区块链不可能三角问题研究与量化分析

刘岵[1,2] , 荆林波[3] , 王静逸[2]

[1] （中国社会科学院研究生院，北京100102 ）
[2]（第一视频集团研究院，北京 100102）
[3]（中国社会科学院中国社会科学评价研究院，北京100732 ）
通讯作者: 刘岵，E-mail: stevenliu_vip@hotmail.com

摘要：区块链技术与应用近年来受到了非常热切的关注，它综合了密码学、分布式存储、共识机制、智能合约等技术，建立了一种新型的信任与激励体系，大大提升了透明度，减少了信用风险，提升了效率。在没有第三方权威机构的中介协调下，区块链在互不了解的交易双方间建立了可靠的信任，去中心化地实现了可信的价值传输。它颠覆现有的生产关系，为金融、产权、供应链等诸多行业提供变革和增长的机会。但将技术运用到实际应用当中，必须考虑其实用效率问题。本论文理论结合实验结果分析，对区块链技术的重要特性，即“安全性”、“去中心化”与区块链应用的“效率”进行理论研究与量化分析。并结合实验进行分析，给出相应的结论和建议，以便更好的优化区块链技术方案并运用到实际当中。

关键词： 区块链 分布式数据库 安全 去中心化 不可能三角形

Research and quantitative analysis of the Blockchain impossible triangle issue

LIU Hu[1,2] , Jing Lin-Bo[3] , Wang Jing-Yi[2]

[1] （Graduate School of Chinese Academy of Social Sciences, Beijing 100102, China ）
[2]（ Research Institute of V1 Group，Beijing 100102, China）
[3]（Chinese Academy of Social Sciences Evaluation of Chinese Academy of Social Sciences，北京100732 ）

Abstract: Blockchain technology and its application have received much attention in recent years. By integrating cryptography, distributed storage, consensus mechanism, intelligent contract and other technologies, a new trust and incentive system has been established, which greatly improves transparency, reduces credit risk and improves efficiency. Without the mediation and coordination

of the third party authority, the blockchain has established reliable trust between the two parties who do not know each other and realized credible value transmission in a decentralized way. It upsets existing production relations and provides opportunities for change and growth in finance, property rights, supply chains and many other industries. However, when applying technology to practical application, we must consider its “efficiency” from the perspective of economics. This paper using the method of technical analysis and economic, made the theoretical research and quantitative analysis on the important feature of block chain technology, namely, "security", "decentralization" and "efficiency" of block chain application. The conclusion was drawn that in the application of blockchain, these three factor can’t be can not satisfied simultaneously - so called Impossible Triangle Decentralization in blockchain applications. Combining with experimental analysis, the corresponding conclusions and recommendations are given, in order to optimize blockchain technology better and applied to practice.

Key Words: Blockchain Security Distributed system Security Impossible Triangle Decentralization

1 引言

区块链技术起源于化名为“中本聪”(Satoshi Nakamoto) [1]的学者在 2008年发表的奠基性论文《比特币: 一种点对点电子现金系统》。正如维基百科英文版[b]所言，“A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block,a timestamp, and transaction data.” 狭义来讲, 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。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。这些技术确保了区块链具备如下的特征:

1) 不可篡改:区块链加密技术采用了密码学中的哈希函数，该函数具有单向性，因此存在于链中的非本节点产生的数据是不可被修改的。同时由于区块链系统共识算法的限制，几乎无法单方面修改本节点产生的数据并使其被确认(除非达到全网算力的51%)，保证了内容的安全可靠。

2) 可追溯性: 区块链上每一个区块都记录着上一个区块的身份信息，因此只需回溯历史区块就能找到当前区块 信息的来龙去脉。

3) 去中心化: 相对于“中心化”的一个概念。区块链系统没有特定的中央服务器，是一个基于点对点技术的开源系统。每个节点共同实现系统的维护并保证信息传递的真实性。整个系统采用分布式存储模式，数据完全公开透明没有中心进行集中管理。

4) 一致性：在分布式去中心化环境下，数据要保证一致性，需要使用一致性协议。通过算法和全网的算力以及节点通信的代价实现全网成员达成一致。

5) 去信任化: 任意节点之间的连接或数据交换都不需要信任为前提并受到全网监督，即每个节点都是区块链系统的监督者。

6) 实时性: 从信息披露角度来看，数据交换一旦完成便会立即上传到区块链网络中。从数据传输角度来看，如跨境支付这类目前需要多方多个环节处理的数据处理缓慢的领域，已经

可以通过区块链技术大大提升效率 。

区块链通过技术手段，解决了信息和信用可靠及传递的问题，相关的场景理论上都可以引入区块链来解决问题。正如权威期刊《经济学人》里提到到:“区块链是一个制造信任的机器，在任何需要信任的领域，区块链都有用武之地” 。区块链的核心价值是构建了一种去中心化的信用机制，其应用价值，主要表现在三个方面[3]。第一，公开透明，避免欺诈。存储在区块链的记录不可篡改，不可消除，监管方能清晰地看到每一笔交易的来龙去脉，在链条长、参与方多的复杂情况下，区块链能有效地防止作假伪造，减少侵犯隐私和滥用的行为。第二，制定规则，降低信用风险。通过将双方的约定写在区块链智能合约上，交易在满足约定的条件后自动执行，避免违约。第三，去中心化，提高效率。区块链去中心化的存储和共识，形成可追溯、不可篡改的信息，告别了必须经由中心机构验证带来的重复验证流程，可缩短中间链条，减少清结算成本，提升效率。目前区块链应用的领域有:

