可信区块链推进计划
TRUSTED BLOCKCHAIN INITIATIVES

公有链白皮书

（1.0版）

可信区块链推进计划

2019年5月

版权声明

免 责 声 明

本白皮书涉及的各类公有链项目仅用于原理性说明及技术架构分析研究，本白皮书的内容不构成对任何人的投资建议或市场预测。

编写组单位：

中国信息通信研究院、杭州秘猿科技有限公司、上海分布信息科技有限公司、成都链安科技有限公司、北京猿链网络科技有限公司、北京欧链科技有限公司

编写组成员：

何宝宏、魏凯、和涛、杨白雪、张启、卿苏德、张奕卉、钱靖、王博、胡凝、杨霞、黄婧祎、谭智勇

致谢：

特别感谢以下单位和专家对本白皮编写工作的深度参与和大力支持:

Conflux Foundation	杨光
BFTF 区块链技术联盟	王渊命
北京大学	肖臻
Qtum Chain Foundation LTD	郑义
ConsenSys Hong Kong Limited	阳靳光

前言

区块链技术源自2008年诞生的比特币系统，它通过点对点网络和分布式的时间戳服务器，集体维护和审计数据，解决困扰电子现金系统的“双花”难题。在之后的发展过程中，区块链技术的应用逐渐从电子现金领域向其他领域扩展，经历了新的分化与发展，出现了公有链（Public blockchain）和联盟链（Consortium Blockchain）两个发展方向。

公有链是指任何人都可以参与、无访问限制（Permissionless）的区块链。每个互联网用户都可以在公有链上发布、验证、接收交易，都有机会参与记账。公有链不仅是一个单纯的技术产品，其“共有、共建、共治、共享”的核心特征，使其具有在全球范围提供一般信任服务的潜力。公有链虽由技术驱动，但可能对经济、金融、社会的组织形态及治理产生深刻影响，受到全球各界高度关注。

目前，公有链的发展还处于早期阶段，总体上呈现技术热、应用冷的态势。全球公有链的应用高度集中在加密数字资产领域，而且呈现明显的头部效应，由于合规的链上身份系统缺乏、合约隐私性保护不足、与现有法律制度不协调等问题，与实体经济的对接还在探索中，“杀手级”应用尚未出现。但与此同时，公有链为区块链的技术创新发展提供了全球化的试验场，各种技术路线百花齐放，提升区块链可扩展性、互操作性、隐私性及安全性的技术方案不断涌现。

本白皮书旨在厘清公有链的起源、概念、特性及其创新价值，分析当前全球公有链的技术、应用、治理等方面的现状及趋势，探讨公有链发展面临的挑战。

目录

一、 公有链起源与概念

区块链的概念起源于 2008 年，由中本聪（Satoshi Nakamoto）在其论文《比特币：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）中首先提出，旨在解决困扰电子现金系统的“双花”难题。

自二十世纪末的密码朋克（Cypherpunk）[1]运动以来，极客们不断地尝试和探索不依赖第三方的电子现金系统。从 1982 年大卫·乔姆（David Chaum）发布的关于盲签名技术（Blind signatures）的论文，到戴维(Wei Dai)提出匿名的、分布式的电子加密货币系统 B-money，再到 2004 年哈尔·芬尼（Hal Finney）把哈希现金算法改进为“可复用的工作量证明机制”（Reusable Proofs of Work），技术极客们前赴后继，但却无法获得真正的成功。

中本聪将非对称加密、点对点技术、工作量证明三项关键技术结合在一起，创造了第一个不依赖于中心化机构的点对点电子现金系统，并且在全球大规模部署。比特币系统的底层是一个由多方共同维护，使用密码学保证传输和访问安全，实现数据一致存储、难以篡改、防止抵赖的分布式账本，也称为区块链（Blockchain）[2]。

在后续发展过程中，区块链技术逐渐从比特币和电子现金的领域向其他领域扩展，产生了公有链以及联盟链的应用方向。

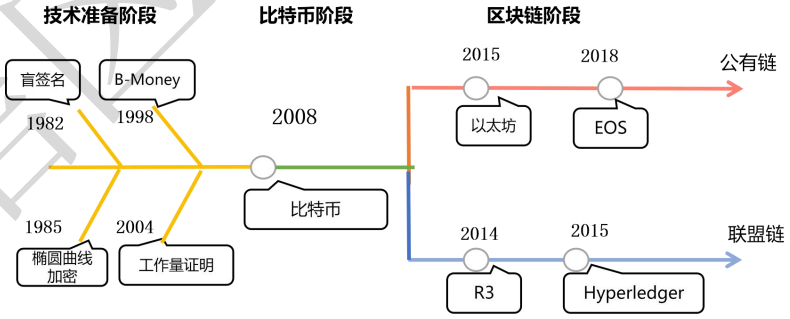

图 1：从电子现金到区块链

2014 年，以太坊的出现极大地扩展了区块链的可编程性。以太坊（ETH）

[1] 密码朋克（Cypherpunk）运动，起始于 1992 年的 Cypherpunks 邮件列表，提倡广泛使用强密码和隐私保护技术，实现个人的隐私和安全。

[2] 详见中国信息通信研究院：《区块链白皮书》，2018 年 9 月。

提出了智能合约的概念，用户可编写智能合约的程序并将其部署在区块链上，使得区块链从主要用于记录电子现金转账的“专有账本”，升级为可记录计算状态（state machine）的“通用账本”，区块链进入可编程时代，这很大程度上丰富了区块链的应用潜力。

几乎在以太坊出现的同时，一些大型机构也开始将区块链思想引入 IT 系统的变革中，逐渐兴起了联盟链（又称许可链）的范式。2014 年，R3 公司联合 9 家金融机构（巴克莱银行、毕尔巴鄂比斯开银行、澳大利亚联邦银行、瑞士信贷、高盛、J.P 摩根、苏格兰皇家银行、道富银行和瑞银集团）组建了 R3 金融区块链联盟。2015 年，Hyperledger 由 Linux Foundation 于创立，旨在帮助企业开发、应用区块链技术，其成员包括 IBM、Intel、思科、德意志银行、NEC、日立、百度、万达、华为等 280 个会员单位。联盟链方案催化了企业家和管理人员将区块链技术应用于从供应链管理、司法记录、数字版权、食药溯源等各个方面，联盟链（许可链）一般由行业联盟或是科技公司设计、实现和推动，具有高性能，注重金融和企业场景。

自此，区块链的发展范式分化为公有链和联盟链（许可链）两条路径：

——**公有链：**公有链是指任何人都可以参与、无访问限制（Permissionless）的区块链。每个互联网用户都可以在公有链上发布、验证、接收交易，都可以竞争记账权。比特币、以太坊是公有链的典型代表。

——**联盟链：**联盟链是由符合某种条件的成员组成的联盟来管理的区块链。它不像公有链那样对全社会开放，只有经过许可的可信节点才能参与该联盟链的记账，其它用户仅有部分权限。联盟链的一个例子是各大银行之间为了协同合作而构造和维护的区块链。

分类	公有链	联盟链
激励机制	区块奖励 记账手续费等	无
Token[3]	必须	不必须
节点准入限制	无	有

[3] Token 在不同语境下有多种中文翻译，比如加密货币、加密资产、代币和通证等，为避免混淆或歧义，本白皮书使用 Token 而非其中文翻译。

服务对象	不特定对象	特定对象
典型场景	数字资产 智能合约平台等	供应链金融 司法存证 政务协同 食药溯源 跨境支付等

表 1：公有链与联盟链的对比

二、 公有链的价值和特征

(一) 公有链的核心价值——提供基于机器的公共信任服务

信任是社会秩序的基础，缺少信任，任何社会关系都不可能持久存在。信任增强社会成员的向心力，降低社会运行的成本提高效率，也是稳定社会关系的基本因素。社会学家尼克拉斯•卢曼（Niklas Luhmann）把信任分为人际信任与制度信任[4]。

人际信任以血缘社区为基础，建立在私人关系和家庭或准家族的关系上，其基础是经验性的“道德人格”，并以熟人社会的舆论场来维护。人际信任是一切信任的基础，是主观化、人格化的信任。人际信任的特性是具体而经验的，缺乏普遍性，信任感及信任程度依对象的变化而变化。同时，人际信任的范围也极为有限，且需要大量的时间进行培育，但人际信任的内容和灵活度确是最高的。

制度信任是以契约、法规、制度作为约束的信任。制度信任不以关系和人情为基础的，而是以正式的规章、制度和法律为保障，如果当事人未按规章制度和法律条文行事,则会受到惩罚。制度信任是一种不以人的意志为转移的社会选择。违法必罚的法律逻辑所形成的稳定行为预期，是人们产生制度信任的基础。制度信任主导是现代社会运行的基本准则。

[4] 卢曼，《信任》，翟铁鹏、李强译，上海：上海世纪集团出版社，2005

相比于人际信任，制度信任是一种信任中介，它把人与人的信任转化为人与制度的信任关系。因此，制度信任是一种客观的、普遍的、抽象的、确定的、公共性的信任机制，以实在法规范和审判制度为保障的信用（credit）体系。[5]简单说，制度信任是不依靠具体人的信任，在制度信任的框架下，双方无需有真正意义上的“人际信任”，却可以依靠共同的制度信任保证互相行为在预期中完成。从历史上看，制度信任的出现极大地扩展了人类社会的信任范围，陌生人间只需信任共同的“制度”便可完成信用活动。但制度信任需要建立社会契约和立法的过程，而其范围是制度约束和订立的人群内，信任内容则包含了制度所明文制定的内容。

公有链的信任是一种人类信任协作的新形态，它有着最为广泛的信任范围。正如宾夕法尼亚大学教授 Kevin Werbach 在其论述区块链信任的专著中所述，“为所有的使用者提供最为一般化的信任（信用）服务是公有链最为核心的价值，它使得人类首次在达成全球范围内自发性信任。”[6]

区块链信任的基础在于各方在平权、分散的网络中，独立地记账、验证过程。各个参与者在公有链无门槛、自由出入、多方持有、多方维护的公共账本上独立地记录、验证每一笔交易及合约。在共识机制的作用下，每一个网络参与者都有可能成为会计（记账人），而在交易确认验证的机制下，每一个网络（全节点）都是审计人。因此，公有区块链是一个全球记账、全球审计的网络。共识机制保证了记账的随机性、分散性、不可伪造性，交易确认验证保证了记账的合法性，内在的经济和博弈论原理又使记账人基于经济理性原则不会破坏整个系统。

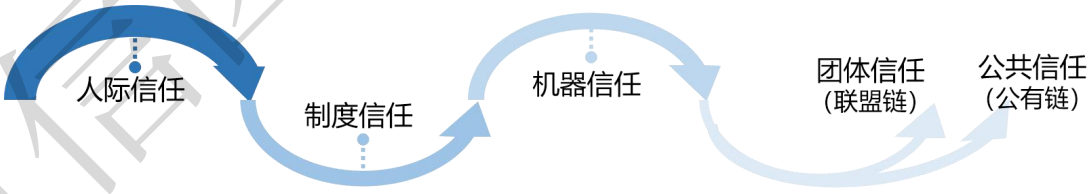

图 2：信任机制的发展历程

因此，区块链信任也是一种信任中介，它把人与人的信任转化为人与机器的信任。对于公有区块链的使用者来说，他无需信任任何具体参与这个网络生态的成员，就可以完成对于记账和合约计算的信任。公有链在信任范围上是全球的，

[5] 同上

[6] Werbach, Kevin. The Blockchain and the New Architecture of Trust. MIT Press, 2018.

