域存在中也存在广泛应用场景。但是，区块链在这些领域的应用尚处于起步阶段，未来仍具有极大的探索空间和发展潜力。



■ 4.2.1 金融服务

区块链的核心创新点在于去中心化信用，能够不依靠中心机构信用背书建立金融市场，成为“金融脱媒”的重要实践，也对传统金融机构、金融服务模式产生极大冲击。自 2015 年以来，全球主流金融机构纷纷开始布局区块链，以高盛、摩根大通、瑞银集团为代表的银行业巨头分别成立各自的区块链实验室、发布区块链研究报告或申请区块链专利，并参与投资区块链初创公司。除此之外，上海证券交易所、纳斯达克、纽约证券交易所、芝加哥商品交易所等各国证券交易所也对区块链技术进行深入探索。区块链在金融领域的应用，体现在证券与银行业务、资产管理、贸易融资、保险业务和反洗钱业务等方面。

在证券银行业务方面，区块链可编程的特性能够提高证券交易与金融服务的效率，节约交易成本，并简化交易流程。同时，区块链和比特币即时到账的特点可使银行实现比 SWIFT 代码体系更快捷、经济和安全的跨境转账。

在资产管理方面，区块链的时间戳技术和不可篡改的特性为防假防伪、知识产权保护、资产授权和控制提供便利，对无形资产管理和有形资产管理方式都进行了革新。

在贸易融资方面，区块链凭借数字加密、点对点技术、分布式共识与智能合约，能够实

现信息的快速、透明交换，克服了人工搜集数据、核对信息、贸易接洽的高成本和潜在风险。一个完整区块链贸易融资平台，能够在线全流程管理并实时掌控贷前调查、贷中审核、贷后管理各个方面，让贸易融资流程简化。

在保险业务方面，区块链智能合约对传统保险模式的影响最大。保险公司所有的理赔记录都能够在全网公开并被集体验证，防止“双重索赔”现象发生，防范骗保行为，规范保险秩序。

在反洗钱业务方面，根据《中华人民共和国人民币管理条例》规定，假币是“伪造、变造的人民币”。由于数字货币式存储在计算机中的电磁符号，不存在物理形态的仿冒或改变，能够从源头上组织假币问题泛滥。同时，数字货币认证登记系统能够鼓励商业银行、工商企业和居民个人共同识别打击数字货币造假和洗钱问题。

■ 4.2.2 智能制造

《中国制造 2025》提出“创新驱动、质量为先、绿色发展、结构优化、人才为本”的基本方针，在新一轮科技革命和产业变革与我国加快转变经济发展方式形成历史性交汇的背景下，提升制造业效率和竞争优势成为建设智能制造格局的重心。区块链技术能够利用大数据分析为制造企业提供更为高效、安全的运营机制，让制造企业第一时间掌握库存、产能、订单和市场供求信息，提升企业上下游互联互通水平。

■ 4.2.3 供应链管理

区块链与物联网的结合掀起了供应链管理领域的深刻变革。传统供应链管理面临由于信息不对称导致的效率低下、协调困难等问题，在流程追踪和统筹安排方面困难重重。区块链能够使交易网络信息公开化、透明化，可以在很大程度上减少信息不对称、提高供应链周转效率。同时，区块链数据不可篡改和交易可追溯的特征能够有效遏制供应链管理中假冒伪劣产品问题，形成完整的供应链闭环。目前，京东已经将区块链与物流结合，用于加强食品安全；菜鸟与天猫国际共同宣布启用区块链跟踪、上传、查证跨境进口商品物流全链路信息。

■ 4.2.4 文化娱乐

在音乐领域，区块链技术被称为“一旦被广泛应用，将成为颠覆现有音乐产业格局的一股强大力量”，在实现粉丝经济最大化、解决数字音乐版权管理难题、帮助音乐人实现完全创收等方面大有可为。

全球最大音乐流媒体平台 Spotify 于去年收购了区块链初创公司 Mediachain。该公司可

以通过提供开放源代码对等数据库和协议的方式，让创作者将自己的身份与其作品关联起来，进而能够确保所有歌曲都能追踪到创作者和版权所有人信息，并由 Spotify 使用合理的途径支付版权费用，同时也能缓解流媒体平台与版权所有人之间的矛盾。此外，在全球范围内拥有超过 20 万音乐人客户的数字版权管理及货币化初创公司 Vydia 刚于上个月完成了 700 万美元的 A 轮融资；MIT 的 Media Lab 与伯克利音乐学院合作的音乐区块链应用项目也将于今年投入使用，这项由三大版权公司、英特尔、Spotify 和 Netflix 参与的大项目有望在区块链应用领域激起千层浪，成为区块链技术能否在全球音乐产业里大规模推广使用的重要转折。