1）数字货币：区块链在数字货币的应用产品已经产生多年，并日臻成熟，其价值和相关的技术得到验证。如比特币是全球范围内可以交易的数字货币，是目前区块链技术最成功的应用。但如ICO，近期引起了全球的密切关注并广泛的传播。这类应用未来的发展趋势以及如何应对，这对广大人民甚至政府层面都会有一定的影响。

2）金融领域：在金融领域的应用，其根本的意义是改善信息不对称的问题。同时也应做到降低成本和提升效率或者降低风险（即减少损失就是收益)。如一，在支付领域，区块链技术的应用有助于降低金融机构间的对账成本及争议解决的成本，从而显著提高支付业务的处理速度及效率，这一点在跨境支付领域的作用尤其明显。二，区块链技术的核心特质是能以准实时的方式，在无需可信的第三方参与的情况下实现价值转移，清算，结算。三，在供应链金融领域，解决由于信息分散，信用不清导致非核心企业享受不到授信及贷款的问题。提高了整个供应链的效率。

3）数字版权：使用区块链技术，可以通过时间戳、哈希算法对作品进行确权，证明一段文字、视频、音频等存在性、真实性和唯一性。一旦在区块链上被确权，作品的后续交易都会被实时记录，文化娱乐业的全生命周期可追溯、可追踪，这为司法取证提供了一种强大的技术保障和结论性证据。也为数字产品的产生，分销，消费的跟踪记录提供了很好的方式。

4）供应链及物流：在物流过程中，利用数字签名和公私钥加解密机制，可以充分保证信息安全以及寄、收件人的隐私。区块链不可篡改、数据可完整追溯以及时间戳功能，可有效解决物品的溯源防伪问题。另外，通过智能合约能够简化物流程序和大幅度提升物流的效率 。

除此以外，区块链在物联网，存证记录，数字产权等诸多领域都有很多应用。从应用系统结构总结起来大体分两类：

第一类：原有系统是中心化系统，但由于系统架构的纵向层级太多，或者横向的节点多，导致系统总体效率低下，或者中心节点主观问题、客观受攻击导致了整个系统的信用及效率出现严重问题。在如何优化中心化系统结构，或者将中心化系统解构成去中心化，或是多中心化系统过程中，运用到区块链技术。

第二类：系统原本是多中心化系统，但每个单独系统都维护自身的利益、如何利用区块链技术在保护自身权益的同时，按照严格的规则约定，进行数据及信息的分享、同步、交易，从而进一步提高系统效率。

但是，目前大众和业界对区块链的认知及应用还有很多误会，其中一类声音是极度夸大区块链的功能，而另一类极端的声音是极力抨击区块链存在的缺陷。大众对区块链有诸多的误区，如将比特币等同于区块链。一提到区块链，谈论最多的是比特币等虚拟货币带来的价值。另一种误区是说区块链是万能的技术，能颠覆性的代替数据库，代替互联网。这种认识上的误区阻碍了区块链技术的正常发展以及行业应用、也会打击人们区块链应用的积极性。

作为一种ICT (information communication technology) 信息新技术, 如何合理的应用到行业当中，对行业及相关经济产生正面影响呢？相关经济学学者有如下论述[4]：“商务为本，技术为辅;商务是基础，技术是支撑。两者相辅相成，不可或缺。那种主张技术至上的观点是十分危险的，极易掉入技术导向的陷阱之中，而迷失了商务的方向。”在进行应用系统设计时，必须以自己的商务为核心，应当从自身的实际优劣势出发，切忌好高骛远，脱离实际，耗费财力而没有成效。ICT技术对经济增长的巨大促进作用已经成为共识，但新技术从出现使用到在经济增长中体现有技术迟滞现象。从根本上来讲技术应用要对其经济效率水平有提高、对生产率有提升，甚至对经济增长速度有推动作用。所以在应用层面，我们要抓住“效率”这个关键词，进行理性的研究和应用设计。

目前在围绕区块链技术应用的效率问题，即“高效低能”及其它两个主要因素“去中心化”和“安全”组成的“不可能三角”[5]课题，学术界和产业界也有些研究与分析，但大都是定性的、粗线条的阐述如何无法同时达到“高效低能”，“去中心化”和“安全”三个要求。基本停留在理论定性论述，缺少定量模型分析及实验总结。

通过对区块链技术的研究和经济学理论学习及案例分析，本文作者结合具体的实验结果，运用定性分析与定量分析结合法研究并取得评估其安全，效能和去中心化程度特性的量

化指标，并对三个因素关系即整体的合理性进行定性和定量评估。试图为业界进一步研究三难问题，即如何更好的将区块链运用到实际当中，起到参考作用。

2 区块链系统架构及关键技术

2.1系统设计架构

各种区块链的技术及应用尽管各不相同，但从整体架构上有共性，整体上可以分为五层，即网络层、共 识层、数据层、智能合约层和应用层[6]。

		比特币	以太坊	Hyperledger Fabric
应用层		比特币交易	Dapp/以太币交易	企业级区块链应用
智能合约层	编程语言	Script	Solidity/Serpent	Go/Java
	沙盒环境		EVM	Docker
数据层	数据结构	Merkel树/区块链表	Merkle Patricia树/区块链表	Merkle Bucket树/区块链表
	数据模型	基于交易的模型	基于账户的模型	基于账户的模型
	区块存储	文件存储	LevelDB	文件存储
共识层		PoW	PoW/PoS	PBFT/SBFT
网络层		TCP-based P2P	TCP-based P2P	HTTP/2-based P2P