任何国家和地区素未谋面的人在不依赖制度信任的前提下即可完成可信交易。并且，只要公有区块链系统健康运行，非法和无效的交易无法通过全球记账、全球审计的共识确认过程，因此也不存在违约和失信的情况。但是目前来看，区块链信任的使用场景仍较为有限，仅能在纯粹记账和封闭性合约的领域中，灵活度较低。

总的来说，公有链信任创造性地扩大了信任的范围，降低信任的成本，进一步推动了人类信任客观化的进程，为更大范围内的全球一体化协作开辟了新的可能。在未来的发展中，区块链信任可能与制度信任互为补充，建设更为普遍和高效的全球信任体系。

然而，必须要阐明的是，公有链造就的全球化技术信任网络仍旧是建立在一个复杂的技术堆栈之上。正如哈佛大学甘迺迪学院的信息安全大师 Bruce Schneier 指出“区块链的作用是使人们对他人或机构的信任转移到技术上来，需要相信加密学、一系列的协议、软件、电脑与网络。”[7]上述技术中任何其中一部分出现失效和错误，都会导致信任网络出现致命的问题。同时，区块链信任也不是万能的，它所创造的信任环境，不能简单外推到区块链外，一旦脱离链内的原生场景，区块链要解决现实中的信任问题，往往需要引入区块链外的可信中心机制予以辅助。[8]

信任类别	人际信任	制度信任	区块链信任
信任对象	具体人	抽象实体（规则、法律）	区块链网络
信任机制	情感、血缘、道德	社会契约、立法	共享账本记录、共享账本验证
信任范围	家族、社群	公司、国家、国际	全球范围、无条件准入
惩错机制	失信、声誉丧失	违法、司法处理	只要系统正常，原则上不会出现失信
信任内容	无限制	法律规范内的社会活动	仅限于记账、合约计算

[7] https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/

[8] 参见徐忠,邹传伟，《区块链能做什么、不能做什么？》，中国人民银行工作论文 No.2018/4 ，2018 年 11 月 6 日

灵活度	高	中	低

表 2：三种信任机制的对比

(二) 公有链的四大特征——共建、共有、共治、共享

为了实现基于机器的公共信任，一般来说，公有链具有**共有、共建、共治、共享的特征：**

第一，从“人”的角度出发，基于共建特征，记账公共化。公有链上的所有用户基于共识协议进行记账。每个用户都可以竞争记账权（俗称“挖矿”），检查交易的合法性。全体用户以一种去中心化的方式来维护公有链上数据的完整可靠、不被篡改。

第二，从“数据”的角度出发，基于共有特征，账本公共化。公有链上的数据是公开透明的，任何人都可以拥有全部历史数据的账本，查看账本内容，同时记录在区块链上的历史数据会被永久保存。

第三，从“代码”的角度出发，基于共治特征，治理公共化。公有链的代码维护、技术升级由公共社区完成，相关决策（包括对共识协议、出块奖励等修改）由公共社区做出，不由少数个人或机构来决定公有链的发展方向。公有链的代码必须是开源的，接受公众审查和监督，公有链的开发工作也由公众组成的自组织社区来完成。

第四，从“价值”的角度出发，基于共享特性，激励公共化。公有链为持续发展，必须设计经济激励原则，使参与贡献的人可获得相应的经济奖励。系统对于诚实节点进行了激励，对于恶意节点进行了惩罚，以概率收敛的方式实现了全网范围内的一致性算法，从而造就一个自发性的永远在线的全球化服务网络。同时，公共化的激励创造了内生的价值体系，不仅保证系统的可用性和安全性，更是从代码走向价值的突破性进展。激励的公共化是公有链最重要的特征之一，也是区块链能够吸引技术、金融甚至社会政治等不同领域的企业家和学者的重要原因。

(三) 公有链的价值载体——Token

作为价值激励的载体，Token 与公有链密不可分。但实际上 Token 又有若干类型，业界也有不同的划分标准。例如，澳大利亚金融市场管理局从金融监管的角度把 Token 划分证券型、投资型、支付型、货币型及实用型。[9]本白皮书按技术的角度，将 Token 划分为原生 Token 和衍生 Token 两种类型。

原生 Token 与公有链底层的价值、激励、治理与安全有着深刻逻辑关联，体现了公有链的价值特性。从价值上看，原生 Token 凝聚了公有区块链“信任价值”和“共识价值”的载体；从激励上看，原生 Token 是激励网络中“记账人”的参与的经济奖励；从治理上看，原生 Token 是参与公有链网络的权益凭证；从安全上看，价值激励的存在，提升了公有链的网络安全性。[10]

衍生 Token 通常是利用已有公有链之上的智能合约而实现，其本身与区块链底层系统没有内在关联。例如，以太坊 ERC20 为代表的 Token 合约，规定 Token 的总量、发行规则、转让规则和销毁规则等一系列逻辑。由于衍生 Token 与公有链底层实现没有逻辑联系，因此没有凝聚公有链网络的价值，一般情况仅被用来作为上层应用的资产标记来使用。

分类	原生 Token	衍生 Token
发行人	底层开发者	智能合约用户
发行方式	原生 Token 是底层链的设计，主要是通过出块奖励（Coinbase）、预先分配等方式	衍生 Token 是通过公有链上部署的智能合约实现
激励作用	激励节点进行记账（挖矿），提高系统参与度与安全性	无

[9] 资料源自：Nevenka Gobeljic《Australian Financial Market Creates New Rules For Security Tokens》,https://medium.com/token-dashboard/australian-financial-market-creates-new-rules-for-security-tokens-5139ab363278

[10] Catalini 等认为 Token 可以在无需传统受信任中介的情况下降低网络成本并启动网络。参见：Catalini, Christian, and Joshua S. Gans, 2016, "Some Simple Economics of the Blockchain", NBER Working Paper Series.

权益作用	可作为权益凭证进行记账、治理投票等	无
实用功能	可作为转账手续费、智能合约执行费用等	资产标记

表 3：两种 Token 的对比

三、 公有链的产业发展

公有链是一个全球化的信任平台，其应用产业即是在“平台”框架之上的垂直行业应用。目前来看，公有链已经探索了包括支付服务、保险服务、隐私、社交、娱乐、商业服务等多个领域。另一方面，在公有链内部也产生了与其自身相关的基础设施产业，如矿机生产、矿池、交易、托管、钱包等服务。

公有链应用	基础设施、支付服务、保险服务、隐私、社交、娱乐、商业服务等多个领域
公有链基础设施	矿机生产、矿池、交易、托管、钱包等

表 4：公有链产业划分

(一) 全球公有链发展头部效应集中

截至 2019 年 4 月，全球范围内的公有链项目共计超 400 个，其中实际主网上线的公有链大约在 100 个左右。[11]根据对实际上线公有链的链上数据进行分析发现，目前公有链发展头部效应明显，具体体现在以下四个方面：

一是从链上活跃地址数看。地址是公有链触发交易、合约的起点，因此链上活跃地址体现了公有链用户的参与量和参与活跃度。根据数据显示，比特币占据最多的 24 小时活跃地址数（80 万），以太坊占据第二（20 万）。

[11] 数据由区块链数据分析机构 bvaluate 统计。

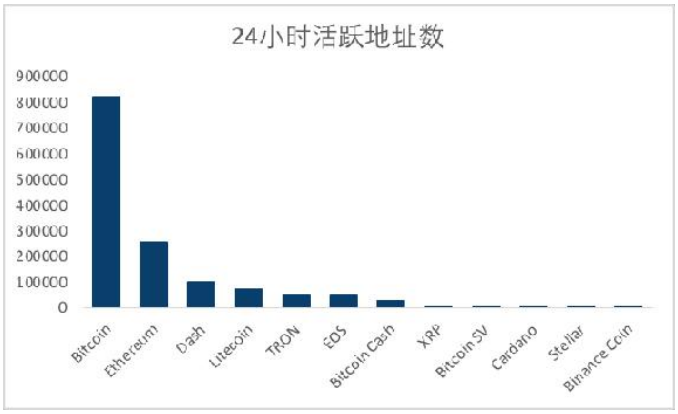

图 3：主流公链的 24 小时活跃地址数量

数据来源：messari，时间：2019 年 5 月 14 日

二是从链上交易（Transaction）总数看，交易是使用公有链最为基础的指令，链上交易量可以体现出公有链的使用量。数据显示，EOS、Tron、ETH 位列前三。

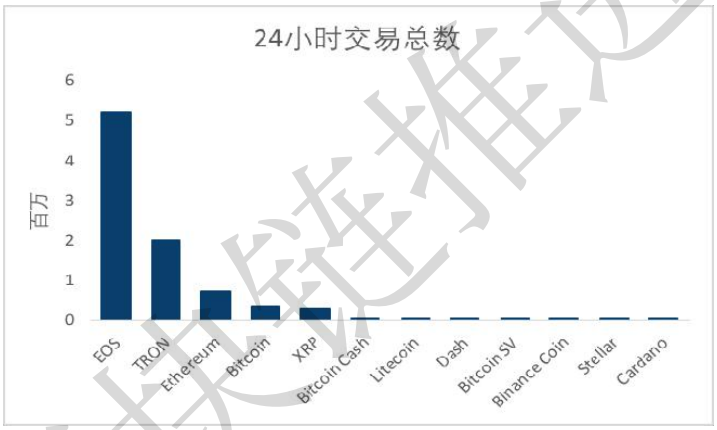

图 4：24 小时链上交易数

数据来源：messari，时间：2019 年 5 月 14 日

三是从链上交易量（折合美元）看。链上交易量（折合美元）是指一定时间链上价值量的指标，比特币链上交易价值量（折合美元）占据首位，以太坊次之。

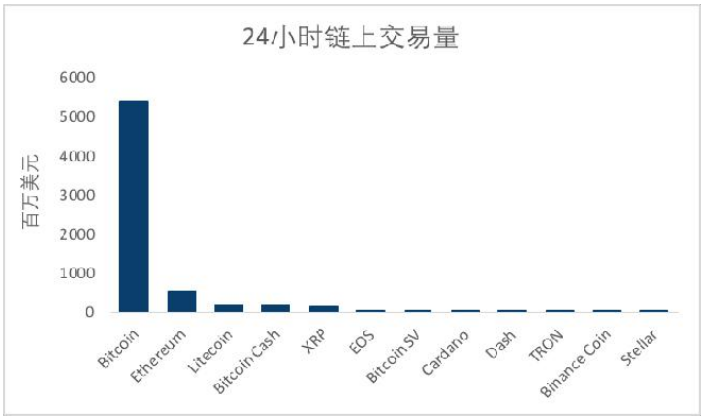

图 5：24 小时链上交易量（折合美元）

数据来源：messari，时间：2019 年 5 月 14 日

四是从开源开发者社区关注度看。以 GitHub 上各开源区块链项目的 Watch、Star 数为基础，可以体现出公有链在开发者社区的影响力和认可度。比特币、以太坊、EOS 居开发社区关注度的前三，其他收录的项目关注度水平非常接近。