目前，区块链技术在游戏行业的应用存在这样几方面：区块链游戏、游戏基础研发、基于区块链的道具交易平台、特色内容的版权保护、支付环节、分布式算法硬件发售等。根据 DappRadar 的统计数据，目前全球范围内至少已经出现了 100 多款区块链游戏。这些游戏中主要分为宠物养成类、地产类、经营类、购买类和博彩类等。

区块链技术围绕媒体信源认证、公民新闻审核、数字版权保护、付费内容订阅、传播效果统计、用户隐私保护、数字资产管理等一系列应用，为媒体深度融合提供了全新的视角和解决方案。

■ 4.2.5 社会公益

公益事业信息的不公开、不透明成为社会公益难以发展和存在争议的重要原因。社会公益与区块链的结合，集中体现在区块链不可篡改性和高透明度的特征上。区块链上存储的数据利用了分布式技术和共识算法，以共信力助力公信力，天然适用于公益场景。公益项目的相关信息，如资金流向、捐助对象、募捐明细等，都能够加入区块链节点，受到全网的验证与监督。区块链与公益的结合，让区块链真正成为“信任的机器”，让社会公益的运作“在阳光下进行”。目前，腾讯“公益寻人链”、支付宝听障儿童公益基金、“心链”等项目，都是区块链与社会公益结合的成功案例。

■ 4.2.6 政府管理

区块链技术在政府管理领域的应用主要体现在选举投票与智能监管。运用区块链不可篡改的特性和分布式共识验证技术，能够高效率、低成本地完成政治选举，避免人为操作和清点票数造成的失误，同时提高了投票选举过程的透明度，保证了数据存储的安全。

4.3 区块链发展现存障碍

技术问题

区块链是多种技术（例如私钥加密算法、P2P 网络、工作量证明机制 PoW 等）集成创新的结果，这些技术从诞生至今已经十余年，虽然发现并改进了不少弊端，但仍存在很多难以解决的问题，需要谨防这些弊端综合起来产生的严重后果。

从密码学来看，加密算法的安全通常定义为在当前技术水平下，加密信息在相当长的一段时间内（例如 100 年以上）无法被解密。但是，随着新的数学算法的出现以及计算能力的提高（例如量子计算机），以往安全的加密信息可能在较短时间内被解密。

从 P2P 网络的稳定性来看，当前大量节点的参与维持了网络的健壮性。一个重要原因是比特币自身的价格处于高位，且电费便宜，成本可以覆盖收益。但是，如果有一天因为成本、政治或其他因素，大量节点开始退出网络，则要防范由此可能带来的区块链网络的不稳定性。

从工作量证明机制来看，系统在仅拥有少数节点的时候，使用工作量证明机制存在一定的风险。因为，供给者此时很容易超过全网算力的 50%，进而轻松实现 51%攻击，导致整个系统的瘫痪和失效。

尚未成熟的区块链技术，也面临着平台安全、应用安全的严峻形势。2011 年 6 月，Allinvain 被盗走了 25000 个比特币，成为比特币历史上第一个因为黑客攻击而遭受重大损失的玩家。2012 年 9 月，比特币平台 Bitfloor 被一个黑客成功攻破，损失 24000 个比特币，Bitfloor 平台也于 2013 年 4 月被迫关闭。2016 年 6 月，基于区块链技术的全球最大众筹项目 The Dao 被黑客攻击，导致价值 6000 万美元的 360 多万以太币被劫持，引起业内震动和高度关注。

在反洗钱业务方面，虽然数字货币能够为反洗钱业务提供技术支撑，但是也需要警惕数字货币本身具有的局限性。例如，由于现行假币识别与处理方法不是适用于数字货币，一旦数字货币出现仿冒行为，将难以被追踪核查。此外，洗钱行为逐渐多样化、复杂化，且日益显现国际化犯罪特征，需要政府及金融监管机构警惕游离于正规数字货币交易场所之外的数字货币洗钱可能性，建立国际间合作监管机制，更新完善反洗钱准则。