图2.1区块链系统架构

网络层：区块链网络中没有中心节点，任意两个节点之间可直接通信并进行交易，每个节点也可自由加入或退出网络，出入自由。所以区块链网络通常选择完全分布式且可容忍单点故障的 P2P 协议作为网络传输协议。该网络节点具有平等、自治、分布等特性，所有节点以扁平拓扑结构相互连通，不存在任何中心化的权威节点，每个节点均拥有路由发现、广播交易、广播区块、发现新节点等功能[7] 。区块链网络的 P2P 协议主要用于节点间传输交易数据和区块数据，比特币和以太坊的 P2P 协议基 于TCP协议实现。

共识层：处理区块链上各个节点对于区块数据的验证和共识达成，保证去中心化数据的有效性、一致性，保持同步。

数据层：通过处理区块链上的数据结构、数据模型和数据存储来实现区块链上去中心化存储。区块链通过规格相同的区块存储和哈希地址计算，形成链式的存储结构。

智能合约层：能合约是一种用算法和程序来编制合同条 款、部署在区块链上且可按照规则自动执行的数字化协议。 智能合约作为区块链2.0技术的代表，运行在区块链的虚拟机上，提供给业务交易的可信凭证。

应用层：基于区块链架构的应用，提供业务逻辑、人机界面给用户。如比特币平台上的应用主要是基于比特币的数 字货币交易。以太坊除了基于以太币的数字货币交易外，还支持去中心化应用(Decentralized Application，Dapp)，即由 JavaScript 构建的 Web 前端应用。

2.2 区块链关键技术

区块链技术与其说是一个颠覆性的全新技术，不如说是一组技术革新与优化的组合。区块链的主要技术要点包括密码学、分布式存储、共识机制等。每个技术的特点如下。

2.2.1信息安全及密码学

信息安全及密码学技术是区块链技术的核心基石。在区块链中，也大量使用了现代信息安全和密码学的技术成果，主要包括:哈希算法、非对称加密、数字签名、数字证书、同态加密、零知识证明等。通常信息系统的安全性需求即响应的措施主要包含五部分[7] ，即:

第一，可用性指尽管存在可能的突发事件，如事故、攻击等，但用户依然可以使用数据，系统服务也能处于正常运转状态。不同的系统有不同的量化指标，比如公有云服务的SLA即服务等级协议对应的一年中服务的可用性时长百分比。

第二，机密性是指保护数据不受非法截获和未经授权浏览，这一点保护敏感数据（如隐私）尤为重要。数据的机密性通常是用加密技术来保证的。加解密技术从技术构成上分为两大类:一类是对称加密，一类是非对称加密。对称加密的加解密密钥相同;而非对称加密的加解密密钥不同，即使用公私钥对数据存储和传输进行加密和解密。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方 解密接收到的加密内容。公私钥对计算时间较长，主要用于加密较少的数据。常用的非对称加密算法有RSA和ECC。与诸多互联网业务层安全加密方案类似[9] ，区块链正是使用基于证书的非对称加密的公私钥对来构建节点间信任的。

区块链尤其是联盟链，在全网传输过程中，都需要 TLS(Transport Layer Security)加 密通信技术，来保证传输数据的安全性。而TLS 加密通信，正是非对称加密技术和对称 加密技

术的完美组合:通信双方利用非对称加密技术，协商生成对称密钥，再由生成的对称密钥作为工作密钥，完成数据的加解密，从而同时利用了非对称加密不需要双方共享密钥、对称加密运算速度快的优点。

第三，完整性指能够保证被传输、或者存储的数据是完整的和未被篡改的。区块链采用哈希算法和非对称加密技术来保证区块链账本的完整性和网络传输安全。哈希(散列)算法能将二进制数据映射为一串较短的字符串，并具有输入敏感特性，一旦输入的二进制数据，发生微小的篡改，经过哈希运算得到的字符串，将发生非常大的变化。此外，优秀哈希算法还具有冲突避免特性，输入不同的二进制数据，得到的哈希结果字符串是不同的。

区块链利用哈希算法的输入敏感和冲突避免特性，在每个区块内，生成包含上一个区块的哈希值，并在区块内生成验证过的交易的 Merkle 根（一种基于哈希算法的树结构）哈希值，即对区块中的具体事务或状态进行结构化组织并将概要信息（根哈希）存入区块头。一旦整个区块链某些 区块被篡改，都无法得到与篡改前相同的哈希值，从而保证区块链被篡改时，能够被迅 速识别，最终保证区块链的完整性(防篡改)。

第四，非否认性指能够保证信息行为人不能否认其信息行为。区块链中每笔交易的发起方用私钥的签名，全网节点对其验证，确保该动作为发起人所为，保证了其非否认性。

第五，可控性是指保证信息和信息系统的授权认证和监控管理，以确保相应的实体的真实性，也可确保系统的安全可控。同产单纯的加密通信，仅能保证数据传输过程的机密性和完整性，但无法保障通信端对端可信(中间人攻击)。因此，需要引入数字证书机制，验证通信对端身份，进而保 证对端公钥的正确性。数字证书一般由权威机构进行签发。通信的一侧持有权威机构根 CA(Certification Authority)的公钥，用来验证通信对端证书是否被自己信任(即证书是否 由自己颁发)，并根据证书内容确认对端身份。在确认对端身份的情况下，取出对端证书中的公钥，完成非对称加密过程。

随着区块链技术的进步和应用的日益广泛，比特币、以太坊等早期公有链项目完全公开化的账本难以满足人们对应用场景中对隐私的更高需求，所以无须泄露数据本身即可证明某些数据真实的零知识证明、同态加密等技术被使用，在新兴的区块链项目中扮演着日益重要的角色。零知识证明指证明者（被验证者）能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的协议。区块链安全是一个系统工程，系统配置及用户权限、组件安全性、用户界面、网络入侵检测和防攻击能力等，都会影响最终区块链系统的安全性和可靠性。区块链系统在实际构建过程中，应当在满足用户要求的前提下，在安全性、系统构建成本以及易用性、和建设使用成本等维度，取得一个合理的平衡。