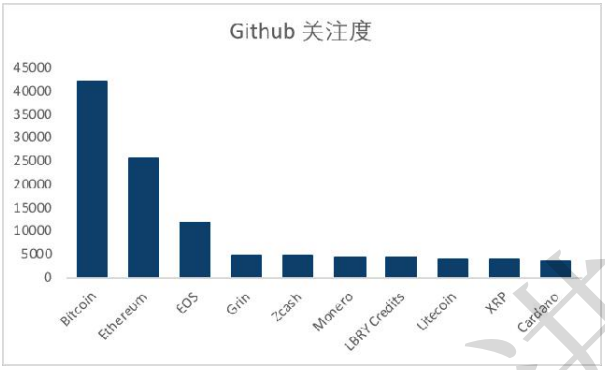

图 6： 全球公有链项目开发者受关注度排行 TOP10

数据来源：messari ，2019 年 5 月

(二) 全球公有链学术研究活跃

虽然公有链产业具有非常显著的头部效应，但全球的公有链学术研究日趋活跃。数据统计显示，全球范围内关于公有链的各类论文数量从 2016 年开始出现大幅增加，2016 年至 2018 年连续三年的增长率分别为 123%、144%、84%。2019 年前 4 个月的论文数量已达 588 篇，预计全年论文数量将达 2500 至 3000 篇。论文数量的逐年增长，反映出在政策、市场和技术等的多重利好推动下，学界对公有链研究兴趣的日益浓厚。[12]

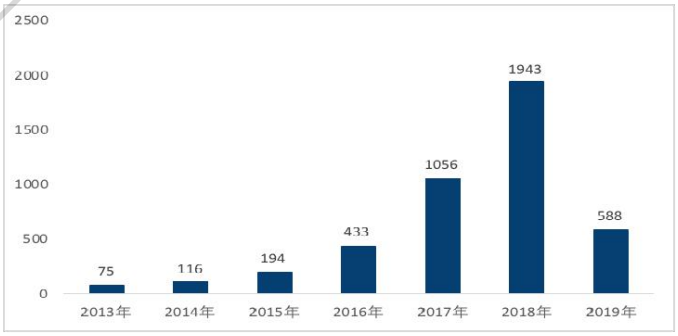

图 7： 2013 年以来全球公有链学术论文年度发布量

[12] 数据来源通过 Google scholar 检索关键词“Bitcoin、Ethereum 、Public blockchain”得到。

数据来源：Google Scholar 数据统计 2019 年 4 月

针对论文发布机构分析来看，2018 年全年公有链相关学术论文发表主要集中发布于康奈尔大学(Cornell University)的 arxiv.org 网站，以及 ResearchGate 的 researchgate.net 网站；电气和电子工程师协会 IEEE 的 ieee.org 网站及总部位于瑞士巴塞尔的 MDPI 网站 mdpi.com 为发布量第 3、4 名的发布机构。

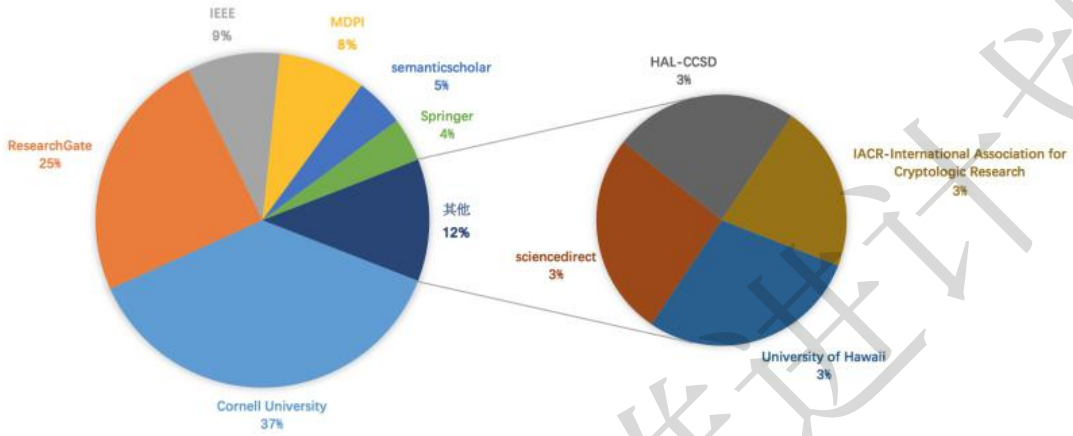

图 8： 2018 年公有链相关论文 Top 10 发布机构分布

数据来源：Bvaluate 数据统计 2019 年 4 月

从论文的研究方向和内容上看，国外学界的研究多围绕两点进行：一是公有链的底层技术架构和相关重大突破，二是政府政策。国内的学术研究旨趣则聚焦在公有链的场景应用上，从金融服务创新、电商、医疗、物联网、即时交易系统、著作权管理，到传媒、农业、教育、电力、房地产、土木工程、智能电网等行业或领域，均有涉猎。

(三) 公有链产业应用仍在探索中，“杀手级”应用尚未出现

目前，业界对于公有链的认识相对较为统一，但对公有链产业的概念尚缺乏明确的、公认的界定分类。本白皮书把围绕公有链技术及衍生出的产品、应用和服务形成的具有一定规模、商业模式较为清晰可行的行业集合视为公有链产业的主要构成。

在此概念下，无论是公有链底层的硬件制造、软件研发等，还是基于公有链的信用服务所触及的应用行业，如金融、能源、商业服务、物联网、游戏、文娱

等都属于公有链的产业据统计，目前全球 400 多个公有链项目的业务范围涵盖了支付、基础设施、支付服务、保险服务、隐私、社交、娱乐、商业服务等共计 65 个领域，其中 71.7%的公有链项目具有支付功能属性，33.3%的公有链项目涉及基础设施服务、支付服务、商业服务、隐私服务、娱乐、股权证明、物联网、社交、游戏等较多的领域，应用方向持续探索，但仍旧缺乏“杀手级”应用。

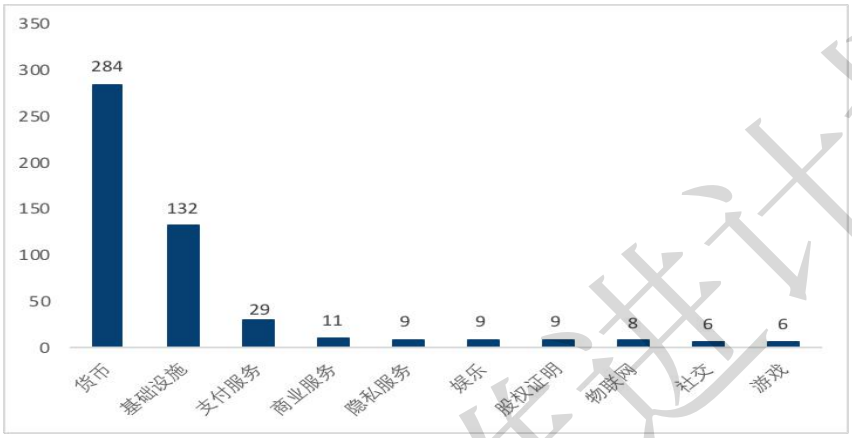

图 9：全球公有链项目涉及领域排行 TOP10

数据来源：Bvaluate 数据统计，2019 年 4 月

(四) 公有链与实体经济结合面临诸多挑战

相比于纯粹数字货币类的应用场景，以以太坊为代表的第二代区块链，将链式账本作为一种通用计算能力的标尺，由此可实现更为丰富的应用场景。然而，经过一段时期的探索，公有链真正走向实体经济仍存在相当的距离，其核心原因是现有公有链的内在逻辑难以适应当前社会、法律和商业环境。具体原因如下：

第一，身份适配问题，公有链本身缺乏身份认证系统，难以与现实主体进行勾连。现实世界的商业法律环境需要明确参与主体的身份，但由于区块链本身的设计有着“公私钥对自由生成”和“只认私钥不认人”的特性，现有参与主体都是以公钥哈希地址的形式标识，无法明确公钥地址背后持有者的身份主体。

第二，商业适配问题，公有链智能合约隐私性较差，且难以处理模糊或开放性合约。在实际的社会活动中，商业协议通常是保密的。然而，由于区块链的

透明性，现有智能合约代码及所执行的交易都会广播到整个网络，所有节点均会公开可见。因此，在大量的商业场景中，智能合约不具有隐私上的可用性。如果没有强有力的隐私保护机制，智能合约不适用像对关键供应商付款，敏感交易及等需高度保密的协议合约。同时，智能合约依赖形式化的编程语言，适合创建刚性代码规则管理的、客观可预测的义务，而不适合记录模糊或开放性的条款，或在签订合约时没有准确边界或明确的权利义务。

第三，数据适配问题，“预言机”（oracle mechanism）[13]机制不完善。公有链要与实体经济结合，必须要进行链下数据上链的环节。由于智能合约及公有链“一经部署，难以更改”的特性，如果智能合约的触发条件来自于外部世界，如某地的气温、商品货物的流转情况等等，则一定会涉及到外部信息上链。通常情况下，外部信息的来源是第三方数据源，但区块链只能保证来自于外部的数据无法篡改，无法保证真实准确。此时，外部信息的真实性就依赖于第三方的主体信用。数据上链问题导致智能合约重新需要依赖上链人的“信用”。尽管目前出现了多种去第三方的预言机方案，但仍没有一个普遍适用的方案存在。

第四，法律适配问题。现实经济活动是在像《合同法》、《公司法》等一系列法律的保障下进行的，而目前的公有链技术架构和设计与法律难以适配。同时，公有链承载的合约也缺乏法律的有效性的认定。例如，身份认证问题在法律上将导致责任主体不明，如果利用公有链的合约出现了法律纠纷，无法确立责任主体，则导致无法提起诉讼，这极大的限制了公有链的商用。

四、公有链的技术发展

以比特币为代表的可编程货币的出现让区块链技术走进大众视野，随后，以以太坊为代表的智能合约平台的问世设置了区块链技术商用的起点。但与此同时，现有的区块链技术尚无法支撑大规模商业应用的搭建，主流的区块链平台存在瓶颈和问题，迫使更多的开发者持续探寻区块链技术边界及新型技术方案。

根据对区块链行业发展历史及现状的综合分析得出，限制区块链规模化应用

[13] 所谓“预言机”是链下数据上链的机制。区块链网络本身没有直接的途径来获取外部世界的信息，无法自动的验证触发智能合约的条件，所谓“预言机”就是一个将外部信息导入智能合约的机制。