高耗能问题

货币经济学中存在着“不可能三角”，即不可能同时达到“去中心化”“低耗能”和“安全”三个要求。区块链技术的应用在节约中心化成本并逐步提高金融安全性的同时，是否过度使用了电子耗能成本。从整体性来考虑，使用区块链技术要权衡成本收益选取最优化的方案。

安全挑战

区块链技术面临极大的安全挑战，2018 年 5 月 24 日 EDU 智能合约爆出漏洞，通过这个漏洞，攻击者不需要私钥就可以转走指定账户的所有 EDU，并且由于合约没有 Pause 设计，无法止损。等等，这类事件使得区块链的面临的安全挑战越来越引起关注。复旦大学教授斯雪明将区块链面临的安全挑战分为算法漏洞、协议漏洞、实现漏洞、使用漏洞和系统漏洞五个方面。并针对这五个漏洞提出了常识性的解决方案，在算法安全性方面，针对量子攻击要进行后量子密码算法研究，同时采用经验验证的密码算法；在协议安全方面，采用能够阶段性离线的共识机制、避免目标确定的共识机制、设计防 ASIC 等共识运算优势明显的共识算法、加强关键节点的网络安全强度；在实现安全性方面，要对智能合约安全性验证同时要对区块链以及使用的模块做标准化处理；使用安全性方面，可以采用冷钱包、多因素验证钱包、物理随机数生成、私钥单一性使用等措施；在系统安全性上，要利用传统网络防御增强网络安全性，同时采用新型区块链架构。

监管风险

2016 年 2 月，中国人民银行行长周小川在谈到数字货币相关问题时曾提及，区块链技术是一项可选的技术，并提到人民银行部署了重要力量研究探讨区块链应用技术。他认为，目前区块链存在占用资源过多的问题，不管是计算资源还是存储资源，还应对不了现在的交易规模。2016 年 9 月 9 日，中国人民银行副行长范一飞在 2015 年度银行科技发展奖评审领导小组会议中提出，各机构应主动探索系统架构转型，积极研究建立灵活、可延展性强、安全可控的分布式系统架构。由此可见，区块链技术的监管不仅应该包括区块链的平台监管，还应该涵盖区块链的应用监管、区块链“生态圈”的监管

区块链的平台监管的对象是诸如比特币、以太坊等系统。这一层网络需要对区块链所有的可用范围进行考虑，而不仅仅是金融方面的监管。区块链的应用监管涉及智能合约等技术和新型的创新驱动融资方式——ICO，但是，ICO 融资手段暴露出了诸如不合规、虚假等等问题，所以，对于加快 ICO 市场监管法规落实的需求日益显现。至于整个区块链“生态圈”的监管，则需要重点关注建设一套系统的分类标准，从而规范化、标准化区块链“生态圈”的管理。

2017 年 9 月，中国人民银行等七部委联合发布的《关于防范代币发行融资风险的公告》中明确指出，代币发行融资（ICO）行为涉嫌非法集资、非法发行证券以及非法发售代币票券等违法犯罪活动，在中国境内叫停包括 ICO 在内的所有代币发行融资活动，清理整顿 ICO 平台并组织清退 ICO 代币。

2018 年 1 月，中国互联网金融协会在其官网发布《关于防范变相 ICO 活动的风险提示》，称随着各地 ICO 项目逐步完成清退，以发行迅雷“链克”（原名“玩客币”）为代表，一种名为“以矿机为核心发行虚拟数字资产”（IMO）的模式值得警惕，存在风险隐患。呼吁广大消费者和投资者应认清相关模式的本质，增强风险防范意识，理性投资，不要盲目跟风炒作。

2018 年 7 月，央行会同相关部门搜查出国内 88 家数字货币交易平台和 85 家首次代币发行融资（ICO）交易平台，并基本实现无风险退出。针对近期相关非法金融活动的新变种与新情况，相关监管部门组织屏蔽“出海”数字货币交易平台。

4.4 挑战与未来

未来，区块链技术必将深刻改变人类的生活方式与生产效率。继区块链 1.0、区块链 2.0 后，人们大胆预测人类社会即将开启区块链 3.0 时代，即可编程社会系统时代。区块链 3.0，代表的是解决了关键性技术难题的全领域生态级别的底层系统出现以及区块链技术应用到各个垂直行业中去的时代。这个时代的底层协议能够在保证去中心化、去信任中介的同时，保证了商用级别的高性能。在现有阶段，大部分底层协议项目为以太坊为原本在此基础之上进行迭代，还远远未能达到 3.0 时代的标准。区块链技术若要进一步深入实际场景，必须克服其在技术上、人才上、开发成本上和法律上的障碍，形成区块链研究与应用标准化体系，为学术研究和行业实践带来新的创新红利。

参考文献

[1] Haitsma J, Kalker T. Robust Audio Hashing for Content Identification[J]. Proc. of the Content-Based Multimedia Indexing, 2001.