2.2.2 分布式存储

区块链账本采用的分布式存储记账方式即分布式账本技术DLT (Distributed Ledger Technology)[10]，是一种从分布在不同物理地址或不同组织内的多个网络节点构成的网络中进行数据分享、同步、复制的去中心化数据存储技术。相较于传统的分布式存储系统，分布式账本技术主要具备两种不同的特征。

传统分布式存储系统执行受某一中心节点或权威机构控制的数据管理机制，分布式账本往往基于一定的共识规则，采用多方决策、共同维护的方式进行数据的存储、复制等操作。面对互联网数据的爆炸性增长，当前由单一中心组织构建数据管理系统的方式正受到更多的挑战，服务方不得不持续追加投资构建大型数据中心，不仅带来了计算、网 络、存储等各种庞大资源池效率的问题，不断推升的系统规模和复杂度也带来了愈加严峻的可靠性问题。然而，分布式账本技术去中心化的数据维护策略恰恰可以有效减少系统臃肿的负担。在某些应用场景，甚至可以有效利用互联网中大量零散节点所沉淀的庞大资源池。

传统分布式存储系统将系统内的数据分解成若干片段，然后在分布式系统中进行存储，而分布式账本中任何一方的节点都各自拥有独立的、完整的一份数据存储，各节点之间 彼此互不干涉、权限等同，通过相互之间的周期性或事件驱动的共识达成数据存储的最终一致性。经过几十年的发展，传统业务体系中的高度中心化数据管理系统在数据可信、网络安全方面的短板已经日益受到人们的关注。普通用户无法确定自己的数据是否 被服务商窃取或篡改，在受到黑客攻击或产生安全泄露时更加显得无能为力，为了应对这些问题，人们不断增加额外的管理机制或技术，这种情况进一步推高了传统业务系统的维护成本、降低了商业行为的运行效率。但终究无法解决中心化的可信度问题。分布式账本技术可以在根本上大幅改善这一现象，由于各个节点均各自维护了一套完整的数据副本，任意单一节点或少数集群对数 据的修改，均无法对全局大多数副本造成影响。换句话说，无论是服务提供商在无授权情况下的蓄意修改，还是网络黑客的恶意攻击，均需要同时影响到分布式账本集群中的大部分节点，才能实现对已有数据的篡改，否则系统中的剩余节点将很快发现并追溯到 系统中的恶意行为，这显然大大提升了业务系统中数据的可信度、防篡改性和安全保证。

总之，区块链网络中各参与节点拥有完整的数据存储，并且各节点是独立、对等的，它依靠共识机制保证存储的最终一致性，也通过这些方式来保证分布式存储数据的可信度与安全性，即只有能够影响分布式网络中大多数节点时才能实现对已有数据的篡改。定量的看，参与系统的节点增多，会提升数据的可信度与安全性。但大量的节点的同步、确认会降低系统的效率。

技术方面，有别于传统数据库，区块链只提供“增加”与“查询”操作，通过“增加”交易来实现“修改”和“删除”操作，比如产生区块硬分叉来实现交易的回滚，避免数据的恶意篡改。但这也有缺点，会带来区块链存储无限增大的问题。

2.2.3智能合约

智能合约是用程序语言编写的商业合约，当预设条件满足时，能够自动强制的执行合同条款，从而实 现“代码即法律”的目标。。允许在不依赖第三方的情况下进行可信、可追踪且不可逆的合约交易。这个概念由计算机科学家尼克萨博(Nick Szabo)在1996年提出，描述“以数字形式定义的一组承诺，包括各方履行这些承诺的协议。”区块链的去中心化使得 智能合约在没有中心管理者参与的情况下，可同时运行在全网所有节点，任何机构和个人都无法将其 强行停止。

区块链技术的发展为智能合约的运行提供了可信的执行环境。区块链智能合约是一段写在区块链上的代码，一旦某个事件触发合约中的条款，代码即自动执行。其扩展了区块链的功能，丰富了区块链的上层应用。比特币平台并不支持智能合约。以以太坊为例，智能合约的运作机制是依照商业逻辑编写完智能合约代码后，需要将其发布到区块链网络节点上。部署后的合约存放在区块链上，每次被调用时才被以太坊虚拟机(EVM) 加载运行。智能合约定义了交易逻辑及访问状态数据的 业务规则，外部应用(如以太坊中的去中心化应用 Dapp)需要调用智能合约，并依照合约执行交易和 访问状态数据。外部应用与智能合约间的关系非常 类似于传统数据库应用与存储过程间的关系，存储过程运行于数据库管理系统之中，访问关系数据库数据;而智能合约运行于区块链系统之中，访问区块和状态数据。

目前，较为成熟的以太坊和Hyperledger Fabric框架均包含智能合约，支持图灵完备的语言，在其基础上可实现多种智能合约，包括差价合约、储蓄钱包合约、多重签名合约、保险衍生品合约等，无须依赖第三方或中心化机构，极大地减少了人工参与，具备很高的效率与准确性。

需要注意到，区块链公链上部署的全部智能合约对外可见且可交互，意味着其全部漏洞对外公开。在以太坊公链上就多次出现千万美元级的安全事件。如何编写安全可靠的智能合约是区块链技术面临的核心课题之一。