的技术掣肘主要在四大部分：可扩展性、互操作性、隐私性及安全性。

- 可扩展性：突破现有区块链技术的性能瓶颈，提升区块链系统的吞吐量，以满足主流交易网络高并发的性能要求，主要是通过**发展多样态共识、并行分片方案、二层网络方案及可验证计算**来解决和改善。
- 互操作性：实现不同区块链间的互操作，构建高效的连接机制，主要是通过**跨链机制**打通“区块链孤岛”。
- 隐私性：区块链技术的应用需要保障交易数据、合约数据用等多个方面的安全和隐私保护，主要是通过**假名、混币、环签名、Mimblewimble、零知识证明和可信计算解决。**
- 安全性：保证区块链安全可靠运行，特别是在智能合约方面。

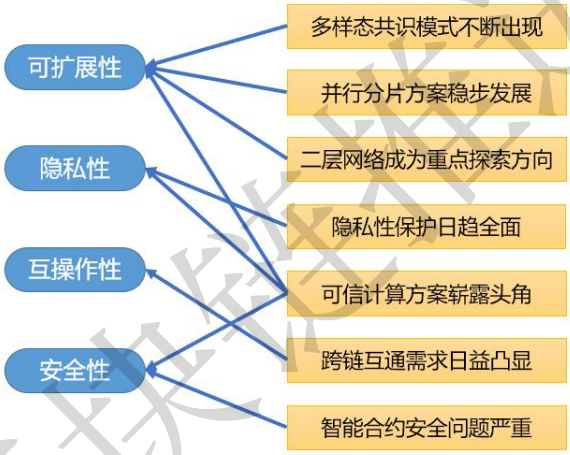

图 12：公有链的技术发展方向

	可扩展性	隐私性	互操作性	安全性
引发问题	主要指的公有链的 TPS（每秒交易）数难以满足日益增长的需求	公有链公开的特性，难以保证商用隐私的需求	区块链间的信息孤岛，无法进行互联互通	突出体现在智能合约安全问题上
解决方案	1、改变共识机	1、混币方案	跨链互通：	

	制 2、二层网络方案 3、并行分片方案 4、可信计算	2、机密交易 3、环形签名方案 4、Mimblewimble 方案 5、零知识证明 6、可信计算	1、中继/侧链 2、公证人机制 3、哈希锁定	

表 5：公有链的技术发展方向

(一) 多样态共识模式不断出现

共识算法用于协调系统中节点的行为和保持数据一致性。在不可信环境中组建的分布式系统，由于节点自身的不可靠性和节点间通讯的不稳定性，甚至节点伪造信息进行恶意响应，节点之间容易存在数据状态不一致性的问题。通过共识算法，区块链协调多个互不信任的节点的行为和状态，由此在不可信环境中组建一个可靠的系统。

共识算法是基于节点行为假设、治理模型和节点网络规模假设的系统实现。本质上，链上业务的特性和网络节点角色的定位决定了共识算法的选择。随着节点参与角色的多样化和业务交互特点的细分，出现了不同的网络假设和治理模型，如何成为可以真正实现的公有链项目，是共识的探索方向。这个方向催生了共识算法在共识顺序、共识轮次、终局性和节点选择方式等方向的差异，形成多样态发展的态势。区块链共识机制的演变也印证了这一点。

在区块链发展初期，主流区块链网络多用基于 PoW（proof of work）的共识算法。由于 PoW 存在资源浪费问题，2017 年后基于 PoS（proof of stake）的共识算法研究得到了迅猛的发展。单一共识算法均具有自身局限性，例如 PoW 共识效率低，DPoS 去中心化程度较低等，区块链研究者尝试将两种或者多种共识算法融合起来，取长补短，来达到更好的共识特性。新一代的共识算法，比如 Algorand、DFINITY、VBFT 等都属于混合共识算法。

指标项	内容	举例

容错性能	节点故障类错误	PoW（小于 100%），BFT（33%）
	节点作伪类错误	PoW（51%），PBFT（33%）
终局性性能	一个候选区块完成终局一致性所需要的时间	工程终局（比特币六个区块确认）
		数学终局（VRF、BFT 类）
扩展性	随着区块链网络节点数目与共识算法性能的相关关系	扩展性好（PoW、PoS）
		扩展性差（PBFT）
共识算法的网络模型性能	受网络波动和通信性能影响，共识算法的容错性和终局性	正影响（PoW）
		无影响（PoS）
		负影响（BFT）

表 6:共识算法性能的四个指标

	可容忍的恶意节点数量	**终局性**	**网络复杂度 (O为消息复杂度、N为网络规模)**	**实例**
PoW	小于1/2	算法不提供终局性	O(N)	Bitcoin
Tendermint	小于1/3	通过BFT实现	O(N^2)	Cosmos
Algorand	小于1/3	通过Byzantine Agreement实现	O(N*log N)	Algorand
EOS DPoS	小于1/3	通过BFT实现	O(1)	EOS
DFINITY	小于1/3	对若干历史区块的加权评估	O(N*log N)	DFINITY
VBFT	小于1/3	通过BFT实现	O(N*log N)	Ontology

PoW-DAG	小于1/2	算法不提供终局性	O(N)	PHANTOM Conflux

表 7： 主流共识算法比较

(二) 并行分片方案稳步发展

区块链采用共识算法解决分布式系统多个节点间状态一致性的问题。区块链系统中每个节点全量处理所有交易，单纯增加节点并不能提升区块链的性能（TPS），反而节点之间达成共识的过程对性能是一个损耗。

直接增加节点并不能提升区块链的 TPS，因为区块链上的交易没有负载分发机制，需要所有节点全量处理所有交易，无法并行处理。区块链的分片就是试图让链并行起来，将链分为多个分片链，然后通过一种负载分发机制，把交易分配给不同的分片执行，每个分片链独立运行，有独立的共识机制，通过并行的方案支撑比较强的水平扩展和按需扩展。分片技术的实现将为区块链各项事务活动的开展带来更高的协作效率与更加可信的生产方式。这种方案的难点在于跨分片的交易确认以及分片链的安全性保证。

因此，如何把分片的理论和区块链的安全理论，包括密码经济学设计、激励机制设计，这些融合在一起来实现一个安全可扩展，而且高性能的区块链是一系列的非常大的挑战。分片技术包含网络分片、交易分片和状态分片：

网络分片：要求分片的消息只在分片内部网络中传播；

交易分片：指不同交易将只在不同的分片中运行，每个分片运行独立的共识算法；

状态分片：要求分片只需要维护分片内部的状态数据而不需要保存其它分片的数据。

随着业务对区块链扩展性的需求量逐渐增大，公有链项目方对于分片有不同程度的尝试，不同的分片技术可以实现存储，通信，计算等不同层面的扩展。可以看到，分片相关的理论和工程化成果稳步发展。

(三) 二层网络成为重点探索方向

区块链二层网络（Layer2）技术旨在解决区块链扩容问题。区块链本身的容量是受限的，仅靠提高吞吐量很难满足所有的应用需求。

实际情况中，不是所有的交易都要在全球范围内达成共识，可以把部分交易以及合约执行只在所需范围内进行共识，以实现扩容的目标。广义的二层网络，包含了侧链，状态通道等各种将区块链的交易从链上迁移到链下（也可能是别的共识范围更小的链）的技术方案。二层网络设计中，脱离的链上共识的交易与合约如何与链上的共识挂接，保证交易和合约的合法性及安全性是需要解决的问题。[14]具体来讲，二层网络需要解决三类问题：

- 证明问题：链上没有全量数据的情况下，链下的交易最终如何给链上提交证明。
- 裁决和惩罚问题：裁决和执行如何进行以产生链下约束力。
- 监督问题：链下状态的监督[15]。

二层网络解决方案				
名称	**简介**	**优点**	**缺点**	**举例**
状态通道	参与方共同建立和维护一个通道，任何一方都可以将通道的最新状态公布到链上进	无需资金池托管[16] 证明和监督简单，吞吐量高	建立通道成本高 节点需要保持在线状态	闪电网络

[14] 以太坊社区将"反事实"（反事实状态通道（Counterfactual state channel））概念引入区块链，试图总结出一种二层网络的通用设计原则。法律本身的约束力也来自于这种反事实推理，如果合约一方违反契约，另外一方则可以通过法律来强制执行，交易双方最佳的策略是忠实执行合约，所以合约有了约束力。如果一个交易虽然没有发生在链上，但如果任何一方都可以让它在链上发生，则也同样产生了约束力，参与方可以假设这个交易已经在链上发生，然后进行下一个交易。

[15]

[16] 资金池托管难题：主要在于如何防止账本托管方作弊。由于链下状态的变化频繁，链下证明提交到链上有一个延迟。而用户要获取交易或者状态的证明需要账本托管方协助，要么托管方公布账本，要么提供专门的查询接口。仲裁机制上需要设计托管方不合作情况下的机制。另外，用户同时用户需要定期监控托管方提交到链上的证明是否作弊，以提交链上仲裁，并且有一定的时效限制。因为如果用户可以对很早以前的交易提起仲裁，会导致后面太多的交易处于不稳定状态。

	行清算			
多方链下账本托管	参与方将资金锁到一个公共的合约中，链下维护一个共用账本	无需建立通道，成本较低	需要资金池托管	
侧链账本	链下账本是一个独立的链，和主链以某种形式绑定，实现资产在主链和侧链之间流转	成本低	安全性依赖侧链本身的设计	
状态账本	逻辑与侧链类似，放弃记录交易，而只记录每个账号的状态，提交给主链的是状态证明			

表 8：二层网路解决问题及方案

(四) 隐私性保护日趋全面

在区块链系统中，用户希望自己的身份、资产状况、交易历史等信息都被尽可能少的人知道。一个完美的隐私性的支付系统中，每笔交易的信息都仅被参与这笔交易的双方知道。作为一个所有交易都要被公开和全网验证的系统，公有链在设计之初就应该考虑隐私性的需求。

1. 假名方案

比特币采用的方案是使用可以任意选取的、和真实身份的无关的公钥地址来作为持有资产和参与交易的主体，并通过地址对应的公钥和数字签名来验证对链上资产的所有权。比特币实现了一个用户使用“假名”的支付系统，用户的真实身

份被隐藏在公钥地址背后。类似的方式也被使用在其他很多公有链项目的设计中，在公有链发展的早期也较好地满足了当时人们对于隐私性的需求。

2. 混币（CoinJoin）方案

混币方案让多个用户共同创建交易来变更其代币的所有权，通过混淆发送者和接受者之间的对应关系来增强用户的匿名性。以下图为例，如果没有采用混币，则很容易看到 Alice 付了 8 个 BTC 给 Carol，Bob 付了 15 个 BTC 给 Ted，结合其他交易信息进行交叉分析就很容易发现这些用户的真实身份；而进行混币以后就只能看到{Alice, Bob}向{Carol, Ted}发送了比特币，但是无法精确判断发送者和接受者的对应关系。通过不同的用户间多次重复混币操作，最终就会把可能的发送者和接受者集合都变得很大，从而保护其中每个人的匿名性。