[2] Distributed Ledger Technology: beyond block chain. The UK Government Chief Scientific Adviser. 2016.

[3] Szabo N. Smart contracts[J]. Unpublished manuscript, 1994.

[4] National Institute of Standards and Technology (NIST). Secure Hash Standard (SHS). Digital Signature Standard (DSS). FIPS PUB 180-2 Standard, 2002.

[5] Shannon C E. Communication theory of secrecy systems[J]. Bell Labs Technical Journal, 1949, 28(4): 656-715.

[6] Meyer C H. Design considerations for cryptography[C]//Proceedings of the June 4-8, 1973, national computer conference and exposition. ACM, 1973: 603-606.

[7] Diffie W, Hellman M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6): 644-654.

[8] Rivest R. The MD5 message-digest algorithm[J]. 1992.

[9] FIPS N. 180-2: Secure hash standard (SHS)[J]. US Department of Commerce, National Institute of Standards and Technology (NIST), 2012.

[10] Rivest R L, Shamir A, Adleman L M. Cryptographic communications system and method: U.S. Patent 4,405,829[P]. 1983-9-20.

[11] Lamport L, Shostak R, Pease M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.

[12] Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults[J]. Journal of the ACM (JACM), 1980, 27(2): 228-234.

[13] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//OSDI. 1999, 99: 173-186.

[14] Douceur J R. The sybil attack[C]//International workshop on peer-to-peer systems. Springer, Berlin, Heidelberg, 2002: 251-260.

[15] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures[J]. Ad hoc networks, 2003, 1(2-3): 293-315.

[16] Newsome J, Shi E, Song D, et al. The sybil attack in sensor networks: analysis &

defenses[C]//Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, 2004: 259-268.

[17] Montet C, Serra D. Game theory and economics[M]. New York: Palgrave macmillan, 2003.Aumann R J. Game theory[J]. The New Palgrave Dictionary of Economics, 2017: 1-40.

[18] Nash J F. Equilibrium points in n-person games[J]. Proceedings of the national academy of sciences, 1950, 36(1): 48-49.

[19] Nash J. Non-cooperative games[J]. Annals of mathematics, 1951: 286-295.

[20] Zhu Liehuang, Gao Feng, Shen Meng, Li Yandong, Zheng Baokun, Mao Hongliang, Wu Zhen. Survey on Privacy Preserving Techniques for Blockchain Technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186.

[21] 郑东，赵庆兰，张应辉.密码学综述[J].西安邮电大学学报，2013，18(06):1-10.

[22] 朱雷钧.哈希函数加密算法的高速实现[D].上海交通大学，2008.

[23] 袁勇，王飞跃.区块链技术发展现状与展望[J].自动化学报，2016，42(04):481-494.

[24] 李靖.比特币的发展研究综述[J].当代经济，2015(31):134-137.

[25] 贾丽平.比特币的理论、实践与影响[J].国际金融研究，2013(12):14-25.

版权声明

AMiner 研究报告版权为 AMiner 团队独家所有，拥有唯一著作权。AMiner 咨询产品是 AMiner 团队的研究与统计成果，其性质是供用户内部参考的资料。

AMiner 研究报告提供给订阅用户使用，仅限于用户内部使用。未获得 AMiner 团队授权，任何人和单位不得以任何方式在任何媒体上（包括互联网）公开发布、复制，且不得以任何方式将研究报告的内容提供给其他单位或个人使用。如引用、刊发，需注明出处为“AMiner.org”，且不得对本报告进行有悖原意的删节与修改。

AMiner 研究报告是基于 AMiner 团队及其研究员认可的研究资料，所有资料源自 AMiner 后台程序对大数据的自动分析得到，本研究报告仅作为参考，AMiner 团队不保证所分析得到的准确性和完整性，也不承担任何投资者因使用本产品与服务而产生的任何责任。