2.2.4 共识机制

区块链是一个可追溯、不可篡改，解决多方互信问题的分布式(去中心化)系统。 分布式系统必然面临着一致性问题，即如何确保节点之间的一致性和同步确认，而解决一致性问题的过程我们称之为共识。

共识算法通常解决的是分布式系统中由哪个节点发起提案，以及其他节点如何就这个提案达成一致的问题。我们根据传统分布式系统与区块链系统间的区别，将共识算法分为可信节点间的共识算法与不可信节点间的共识 算法。前者已经被深入研究，并且在现在流行的分布式系统中广泛应用，其中Paxos 和Raft 及其相应变种算法最为著名。而后者，虽然也早被研究，但直到近年区块链技术发展后，相关共识算法才得到大量应用。而根据应用场景的不同，后者又分为以 PoW(Proof of Work)和 PoS(Proof of Stake)[11] 等算法为代表的适用于公链的共识算法和以 PBFT(Practical Byzantine Fault Tolerance)及其变种算法为代表的适用于联盟链或私有链的共识算法。

因为共识算法是研究系统去中心化与系统高效之间的重要因素，所以有必要做更详尽的描述，以工作量证明(Proof Of Work，简称POW) 为例。

工作量证明，简单理解就是一份证明，用来确认你做过一定量的工作。即通过对工作的结果进行认证来证明完成了相应的工作量，从验证角度来看，是一种非常高效的方式。工作量证明系统，是一种应对拒绝服务攻击和其它服务滥用的经济对策。它要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的时间和算力。这个概念由Cynthia Dwork 和 Moni Naor 1993年在学术论文中首次提出。而工作量证明（POW）这个名词，则是在1999年 Markus Jakobsson 和Ari Juels的文章中才被真正提出。比特币系统中采用的POW算法于 1998 年由 W. Dai 在 B-money 的设计中提出。

那么我们如何找到一种数学的方法来实现POW算法？哈希函数正是这样的一个数学基石。哈希函数（Hash Function），也称为散列函数，给定一个输入x，它会算出相应的输出H(x)。哈希函数的主要特征是：

1）输入x可以是任意长度的字符串； 2）输出结果即H(x)的长度是固定的；3）计算H(x)的过程是高效的（对于长度为n的字符串x，计算出H(x)的时间复杂度应为O(n)）.

而对于比特币这种加密系统所使用的哈希函数，它需要另外具备以下的性质：

1）免碰撞，即不会出现输入$x \neq y$，但是H(x)=H(y)。其实这个特点在理论上并不成立，比如，比特币使用的SHA256算法，会有2^256 种输出，如果我们进行2^256 +1次输入，那么必然会产生一次碰撞；甚至从概率的角度看，进行2^130 次输入就会有99%的可能发生一次碰撞。不过我们可以计算一下，假设一台计算机以每秒10000次的速度进行哈希运算，要经过10^27 年才能完成2^128 次哈希！所以说，即便是人类制造的所有计算机自宇宙诞生开始一直运算到今天，发现碰撞的几率也是极其小的。

2）不可逆性，也就是说，对于一个给定的输出结果H(x)，想要逆推出输入x，在计算上

是不可能的。不存在比穷举更好的方法，可以使哈希结果H(x)落在特定的范围。

工作量证明的基本原理：工作量证明系统主要特征是客户端需要做一定难度的工作得出一个结果，验证方却很容易通过结果来检查出客户端是不是做了相应的工作。这种方案的一个核心特征是不对称性：工作对于请求方是适中或者费力的，但对于验证方则是易于验证的。其原理与验证码不同，验证码的设计出发点是易于被人类解决而不易被计算机解决。

例如，给定的一个基本的字符串”Hello, world!"，我们给出的工作量要求是，可以在这个字符串后面添加一个叫做nonce的整数值，对变更后（添加nonce)的字符串进行SHA256哈希运算，如果得到的哈希结果（以16进制的形式表示）是以"0000"开头的，则验证通过。为了达到这个工作量证明的目标。我们需要不停的递增nonce值，对得到的新字符串进行SHA256哈希运算。按照这个规则，我们需要经过4251次计算才能找到恰好前4位为0的哈希散列。

以比特币系统为例，解释下工作量证明的具体过程：

比特币网络中任何一个节点，如果想生成一个新的区块并写入区块链，必须解出比特币网络出的工作量证明的迷题。这道题关键的三个要素是工作量证明函数、区块及难度值。工作量证明函数是这道题的计算方法，区块决定了这道题的输入数据，难度值决定了这道题的所需要的计算量。

1）工作量证明函数：比特币系统的工作量证明采用函数SHA256。SHA是安全散列算法（Secure Hash Algorithm）的缩写，是一个密码散列函数家族。这一组函数是由美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST） 发布的，主要适用于数字签名标准。SHA256就是这个函数家族中的一个，是输出值为256位的哈希算法。到目前为止，还没有出现对SHA256算法的有效攻击。

2） 区块：比特币的区块由区块头及该区块所包含的交易列表组成。区块头的大小为80字节，由4字节的版本号、32字节的上一个区块的散列值、32字节的Merkle Root Hash、4字节的时间缀（当前时间）、4字节的当前难度值、4字节的随机数组成。区块包含的交易列表则附加在区块头后面，其中的第一笔交易是coinbase交易，是为了让矿工获得奖励及手续费的特殊交易。区块的大致结构如图所示：

拥有80字节固定长度的区块头，就是用于比特币工作量证明的输入字符串。因此，为了使区块头能体现区块所包含的所有交易，在区块的构造过程中，需要将该区块要包含的交易列表，通过Merkle Tree算法生成Merkle Root Hash，并以此作为交易列表的摘要存到区块头中。其中Merkle Tree的算法图解如下：