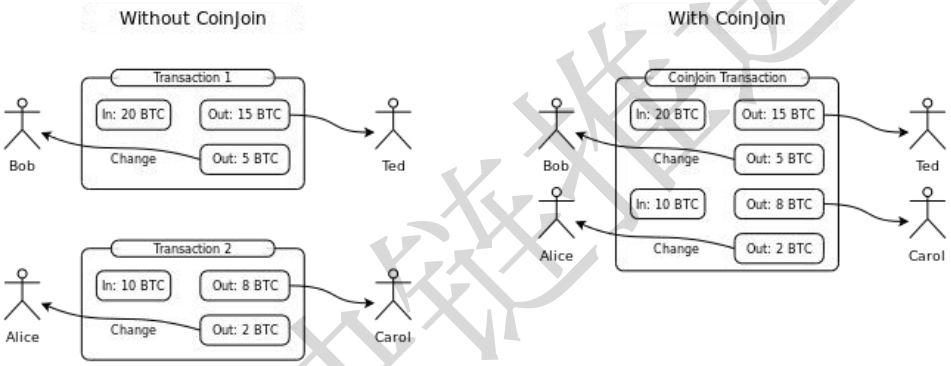

图 13：混币的基本原理

3. 机密交易（Confidential Transaction）组件

机密交易是由 Adam Back 和 Greg Maxwell 在 2013 年提出的增强比特币隐私性的提案，可以实现对于交易金额和账户余额隐私性的保护，即其他人虽然可以看到 Alice 发送了一些代币给 Bob，但是无法知道具体发送了多少。

机密交易的核心思想是用一种称为 Pedersen Commitment 的承诺方案代替以（哈希地址，金额）的方式存储每一笔交易的输出，然后用同态加密的方式验证每笔交易中发送的总金额和接收的总金额是平衡的。在矿工看来，只需要对着输入输出的同态加密密文做一些线性运算就能验证一笔交易的金额是合法的了，整个过程中无需把交易金额暴露给矿工。机密交易它提供了一种简单高效的隐藏交易金额的方法，在以后的很多隐私保护方案中都被作为组件使用。

4. 环签名（Ring Signature）方案

混币方案最大的缺陷就在于当参与人数不够多的时候能提供的隐私性保护非常有限。环形签名方案就是让其他用户在不知情的情况下“被动地”参与到混币中来，达到隐私保护的目的。简单来说，环签名技术允许一个用户列表中的任何一个用户都能独自生成一个合法的签名，且不同的用户生成的签名看上去是一样的。进行交易时就只能验证一笔交易的所有发送者中的某一个许可了这笔交易，而无法精确判断具体是哪个发送者签名的，因此也无法判断交易真实的发送者。

另外，为了保护交易接收方的隐私，还可采用了潜行地址的技术。潜行地址技术允许发送方根据接收方公开的信息生成一个一次性的公钥地址，这个地址依然由接收方通过私钥控制，但是其他人无法从这个一次性地址关联到接收方的身份。通过环签名加上潜行地址的方式，对交易不可关联性方面的表现至少等同于多名用户参与的混币交易。而且由于协议强制要求每笔交易必须选择多个输入进行环签名，所以其实际上隐私性要高于只有少部分有需求的用户使用的比特币混币方案。

5. Mimblewimble 方案

Mimblewimble 方案的所有交易都以机密交易的方式进行，并且强制采用了区块级的混币和交易裁剪技术，因此它能够提供比单纯使用机密交易或者混币都更好的安全性。按照 Mimblewimble 协议，矿工会把每个区块中所有的交易混合成一笔交易，从而隐藏发送者和输出者之间的关联性。更进一步地，矿工们会从交易历史中删去已经被花掉的交易输出，只保留尚未被使用的交易输出（UTXO）。因此，其他人就很难再对历史交易进行关联性分析了。最好的情况下，一个新加入的节点相当于只能看到从 coinbase 到 UTXO 转账的一笔交易，除此以外得不到任何信息——UTXO 中每笔输入的金额都是隐藏的。

6. 零知识证明（Zero—Knowledge Proof）方案

零知识证明技术允许证明者在不告诉验证者任何关于 x 的具体信息的情况下，让验证者相信证明者是确实知道 x 的值的。原始版本的零知识证明技术是基于交互式证明设计的，并不适合直接用到区块链上。适合区块链使用的零知识

证明必须满足两个条件：非交互性，即证明者只生成一个证明，此后便可由不同的验证者分别验证证明的正确性；易验证性，即验证一个证明所花费的计算资源非常低。此外，为了节约宝贵的链上共识数据吞吐量，最好这个证明的长度也尽可能简短。

利用密码学技术在比特币上实现隐私保护功能吸引了很多密码学家进行研究。2012 年 Bitansky 等首次提出了“零知识的简短非交互式证据”（zk-SNARK for zero-knowledge succinct non-interactive argument of knowledge）的概念，其中简短和非交互两点即为在区块链上应用所必须的特点。“证据”是指这种方式在原理上是存在伪证的可能性的，只不过因为找到一个伪证需要天文数字的计算量，所以作为证据还是很有说服力的——毕竟如果攻击者可以完成那么大的计算量的话，任何加密算法都会被破解，也就无所谓伪证了。

零知识证明技术具有非常巨大的潜力。首先，零知识证明是一种通用的证明技术，可以证明任何计算的正确性，这与只能证明转账交易合法性的机密交易技术有着本质区别。因此，零知识证明技术可以解决更复杂的系统中的隐私保护问题。其次，零知识证明技术的另一个优点是明确地区分了计算和验证，使得验证的成本可以比计算低很多。这使得在区块链上以较低成本进行复杂运算成为了可能——这对于现有公有链是难以想象的，因为在这些公有链上验证一个状态的正确因为在这些公有链上验证一个状态的正确性需要所有节点重复执行一遍整个计算过程，效率自然非常低。最后，零知识证明技术还可以用于压缩交易历史，让节点在无需存储所有历史交易的情况下依然保持几乎相同的安全性。这点对于一个高吞吐量的公有链项目尤为重要。

方案	存在的问题
假名	每个地址上存储的比特币数量都是公开的；已经发生的所有交易都是公开的，可以通过交易之间的关联性和使用模式等分析识别出地址对应的用户的身份；用户在发起并广播交易的时候也会暴露自己的 IP 地址，这也会在一定程度上泄露用户的身份信息。[17]

[17] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S., 2013, October. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference

混币	隐私性依赖于参与混币的用户数量，而实践中每项混币交易的参与者往往不超过 4 个；通过对混币的发送和接收金额进行分析可以一定程度上推测出关联性；事实上，研究人员能够将 67%的混币交易去匿名化。
环签名	因为环签名技术本质上包含发送者集合中每个人的一个签名，造成交易的体积较大（每笔交易大约 10KB）。
Mimblewimble	矿工知悉发送者和接受者的对应关系；对脚本和合约等支持较差
零知识证明	现有的零知识证明技术尚不够成熟，使用的成本过于高昂；理论结构复杂，大部分零知识证明方案都只能停留在理论设计和实验代码阶段；存在安全隐患，复杂的零知识证明系统需要基于很多密码学假设，其中任何一个不成立都会令整个系统失效。

表 9：隐私保护各方案对比

(五) 可信计算方案崭露头角

在区块链的应用场景下，可信计算的目标主要有两个：一是数据隐私保护，即除了指定的计算任务外，用户的数据不应当被擅自挪作他用；二是可验证计算，这是对于计算过程的真实性和完整性的保护，使得用户不需要重复执行运算即可验证计算结果是否正确。目前用于实现可信计算的技术主要有基于硬件安全的可信执行环境（Trusted Execution Enclave，TEE）和基于密码学的全同态加密技术（Fully Homomorphic Encryption， FHE）等。

1. 可信执行环境

可信执行环境的基本原理是给每个支持 TEE 功能的芯片分配一对公钥和私钥，公钥与芯片序列号一起公开，私钥存储在 TEE 内部。需要进行安全计算时，用户首先与 TEE 通信建立一个临时性的会话密钥，然后把输入数据用会话密钥加密后发送给 TEE 在受保护的独立的区域内将输入数据解密后完成计算，

on Internet measurement conference (pp. 127-140). ACM.

最后用会话密钥把计算结果加密返回给用户。为了验证计算的正确性和完整性，通常计算结果中还会包括关于计算任务的快照以及使用 TEE 私钥做出的签名。

可信执行环境的逻辑在于整个计算过程中输入和计算结果只在用户端和 TEE 内部以明文的方式出现。只要不暴露 TEE 内部信息，即使可以完全控制服务器的操作系统也无法窥探或篡改计算结果。对芯片直接进行测量的难度极高，大大提升攻击难度。

TEE 技术的主要优势在于计算的成本较低[18]。对于区块链来说，TEE 技术可以大幅度降低验证智能合约执行的成本，彻底改变链上所有运算都要被所有全节点分别执行一遍的现状，突破单点的硬件性能对于区块链吞吐量的限制。目前 TEE 技术已有一些商用产品，例如英特尔（Intel）2015 年推出了采用 SGX（Software Guard Extensions）技术的处理器，近两年也有一些区块链项目支持用 SGX 验证智能合约等复杂计算的运行结果。

TEE 的主要缺点有两个：首先，每个 TEE 芯片初始的密钥必然是由芯片制造厂商产生和分配的，因而芯片厂商是一个必须信任的中心化节点；其次，TEE 芯片虽然通过独立封装硬件的方式将其与服务器中的其他程序隔离开来，但是仍然可以通过旁路攻击的方式间接地获得芯片内部运行状况的信息。例如 2018 年 3 月份，美国俄亥俄州立大学的一个研究小组展示了一种名为“Sgx Spectre”的新型攻击技术，可以通过观察多次重复执行中缓存区大小的细微变化实现从 SGX 中提取数据的效果。

2. 同态加密/全同态加密

加密算法的同态性指的是对于密文信息进行一些运算后，得到的新的密文与原密文所对应的明文有某种可以预测的对应关系。例如加密算法 Enc 满足对于任意的 x 和 y，Enc(x)+Enc(y)=Enc(x+y)，就可以说 Enc 对于加法具有同态性。常见的如 RSA 加密算法和椭圆曲线群都是关于加法同态的。全同态加密[19]对于

[18] TEE 计算实际上是以明文的方式进行的，这种特点使得用户能以较低的成本安全地使用远程芯片，特别适合于云服务器厂商提供安全可靠的外包计算服务。

[19] 对任意运算都满足同态性的全同态加密算法基本上都是基于格（Lattice）密码学假设的。还有一种“有点同态（somewhat homomorphic）”的加密算法，此类算法对加法和乘法都具有同态性，但是由于误差累积的缘故仅允许在密文上进行很少几次乘法。实际上，Gentry 于 2009 年提出世界上第一个全同态加密算

加密算法的结构性要求则更高一些：对于任意函数 f，都可以通过在关于 x 的密文上进行一系列操作得到一个新的对应于 f(x) 的密文，即 Eval(f,Enc(x))=Enc(f(x))。全同态加密对密文进行的运算的整个过程中不会用到解密密钥，因而其作为加密算法的安全性可以保证不会泄露任何关于输入 x 或者计算结果 f(x) 的信息。

全同态加密算法可以很好地解决数据隐私保护的问题，在有可信的安全设置（trusted setup）的前提下也可以实现可验证计算，是一种应用前景非常广阔的通用技术。目前限制同态和全同态加密算法广泛应用的主要瓶颈在于其过低的执行效率[20]。提高效率是现在全同态加密算法研究的核心方向，但是如果要获得大幅度改进需要理论密码学上的重大突破。

(六) 跨链互通需求日益凸显

跨链技术的核心在于让不同的区块链能跨越彼此的障碍，从而在数据和价值的层面进行相互流通。跨链技术的本质是为了解决不同区块链之间的互通性。而这种互通性正是目前区块链在场景落地中碰到了一个非常核心的难题，不管是公有链还是联盟链，跨链技术都是实现价值互联网的关键，也是避免目前各个不同的区块链分别发展，导致数据孤岛的唯一途径。在具体的实现层面，由于跨链技术实现了多条区块链之间的逻辑关联，所以在很多应用场景中，跨链技术也会被应用到拓展区块链事务处理能力方面。

类别	公证人	侧链/中继	哈希锁定

法正是通过控制有点同态的加密算法的误差改进而来的，而现有的全同态加密算法也都基于相同的框架。

[20] 一般来说，同态加密运算是明文运算效率的千分之一左右，全同态加密运算是明文运算效率的百万分之一

跨链方向	双向	双向/单向	双向
资产交换	支持	支持	支持
资产转移	支持	支持	不支持
信任	需要第三方	不需要	不需要
类型	协议	技术架构	算法
难度	中等	困难	容易
案例	Ripple	BTC relay Poldadot COSMOS	Lightning network

表 10：跨链各方案对比

(七) 智能合约安全问题尤为严重

智能合约是一种旨在以信息化方式传播、验证或执行的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。智能合约的出现使得区块链的扩展性和便捷性获得极大的提升，但图灵完备的合约也带来了更多的安全风险。2016 年 6 月 17 日，当时区块链业界最大的众筹项目 The DAO(被攻击前拥有 1.5 亿美元左右资产，约占当时发行的以太币总量的 14%)遭到攻击，并导致 360 万的以太币资产被分离出 The DAO 资产池(当时价值约为 5000 万美元)。该次攻击事件直接导致了以太坊硬分叉为 ETH 和 ETC。2017 年 11 月 7 日 Parity 多重签名合约漏洞导致 93 万个以太币（当时价值约 150 亿美元）永久丢失。相关数据显示，2018 年整个区块链行业因为安全问题导致损失金额超过 20 亿美元。针对区块链行业发起的所有攻击中，交易所和智能合约是最受

攻击者关注的攻击点。

目前，智能合约安全问题的主要有以下四个方面：

漏洞类型	攻击方式	攻击原理
基于智能合约编程语言的漏洞	整型溢出	以太坊的合约虚拟机（EVM）为整数指定固定大小的数据类型。这意味着一个整型变量只能有一定范围的数字表示。在智能合约开发中，如果没有检查用户输入就直接执行计算，可能导致数字超出存储它们的数据类型所允许的范围，该变量就很有可能被用来组织攻击。
基于区块链平台特性的漏洞	重入	以太坊的智能合约能够接收和发送以太币。调用外部合约或将以太币发送到合约地址的操作需要合约提交外部调用。这些外部调用可能被攻击者劫持，迫使合约执行进一步的代码（即通过回退函数），包括回调自身，因此代码执行"重新进入"合约。
	随机数	由于大多数区块链平台本身不提供随机数生成接口，智能合约只能自己实现随机数生成算法，如果智能合约本身生成的随机数算法不当，可能导致随机数被提前预测、或者可被篡改。
基于业务逻辑的漏洞	越权调用	由于公有链的开放性，任何地址都可以与区块链上的智能合约进行交互，如果智能合约的函数中未做权限限制，那么任何地址都可以成功调用此函数，如果该函数为敏感函数，智能合约可能会因此遭受攻击，造成合约控制权限丢失或者直接导致资产损失。
基于合约虚拟机的漏洞	逃逸漏洞	虚拟机在运行字节码的时候会提供一个沙箱环境，一般用户只能在沙箱的限制中执行相应的代码，此类型漏洞会使得攻击者退出沙箱环境，执行其他本不能执行的代码。
	逻辑漏洞	虚拟机在发现数据或代码不符合规范时，可能会对数据做一些“容错处理”，这就导致可能会出现一些逻辑

		问题，最典型的是“以太坊短地址攻击”。
	堆栈溢出漏洞	攻击者可通过编写恶意代码让虚拟机去解析执行，最终导致栈的深度超过虚拟机允许的最大深度，或不断占用系统内存导致内存溢出。此种攻击可引发多种威胁，最严重的是造成命令执行漏洞。
	资源滥用漏洞	攻击者可以在虚拟机上部署一份恶意代码，消耗系统的网络资源、存储资源、计算资源、内存资源。所以在虚拟机中必须要有相应的限制机制来防止系统的资源被滥用。在以太坊中采用的是 gas 机制，攻击者想要在以太坊虚拟机上进行操作，需要支付 gas。

表 11： 智能合约安全问题

五、 公有链的治理

从社会组织的角度，公有链发展过程是一个通过区块链协议组织社区的过程。公有区块链因其透明的分布式记账方式与建立在博弈论基础上的经济激励机制，使得全球范围互不相识的人共同参与到同一个系统的协作中。但是以“去中心化”为特征的公有链并不是去组织化，相反，由于对公有链协议的认同与参与，在网络上形成了自发性的组织形态，即社区。

社区是基于公有链的组织形态，也是决定着公有链的技术走向共同体。公有链作为软件产品，一定会随着需求和变化更新升级，而技术升级与更新的方案选择则需要决策与选择，并达成统一意见一致。这个社区内决策、选择并达成一致的过程叫做公有链的治理。

(一) 公有链治理是参与者对决策达成一致的过程

决策无法避免分歧与争论。由于参与者的角色和利益不同，区块链协议在修改和升级的过程中往往会出现各种分歧，严重的情况下会导致区块链的硬分叉。硬分叉是指区块链发生永久性分歧，在新共识规则发布后，没有升级的节点无法

验证已经升级的节点生产的区块。业内著名的硬分叉事件是比特币（BTC）的硬分叉。由于社区对比特币扩容方案有不同意见，最终导致 BTC 硬分叉成 BTC 和比特现金（BCH）。因此，区块链的治理是区块链社区和生态中利益相关者对决策达成一致的过程。如何既保证社群的稳定、又能保证社区的去中心化，治理机制就是关于决策机制、财务结构、社区分歧解的系统化安排。

本质上，治理架构是区块链最顶层的设计，它涉及到社会、经济方面的各要素，良好的区块链治理机制有助于减少分裂和混乱的发生，帮助提高软件的更新迭代效率，让区块链协议适应不断变化的环境，并提高社区成员的参与度，促进公有链生态稳定健康发展。

(二) 公有链治理的架构与特征

为了分析不同的治理模式，首先需明确典型公有链生态系统中的治理参与者。公有区块链是以开源软件社区为基础，通过代码迭代和多方共同维护一个商业价值网络信用体系。一般来说，公有区块链治理生态构成由四种角色组成：**区块链协议开发者、矿工、上层应用开发者及用户**。

1. 开发者

开发者对区块链基础协议进行开发、维护和更新，是区块链协议顶层的制定者。一般情况下，在区块链项目的起始阶段，由于项目的影响范围有限，开发者往往是项目的创始团队，例如比特币的初始版本是由中本聪独立开发完成，以太坊的初始版本也是由 Vitalik 及其核心成员完成。

随着项目的推进和社区的发展，由于公有区块链社区极高的开放性，项目的版本更新和技术开发人员也逐渐转移为社区化。正如所有的开源开发者社区一样，开发者们会自发的形成自组织来判断提交的代码的合法性。

2. **矿工**

矿工根据共识算法的规则对整个区块链网络的交易信息进行验证并记账。以当前使用最为广泛的 POW 共识算法为例，矿工主要是通过比拼计算能力来争夺记账的权利。区块奖励机制，则会不断吸引社区成员参与挖矿。由于掌握算力的矿工有着出块的权利，因此，在一定的情况下，矿工团体会对区块链网络的分叉产生重大影响。矿工主要经济动力是为了赚取区块奖励和交易手续费。

3. 上层应用开发者

上层应用开发者在公有链基础上进行应用开发，借助于区块链的一般性共识和信任服务来提供针对性的服务。作为区块链的使用者，上层应用开发团队对于公有链的底层设置及资源配置有着特殊的诉求，他们倾向于使用交易费用低且保持系统高效安全运转的公有链。

4. 用户

用户是区块链网络的最终使用者，是区块链价值的持有者和使用者。从根本上讲，用户是区块链价值的本质基础，但他们往往处于较为被动的角色。我们可以将整个区块链生态划分为两种参与者：积极参与者和消极参与者。开发者、矿工与上层应用开发者主动地参与贡献基础协议、网络维护及应用开发，是生态的积极参与者。而一般的用户除了持有和使用之外，对于网络和协议没有更多积极的贡献。

然而，在公有区块链系统中，由于占据了价值的中心，占绝大多数的消极贡献者（用户）承担了重要的地位。以比特币治理模式为例，用户虽然没有在底层协议、网络记账及应用开发方面积极贡献与创造，但却拥有选择的权利。当社区内部出现分歧时，用户在协议变更和算力战中无法起到作用，但最终会在价值市场上做出选择。换句话说，积极参与者的贡献需要消极参与者的认可才能有实际的经济意义，庞大的用户价格市场上最终决定了公有链的认可与发展程度。

参与者	权利	义务
开发者	对区块链基础协议进行开发、维护和更新，是区块链协议顶层的制定者	开发者们形成自组织来判断提交的代码的合法性
矿工	对公有链出块奖励、手续费等有着特殊诉求，并在一定情况下，矿工会对区块链网络的出块选择和协议选择产生影响	根据共识算法的规则对整个区块链网络的交易信息进行验证并记账
上层应用开发者	对公有链的底层设置及资源配置有着特殊的诉求，如 gas 费	在公有链基础上进行应用开发，借助于区块链的一般性信任服务来提供针对性

		的服务
用户	是区块链价值的持有者，有选择公有链的权利	用户是区块链网络的最终使用者

表 12：公有链治理参与架构

通过对于上述四种参与者的分析可以发现，区块链生态的参与者有着不同的利益诉求，协调参与者的利益诉求十分重要。一个成熟的区块链生态，应该是参与多方各自独立、相互制约制衡，没有一方具有绝对的权利。虽然任何一方都无权单独进行决策，但参与方通过行使各自的权利不断互相博弈，最终达到动态平衡。

公有链治理的博弈既包括生态内部的博弈，也包括来自生态外部博弈。内部博弈是指上述生态内部的参与者之间的博弈，比如以太坊的 gas 价格，矿工希望 gas 价格提高，从而获取更高的区块奖励；而应用开发者和用户则希望 gas 价格下降，从而降低部署和使用合约的成本。双方博弈的结果决定了最终的 gas 价格。内部博弈甚至可以发生在同一类参与者之间，例如以太坊的矿工可以对 gas 上限进行投票，部分矿工会选择提高 gas 上限，从而获取更高的区块奖励；而 gas 上限的提高会提高叔块（uncle block）的概率，影响另一部分矿工的利益，因此这部分矿工会选择降低 gas 上限。两类矿工不断博弈，gas 上限最终达到动态平衡。除上述四类治理的参与者外，外部生态往往也起着重要作用，外部生态可以间接影响价格，从而影响矿工的成本，形成以价格为核心的博弈，最终使整个生态重新达到平衡。对公有链来说，博弈的过程就是治理的过程，而博弈的结果就是公有链的演进方向。