3）难度值，难度值（difficulty）是矿工们在挖矿时候的重要参考指标，它决定了矿工大约需要经过多少次哈希运算才能产生一个合法的区块。比特币的区块大约每10分钟生成一个，如果要在不同的全网算力条件下，新区块的产生保持都基本这个速率，难度值必须根据全网算力的变化进行调整。简单地说，难度值被设定在无论挖矿能力如何，新区块产生速率都保持在10分钟一个。

难度的调整是在每个完整节点中独立自动发生的。每2016个区块，所有节点都会按统一的公式自动调整难度，这个公式是由最新2016个区块的花费时长与期望时长（期望时长为20160分钟即两周，是按每10分钟一个区块的产生速率计算出的总时长）比较得出的，根据实际时长与期望时长的比值，进行相应调整（或变难或变易）。也就是说，如果区块产生的速率比10分钟快则增加难度，比10分钟慢则降低难度。这个公式可以总结为如下形式：

新难度值 = 旧难度值 *（过去2016个区块花费时长 / 20160 分钟）（2-1）

工作量证明需要有一个目标值。比特币工作量证明的目标值（Target）的计算公式如下

目标值 = 最大目标值 / 难度值　　（2-2）

其中最大目标值为一个恒定值：
“0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF”目标值的大小与难度值成反比。比特币工作量证明的达成就是矿工计算出来的区块哈希值必须小于目标值。

我们也可以简单理解成，比特币工作量证明的过程，就是通过不停的变换区块头（即尝试不同的nouce值）作为输入进行SHA256哈希运算，找出一个特定格式哈希值的过程（即要求有一定数量的前导0）。而要求的前导0的个数越多，代表难度越大。

4）工作量证明的过程：我们可以把比特币矿工解这道工作量证明迷题的步骤大致归纳如下：

生成Coinbase交易，并与其他所有准备打包进区块的交易组成交易列表，通过Merkle Tree算法生成Merkle Root Hash；把Merkle Root Hash及其他相关字段组装成区块头，将区块头的80字节数据（Block Header）作为工作量证明的输入；不停的变更区块头中的随机数即nonce的数值，并对每次变更后的的区块头做双重SHA256运算（SHA256(SHA256(Block_Header))），将结果值与当前网络的目标值做对比，如果小于目标值，则解题成功，工作量证明完成。

5）全网同步，答成共识当矿工完成解题之后将结果广播给全网节点，每个节点进行验

算，正确后生成新的区块。

比特币的工作量证明，其实就是我们俗称“挖矿”所做的主要工作。理解工作量证明机制，将为我们进一步理解比特币区块链的共识机制奠定基础。

3. 区块链应用的不可能三角问题研究与量化模型

区块链系统现在已经逐渐的发展成一个复杂多样的技术体系，随着区块链技术发展成熟，将会被用在更多的领域，改变经济发展乃至社会进步。将基于区块链技术成产品或者解决方案应用到实际生产环境或者商业环境中，这不单单是个技术问题，也是个经济问题，即如何配置最优化的资源，以最优化的价格来达到相应的目标。这里我们应借鉴经济学中的不可能三角理论去合理的认识区块链在应用当中的三个重要特性的制约关系。

“不可能三角”（Impossible trinity）是1999年由美国麻省理工学院教授克鲁格曼在蒙代尔-弗莱明模型的基础上，结合对亚洲金融危机的实证分析提出的。“不可能三角”(Impossible triangle/Impossible trinity theory)是指经济社会和财政金融政策目标选择面临诸多困境，难以同时获得三个方面的目标。在金融政策方面，资本自由流动、汇率稳定和货币政策独立性三者也不可能兼得。即一个国家不可能同时实现资本流动自由，货币政策的独立性和汇率的稳定性。也就是说，一个国家只能拥有其中两项，而不能同时拥有三项。如果一个国家想允许资本流动，又要求拥有独立的货币政策，那么就难以保持汇率稳定。如果要求汇率稳定和资本流动，就必须放弃独立的货币政策。