(三) 公有链治理的模式

由于公有链生态的复杂性，任何单一的参与主体都无法决定公有链生态的走向和发展，重要的决策都是通过协商完成，从决策模式来看，公有链的治理包含链上治理和链下治理两个部分。

1. 链下治理

链下治理是决策过程不发生在区块链系统之上的治理模式，其治理基础是

围绕着开源社区展开。

开源开发社区包括许多短期贡献者和长期贡献者。他们不但贡献代码，也负责调查研究、同行评价、测试、文档和翻译等工作。一般来说，开发工作是在类似于 GitHub 的代码托管平台上进行。开源社区不是一个机构实体，而是一个以线上为主的松散组织。原则上，任何人都可参与公有链项目的开发与贡献，但这并不意味着任何代码都可以随意合并到主分支中，合并代码需要维护人员完成。

项目维护人员是通过在一段时间内提供高质量代码，并且在项目中建立了足够社会资本的贡献者。当现有的维护人员组认为，某个贡献者表现出的能力、可靠性和动机足以胜任，他们可授予该贡献者 GitHub 帐户的提交访问权。而首席维护者的角色是负责监督项目的所有方面，并负责协调发布的人。

代码的“维护者”虽然掌握了项目合并的资格，但这并不意味着绝对的权利地位，因为一旦其不公正或滥用权力，不满意的“贡献者们”可以随时离开，并且可自由地运行自己的软件，或者选择分叉原有的软件。

链下治理典型的例子包括比特币改进提议（BIP，Bitcoin Improvement Proposal）和以太坊改进提议（EIP，Ethereum Improvement Proposal）。

BIP 是一项提议改进比特币协议的标准，任何人都可以通过 BIP 对比特币协议提出改进的想法。BIP 提供了一套标准化的流程，以便人们提出的想法可以得到专业的评估以及测试。

BIP 的实施需要经过提出阶段（Proposed），草案阶段（Draft），以及落地阶段（Final）。第一阶段，任何人都可以通过社区等渠道提出初步改进想法，争取更多人支持认同，提议者需将想法提交给比特币邮件开发列表；第二阶段，BIP editors 对重要或者认可较多的提案分配 BIP 序号，将其状态设置为“Draft”，并将其添加到 GitHub 代码仓库；第三阶段，一旦 BIP 被接受，需要对其进行代码实现，若代码经过测试并被社区接受后，状态会被设置为“Final”。

在此过程中，BIP 也可能被社区推迟（Deferred）、拒绝（Rejected）、撤回（Withdrawn）、替换（Replaced）或者激活（Active）。当某些 BIP 不需要实现时，其状态可以设置为“Active”，例如 BIP1 中只是对 BIP 具体的工作机制进行描述，并不需要具体的代码实现。

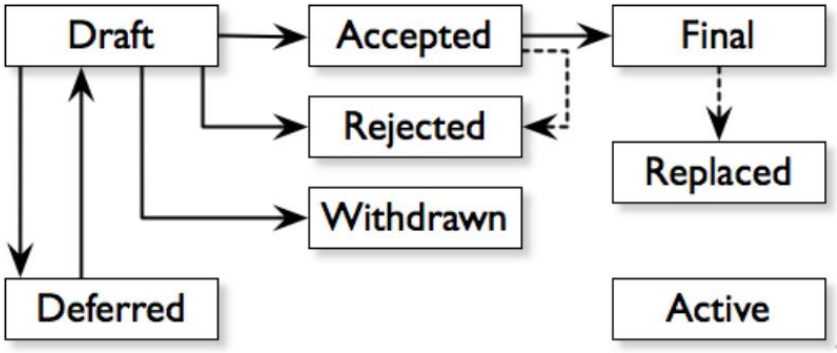

图 14：BIP 的决策流程

和 BIP 类似，EIP 是以太坊上用于提议改进协议的标准。在 EIP 标准中，参与方包括 EIP author，EIP editors 以及以太坊核心开发人员。EIP editors 按照如下流程处理每个提案：Active、Work in progress（WIP）、Draft、Last Call、Accepted、Final。其他例外情况包括 Deferred、Rejected、Active 以及 Superseded。

2. 链上治理

相比于发生在链下的社区治理，链上治理是指网络升级迭代的决策过程是嵌入在区块链系统内部，利用区块链内在的机制完成的治理方式。

链上治理最为常见的解决方式是允许 Token 持有者通过在链上投票的方式决定社区治理的决定。链上治理的投票既包括代理制投票，以去中心化的方式选出核心组织行使权力，如选出超级节点、主节点等；也包括投票并直接实施协议升级。

以全员投票 Tezos 的机制为例，预备更新的代码需要连续投票通过，才能部署至测试网乃至上主网。投票权是通过权益，即 Token 的数量来进行权重；其次在投票的初期，基金会具有否决权，同时，投票率要达到 80%以上方能被系统认定为提案通过。

链上治理除上述只允许 Token 的持有者参与投票的方式外，还可引入生态中其他参与者，包括协议开发者、社区成员及矿工等，进行多方参与的链上投票。由于链上治理的投票往往是通过智能合约完成的，因此具有自动性和强制执行性，可以迅速发展并接受必要的技术改进。链上治理过程公开透明，流程易于审计和回溯，有利于确保流程的贯彻执行，从而提高协调性和公平性，也允许更快的决策。

治理模式	链下治理	链上治理
参与者	开源开发者	Token 持有人
前置条件	对持有 Token 无要求	原则上须持有 Token
参与形式	链下协商 （社交网络、邮件列表、电话会议等）	链上利用智能合约进行投票决策等

表 13：两种治理模式的对比

链上治理的优势很明显，但实际上它同样带来了新的问题：

第一，链上治理中，投票决策实际上是将权力转移到资产持有者手中。但大量的资产持有者对于技术的判断能力极为有限，所通过的提案未必代表项目长期发展的利益。

第二，由于投票的权重是基于 Token 持有量。那么投票过程很可能会刺激资产价格波动，此外，如果链上治理的投票权被少数人掌握，将形成决策被寡头垄断的局面。

第三，链上治理是希望能够满足社区大多数人的意见，但在从目前已知的几次公有链链上治理的案例来看，参与投票的往往只是极少部分持币者，导致最终治理结果仅由投票参与者中少数持币较多的大户决定。

第四，链上治理的投票机制可能会遏制新技术的发展，相比于“硬分叉”，“投票”消灭了探索其他技术的空间。以一个理性和长远的这个角度去看，“分叉”可能不是一件糟糕的事情，它固然可能导致社区出现分裂，甚至有可能对生态发展造成阻碍，但这一过程，同时也会使得社区间有更多的沟通，自由地探索更多的技术发展方向。

六、 公有链的监管

公有链是一个新兴的技术发展方向和特有的产业发展领域，以去中心化治理和激进市场实验为特色，引起了全球科技、经济、法律和政府人士的广泛关注。但公有链社区及其产业并非法外之地，“Code is Law”的激进法律和社会实验也不

能以社会其他人群的受损为代价。因此，对公有链的社区和产业的基于现有法律的监管研究势在必行。相比于主要针对于社区内部参与者的治理过程，监管主要聚焦在公有链对社会整体产生的影响方面，监管的参与者也主要是相关的立法、行政等部门对于技术的监督和规范化。

分类	公有链的治理	公有链的监管
范围	社区内部参与者	社会立法、行政等部门
目的	对于公链自身的技术、商业发展走向的决策	对公有链及其产业的监督和规范化

表 14：公有链监管与治理的对比

(一) 公有链监管总体论述

监管可以从三个维度进行考虑。其一，监管部门对新技术发展可能被某些人滥用，或者冒用新技术发展的名义损害他人合法权益的情况进行监测和追责。纯粹的技术发展和经济实验是中立的，但是使用技术和参与经济实验的人并不是中立的。因此，任何与新技术使用有关的侵权行为、违法犯罪行为并不应当其与新技术有关而得到当然的豁免。其二，对新技术和新经济发展当中，政府提供认证、统计信息、金融数据、财产登记数据等公共产品，以改变或者改善经济博弈结构，提升经济效率，解决产业发展瓶颈的公共管理服务也是监管的重要作用。其三，积极的监管实践可以帮助监管部门更好的发展监管工具，更加深入的理解产业逻辑，为实现监管目标提供事半功倍的解决方案。

自公有链技术诞生之初，其内在就有着抗审查、抗监管的技术特性，但这一技术能力是基于密码学和博弈论的，并非依赖任何一个个人或团体而生存和发展。同时，公有链技术的这些技术特点并非无法加以利用或限制，同时也为监管工具和产业政策的发展提供了足够的空间和想象力。

公有链技术特点	抗监管的特性	监管方利用和限制思路

假名地址	匿名交易	发展公有链账本大数据工具
公私钥对	无法冻结的财产	发展加密资产信托业
点对点网络	无法制止的转账 （洗钱、货币转移）	法币与加密资产交易实名制 AML、KYC 制度
状态难以回滚	无法删除的记录	区块链浏览器信息处理

表 15：公有链的技术特性与监管

1. 公有链监管的特点

目前，公有链仍处于发展初期阶段，对公有链的监管手段仍不完善。对公有链的监管也不同于过去任何一种监管模式，具有非常鲜明的特殊性。正如本白皮书在上一章节：《公有链治理》中指出的，公有链是一种新型的社区及商业形态，是以开源软件社区为基础，通过代码迭代多方共同维护一个商业价值网络的信用体系。正是这样一种新型的人类组织结构，导致了公有链监管呈现出以下特点：

（1）监管客体的分散性

公有链是一个以开源代码为核心形成的社区，其中任何一个参与社区活动的特定的公司或者个人都不能完全等同于公有链本身。而公有链内部如果出现分歧，随时有可能分叉形成多条公有链并分裂成互相交织的多个社区。开源代码本身并不具有任何法律主体地位，开源代码的使用方也是自愿使用开源代码，开源代码的贡献方也没有任何义务保证代码的可用性、安全性和迭代更新。任何强制禁止开源代码更新或者提交的措施都是可以成本极低的规避的。因此，将公有链或开源代码本身作为监管客体是难以实现的。而在参与公有链社区的诸多主体之中，根据他们利用公有链开源软件作为工具从事的各项商业或者非商业业务的具体性质，这些业务使得这些主体需要承担相应的责任，要受相应的监管。

（2）监管政策工具缺乏

目前，针对公有链相关的监管最大的难题是实现监管政策的工具缺乏，给监

管带来了很多不利的影响，具体表现在以下几个方面：

首先，缺乏有效的税收工具。

不同于现有的法币体系下的商业活动和商业主体，在公有链相关的商业活动和收入、利润当中，没有向国家提供税收的工具。这使得监管部门不能从相关的公共服务当中获得财政支持，最终的结果必然是选择监管则需要挤占其他行政资源，而选择不监管则不符合行政职权的要求。