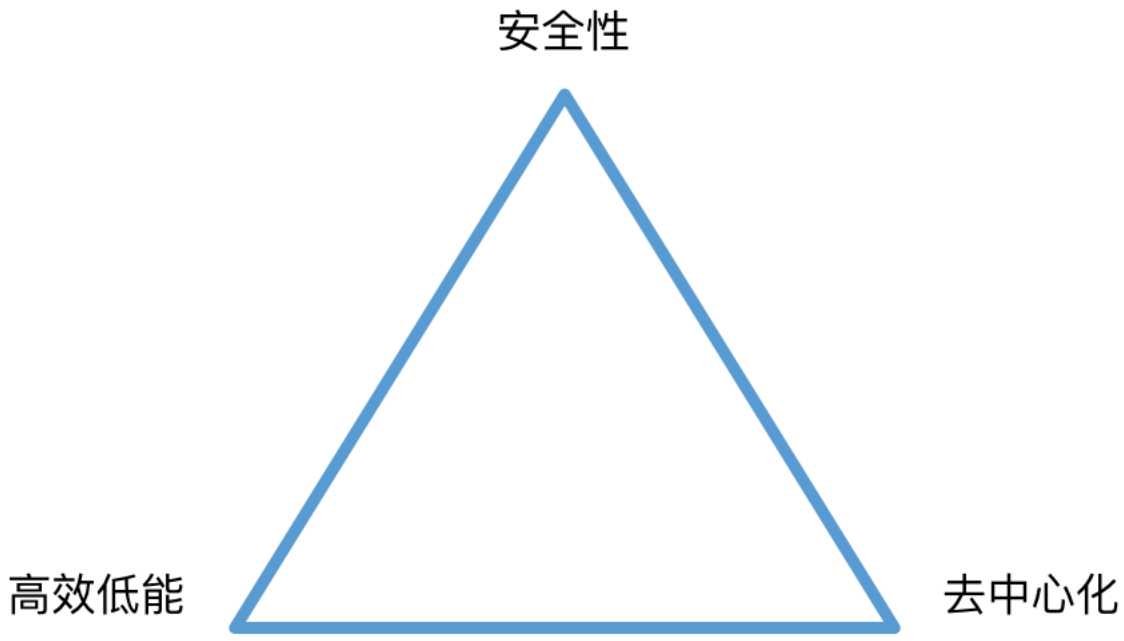

图3.1 不可能三角

对于区块链系统用于实际场景当中，在充分分析区块链三大特性各自的内涵与量化表示、相关影响因素之上，结合试验及分析，要进一步研究它们之间的关系，探讨区块链“不

可能三角”难题 —— 区块链应用难以同时满足“安全”、“去中心化”和“高效低能” 三个条件。

3.1 安全性

区块链安全：区块链系统由于采用了多种安全技术组合，在安全性角度来说有其独特的特性。可以从两个方面去考察其安全性：

1、系统级安全：一般信息系统的安全性是以系统可用性来表征的，如平均故障间隔时间:MTBF (Mean Time Between Failure)，平均修复时间: MTTR(Mean Time To Repair), 以及它们的组合如

$$Availability = MTBF / (MTBF + MTTR) \quad (3\text{-}1)$$

扩展到系统级的，可以有两个模型即串联和并联模型，串联模型的整体可用性分别为

$$A = Ax*Ay \quad (3\text{-}2)$$

$$A= 1-(1-Ax)^2 \quad (3\text{-}3)$$

参考一般信息系统的可用性公式，考察区块链系统安全参数及公式。在在共识机制的作用下，只有当全网大部分节点(或多个关键节点)都同时认为这个记录正确时，记录的真实性才能得到全网认可，记录数据才允许被写入区块中。比如比特币区块链需要51%节点认可。区块链的分布式架构赋予其点对点、多冗余特性，不存在单点失效的问题，因此其应对拒绝服务攻击的方式比中心化系统要更灵活、系统鲁棒性更强。即使一个节点失效，其他节点不受影响，与失效节点连接的用户无法连入系统，非有支持他们连入其他节点的机制。 这种特性可以很好的应对外部的实体攻击。

由此可见区块链有别于其它系统，其系统级的安全性是靠分布式网络全节点的算力来保证的，即51%的算力不受到攻击控制，就能保证其整体安全性。也就是说网络节点数量越大，恶意攻击和控制51%算力的难度越大，其系统安全性就越高，用数学表达式即为：

$$S\ sys = G\ (\ N\ ) \quad (3\text{-}4)$$

其中n为网络的节点数， G为的N增函数，G的函数特性根据所依赖的不同的共识机制不同而不同。

2、数据、信息安全：这是相对的比较微观的安全层面问题。区块链没有固有的信息读取安全限制，但可以在一定程度上控制信息读取，比如把区块链上某些元素加密，之后把密钥交给相关参与者。同时，复杂的共识协议确保系统中的任何人看到的账本都是一样的，这是防止双重支付的重要手段。 也就是说为了确保数据、信息的安全性，相对应的安全措施随着安全加密算法的难度增大而增大用数学表达式为：

$$S\ data = H\ (Diff) \quad (3\text{-}5)$$

Diff 为安全加密算法难度，H位Diff的增函数。而整体的安全量度是系统安全和数据安全的增函数，即

$$S\ total = F\ (S\ sys\ ,\ S\ data) \quad (3\text{-}6)$$，变形后，得到

$$S\ total = F'\ (N,\ Diff) \quad (3\text{-}7)$$

由公式容易得到，区块链的整体安全随着节点数量即区块链规模增大而增大，同时随着加密安全算法的难度提升而增大。

区块链系统的特点及应用场景也面临了相应安全挑战，包括：

1)网络公开不设防: 对公有链网络而言，所有数据都在公网上传输，所有加入网络的节点 可以无障碍地连接其他节点和接受其他节点的连接，在网络层没有做身份 验证等防护。针对该类风险的应对策略是要求更高的私密性并谨慎控制网络连接。对安全性较高的行业，如金融行业，采用专线接入。对接入的连接进行身份验证，排除未经授权的节点接入以免数据泄漏，并通过协议栈级别的防火墙安全防护，防止网络攻击。

2)隐私及信息安全：公有链上交易数据全网可见，公众可以跟踪这些交易，任何人可以通过访问区块链获得信息，不利于个人或机构的合法隐私保护。 针对该类风险的应对策略是:第一，用户资料不上链，而由认证机构代理用户在区块链上进行交易。第二，对用户数据的访问权限加以控制，只有持有密钥的访问者才能解密和访问数据。第三，采用新的加密技术例如“零知识证明”等隐私保护算法，规避隐私暴露。

3)算力的集中度:在所有使用工作量证明型（POW）的区块链解决方案中，都面临51%算力攻击问题。即随着算力的逐渐集中，存在有掌握超过50%算力的组织或者机构出现的可能，逐渐演变强中心化的系统，称为弱肉强食的丛林法则。在自由空间生长的系统，主要是靠系统产生的激励吸引更多的参与者，增大其去中心化程度来规避集中度风险。