其次，缺乏有效的公有链技术安全监测工具。

产业利用公有链技术开展各项业务，对公有链技术的安全性、可靠性并不能完全依赖公有链技术社区的意见，因为这些意见不能排除不受利益的干扰，也有可能同时存在多个观点冲突的意见。而一个站在监管部门角度或者第三方独立机构角度的技术安全监测意见，能够实时公布，供产业参考，是非常有必要的。有了这样一个工具，可以为不熟悉公有链技术的更多其他产业积极利用公有链技术开展业务降低门槛和成本。

最后，缺乏有效的公有链产业分析工具。

根据其所主要支持的产业方向不同，一些公有链是符合国家和地区产业支持发展方向的，可以是产业政策支持的对象；而有一些公有链所支持的产业是违背国家政策和法律规定的，则要严加监管。那么哪些公有链，哪些公有链所支持的产业是可以并且应当支持的；哪些是应该严加监管，禁止发展的；哪些是需要进行有约束条件，特定方向允许发展的，需要统一的依据。而作为产业发展政策的依据，一套公有链产业分析工具是非常有必要的。

2. 公有链监管政策的平衡

任何一项监管政策，都需要兼顾公平和效率，兼顾短期利益和长远利益。如何合理的设立监管目标，平衡各项可能存在冲突的利益关系，需要做细致而深入的设想。

（1）技术中立与合规监管的平衡

公有链技术的发展，离不开开源代码贡献者的充分自由讨论和互相交流。同时，这种技术的发展是中立的，公有链社区是松散的，没有强制性要求任何国家、个人和企业必须使用某一项公有链技术。公有链的分叉模式表明这天然近乎一个

充分竞争市场。

另外一方面，公有链社区不是法外之地。即使公有链技术本身是中立的，但是使用中立的技术从事违法犯罪活动的任何组织和个人都必须承担相应的法律责任，这和历史上任何一次技术发展导致的监管介入并无本质不同。但是，技术和技术发展与利用技术发展进行违法活动的行为是截然不同的，技术社区并没有任何义务来为任何违法犯罪行为承担责任。

（2）区域间监管政策平衡

公有链不但是一个天然跨多部门监管领域，也是一个天然跨区域的受监管领域。跨区域包括跨国界，也包括在一国管辖范围内跨地区。在公有链高速发展的背景下，各国中央和地方政府的监管部门出台了多项监管政策。这些政策有的很激进，有的比较保守，也有许多监管部门处于积极的观察但暂不决策的过程中。

很明显，在对公有链的监管政策态度上，各国态度是不一致的；各国国内，不同地区的监管部门的态度也是有区别的。对于典型的金融离岸地国家，如新加坡、马耳他等国，监管态度是最为积极和开放的，因为公有链带来的高金融流动性使得这些国家受益。对于有强大的 IT 和金融业基础的美国，美国证券监管委员 SEC 的公开监管态度是一直坚持符合现有法规，进行个案监管，而对出台统一的公有链监管政策暂无日程，以谨慎观察态度为主；对创新包容，减少事先判断和干预。而在美国国内部分州，例如内华达州，对公有链的监管态度是比较积极的。

世界各国，各国国内各区域的发展都是非常不均衡的。对于金融发达，互联网基础先进完善的地区和人民而言，公有链所能提供的高流动性和高信用度可以更多的起到产业加速和资金汇集的正面作用。而对于金融欠发达，互联网基础不好，社会结构不够稳定的地区，公有链带来的高流动性和高信用度反而会带来更多的不稳定因素，损害本地的产业，使本地的资金和信用外流，因此更多的希望限制相关产业的发展。

(二) 领域监管

1. 货币监管

由于公有链代码设计和运行中都是包含相应的原生 Token，这些 Token 与现有国家法币体系是什么关系，需要各国货币监管当局进行确定。

（1） 中国监管

中国政府于 2013 年 12 月 5 日发布《关于防范比特币风险的通知》，否定了比特币的货币属性，禁止金融和支付机构开展与比特币相关的业务，要求比特币交易网站进行备案，并且提示了通过比特币洗钱的风险。在此之后，实践案例显示，中国法院对于以比特币等加密货币为支付手段的合同交易均采不受合法保护的监管态度，以合同无效进行处理。但中国法院承认比特币是有价值的物品，侵害他人的比特币财产权益会受到刑法的保护。

（2） 国际监管

日本政府 2017 年《支付结算法》承认比特币等加密货币为合法的电子支付手段。美国监管部门更关注的是，以泰达币（USDT）为首的稳定币是否有超发或者美元资产储备不足的情况，以给持币人带来风险。在这样的监管思路下，纽约金融服务局批准的以真实美元为抵押的，接受官方监督的稳定美元代币 GUSD 和 PAX 的发行获得了市场的高度关注。

2. 证券监管

（1） 中国监管

中国政府于 2017 年 9 月 4 日发布《关于防范代币发行融资风险的公告》。公告将“首次代币发行”（ICO）定义为“一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动”。公告同时要求，各类代币发行融资活动应当立即停止，已完成代币发行融资的组织和个人应当做出清退等安排；任何所谓的代币融资交易平台不得从事法定货币与代币、“虚拟货币”相互之间的兑换业务，不得买卖或作为中央对手方买卖代币或“虚拟货币”，不得为代币或“虚拟货币”提供定价、信息中介等服务；各金融机构和非银行支付机构不得直接或间接为代币发行融资和“虚拟货币”提供账户开立、登记、交易、清算、结算等产品或服务，不得承保与代币和“虚拟货币”相关的保险业务或将代币和“虚拟货币”纳入保险责任范围。公告发布后，首次代币发行活动在国内已属违法，主要的加密货币交易所迁移海外，ICO 引发的

非法筹资乱象得到有效遏制。

（2） 国际监管

新加坡是全球首个提出来区分“证券性代币”和“使用性代币”（Utility Token）并予以官方确认的国家，对“使用性代币”并不按照证券法的规定进行监管。美国对于区分某个具体代币是否属于证券，还是采取个案甄别的方式，依据其判例法确定的“豪威测试”（HoweyTest）原则来确定某一具体代币是否属于证券，需要按照证券管理的法规进行监管。SEC 高级官员在其政策倾向文章中也明确表示，不急于设立统一的判断标准，仍愿意对行业发展保持紧密的观察。对充分分散化、以及广泛普及的比特币、以太币等加密货币，SEC 倾向于不将其作为证券进行监管。

3. 内容监管

公有链作为信息和信用传递的系统，根据所在国的法律，遵守所在国的互联网通信内容监管法规是法定的义务。

（1） 中国监管

2019 年 1 月 10 日，国家互联网信息办公室发布《区块链信息服务管理规定》。规定要求落实区块链信息服务提供者的运营责任，根据《网络安全法》等现行有效法律的规定，对区块链信息服务传播的信息内容进行合规监管；对区块链信息服务及服务提供者进行备案管理，发给备案编号。规定同时明确了国家网信办和省级网信办为区块链信息服务的监督管理执法工作负责单位。

（2） 国际监管

我国首先就区块链提供信息服务出台专门的管理规定。区块链特性使得链上数据难以篡改，区块链可能成为传播危害公共安全、涉及恐怖主义和不良信息的载体。随着监管的发展，我们有理由相信，任何利用公有链区块链技术进行与互联网内容传播有关的违法犯罪活动，在各国一样会受到法律的追究。另外一方面，公有链的发展（特别是 IPFS 等存储数据的公有链）有可能与个人信息控制者的确定、收集信息的目的限定原则、个人信息被遗忘权、个人信息跨境流动等规则可能存在冲突。欧盟推出《通用数据保护条例》（GDPR），因此可能后续会有更多的监管措施出台。

4. 税务监管

公有链作为价值传递的网络和社区，有大量有价值的虚拟物品在被创造和交易，并且这个总价值量还在增长之中。

（1） 中国监管

中国税务监管部门对公有链社区参与方没有进行专门的税务监管，相关企业是按照一般的税务方式进行纳税。例如，比特大陆在招股说明书中披露，该企业是通过包括企业所得税等进行纳税。但是对于更广泛的持币和交易群体而言，既没有征收流转税，也没有征收所得税。

（2） 国际监管

美国国家税务局（IRS）对公有链社区参与方，特别是交易参与方的纳税义务一直十分关注。美国国家税务局曾经起诉美国最大的加密货币交易所之一的Coinbase，要求其提供客户的交易资料，作为征税的依据。公有链的税务监管需要适应加密货币和加密资产会计核算的国际通用会计准则的出台。

七、 结论

自中本聪发表论文《Bitcoin：A Peer-to-Peer Electronic Cash System》已经过去了十年，区块链技术从极客圈子的小众话题，已变为人尽皆知的科技热点。十年来，区块链技术逐渐从比特币和电子现金的领域向其他领域扩展。功能上，区块链从主要用于记录电子现金转账的“专有账本”，升级为可记录计算状态的“通用账本”，进入可编程时代。应用范式和路径上，区块链也分化为公有链和联盟链两种形态。

近年来，公有链发展迅速，学术研究日趋活跃，但产业总体还是呈现技术热、应用冷的态势。全球公有链的应用高度集中在加密数字资产领域，而且呈现明显的头部效应。实际应用方面，现有公有链的内在逻辑难以适应社会、法律和商业环境，缺乏合规的链上身份系统、合约隐私性保护不足等问题，使其难以走进现实世界，与实体经济结合的“杀手”应用尚未出现。但与此同时，公有链为区块链的技术发展提供了全球化的试验场，各种技术路线百花齐放，在提升区块链平台

在可扩展性、隐私性与互操作性的技术方案不断涌现出来，开发者持续探寻区块链技术边界及新型技术方案。

从社会组织的角度，公有区块链发展过程是一个通过区块链协议组织参与者的过程。基于公有链，在网络上形成了自发性的组织形态，即社区。社区是公有链的社会组织形态，也决定着公有链的技术走向共同体。公有链作为软件产品，会随着需求和变化更新升级，而技术升级与更新的方案选择则需要通过完成决策选择，并达成意见一致，这一过程叫做公有链的治理。公有链的治理主要由区块链协议开发者、矿工、上层应用开发者及用户构成，通过链上治理和链下治理两个部分的决策模式完成。

公有链作为一个新兴的技术发展方向和特有的产业发展领域，引起了全球科技、经济、法律和政府人士的广泛关注。但公有链社区及其产业并非法外之地，“Code is Law”的激进法律和社会实验也不能以社会其他人群的受损为代价。因此对于公有链的监管势在必行，相比于主要针对于社区内部参与者的治理过程，监管主要聚焦在公有链对社会整体产生的影响方面，监管的参与主要是相关的立法、行政等部门对于技术及产业的监督和规范化。

区块链经历了十年的发展，虽然真正落地并产生社会效益的区块链项目较少，但已充分展示其潜在的巨大价值。相信在下一个十年里，区块链将更多地走向产业、走向成熟、走向规范。以其独有的信任机制，为社会创造更多的价值。

可信区块链推进计划

地址：北京市海淀区花园北路52号　邮政编码：100191

联系电话：010-62300249　传真：010-62304980

网址：www.trustedblockchain.cn