3.2 去中心化

区块链技术及应用最显著的特征是由去中心化的分布式节点自主有效管理，取代了传统系统中不可或缺的中心管理统治者。即在处理链内数据时，无需依赖于单一信任中心的系统，区块链本身能够创造参与者之间的信任。也就是说无需参与者自身属性及相关的信用背书，通过区块链，通过技术本身就能确保参与者之间的交流、交换、价值传递是可以信任的。

能完成去中心化的数学基石之一就是去中心化分布式数据库，区块链是去中心化的，不存在任何中心节点，由多方参与者共同管理和维护，每个参与者都可供节点并存储链上的数据，从而实现了完全分布式的多方间信息共享。 分布式账本中任何一方的节点都各自拥有独立的、完整的一份数据存储，各节点之间彼此互不干涉、权限等同，通过相互之间的周期性或事件驱动的共识达成数据存储的最 终一致性。

如何使各个独立的节点在互不干涉的前提下还能达成确认和数据的一致性？ 这就引出了基石之二：共识机制。不同的共识算法在应对同样规模的网络规模会产生很大差异的结果。即便在同一个共识算法作用下，不同规模的网络的运营效率也大有不同。

另外，在竞争账本的记账权方面, 全网的节点参与竞争，并且需要得到超过总数51%的节点的确认才能产生新的区块。所以节点数量越大，分布越广，节点的控制者约分散，它越不容易被恶意攻击或被少数人控制。两个个主要因素可以表征去中心化程度即：

1）分布式节点数目规模（S: Scale), 它其实就是直接表征区块链节点数的参数，也可以直接用N来表示。

2）分布的离散度 （Disp: Dispersion)， 也就是节点的控制方越不集中，其离散度越高。

而总的去中心化程度由三者有机的组合而成，即：

$$\text{Decentralization} = E(S, D) = E(N, D) \qquad (3\text{-}8)$$

三者当中，可以认为节点数目规模是最重要的因素, 也可以用N直接来表示。即节点越多其去中心化程度越高。但去中心化系统也有些先天特性和现实应用也带来一些问题，面临挑战，具体如下：

1）去中心化分布式网络的传输延迟。因为在区块链网络中，每个节点都有机会参与记账环节，每个节点需要同步全部区块信息方才可以进行交易的处理与记账。因此，整个网络同步的效率受限于网络中延迟最长的节点。

2）分布式数据管理与安全措施：公有链允许任意节点加入网络、允许任何用户参与交易，全部账本数据公开透明且由多方共同维护。这些有别于传统数据库的特性，使得区块链系统无法直接应用传统数据库的安全机制。用户管理通 常需要运行在中心化的节点上，这就和区块链所强 调的去中心化相矛盾。另外，传统存取控制也与公有链 所强调的数据公开性和透明性相矛盾。对于信息安全而言，区块链系统主要基于数字签名与验证来确保数字货币 的所有权以及交易的不可伪造、不可否认; 依靠每次交易使用不同的数字证书和账户地址来保障交易的隐私性。

3）保证一致性与节点性能问题：目前主流的公有链如比特币、以太坊仍然使用工作量证明共识机制，用于记账的节点需要消耗大量的计算资源来进行哈希运算以竞争记账权，从而在效率上存在一定限制。另外，由于区块链数据只是追加而没有被删除，随着区块数据量的加大，对节点的存储空间和吞吐性能也提出了越来越高的要求。以以太坊为例，目前总区块文件的大小已经突破500GB，如要实现每秒上百万笔交易的交易速度，需要提供数百MB/s吞吐能力的节点，这是很高的要求。影响区块链吞吐量的两个核心参数为区块容量和区块间隔时间。通常区块容量通常不会无限制扩大。而如果区块间隔时间过小，在全网都参与记账的环境中，可能会由于不同节点来不及完全同步最新的区块广播而产生不同的新区块，从而造成严重的分叉问题，进而严重影响区块链的实际可用性。

由以上分析可见，去中心化的结构保证了区块链系统的交易公平性，记账权获取的平等性和系统的安全性，但为了保证去中心化程度更高，对系统算力的消耗更大，对传输网络及单个节点的处理能力的提升越大。

3.3 系统效率

效率，一般指工作产出与投入之比，通俗地讲就是在进行某任务时，取得的成绩与所用时间、精力、金钱等的比值。可以由物理系的公式

效率=输出功率/输入功率 * 100%，即 E = Pout / Pin * 100%　　（3-9）

产出大于投入，就是正效率; 产出小于投入，就是负效率。

为了保持区块链系统数据的一致性，即中心化账本的一致性，需要产生共识，并全网节点对其进行验证和同步。这个过程需要去中心化系统的每个节点参与并产生一定的消耗。而区块链的重要应用场景和作用就是解决效率问题，提升业务处理效率，降低交易成本。因此，在区块链实际应用场景中，应充分考虑共识机制所消耗的成本，并与其在业务层提升的部分比较，从而获得一个比较优化的解决方案。

一般来说，区块链所需的消耗可以从两个维度可以考虑。

1）对能源的消耗，其总能耗等于每个节点的能耗的总和，即

$$P_{total}(N) = \sum P(i),\ i = 1,2,3\cdots N \qquad (3\text{-}10)$$

其中 N为总的节点数目，可知，随着N的数目增大P(N) 值会增大。在Pout不变的情况下，效率 E 与 Pin成反比。另外每个节点的功耗与快生成时解题难度有关，也与区块链上安全机密的程度有关。系统内安全性越高，节点的功耗也越高。

2）另一个维度是时间，即从产生交易，计算，验证，同步整个过程中网络节点所消耗的时间 T，这个时间也可以表征效能。

举例采用PoW共识机制，在区块链系统中区块产生及共识流耗时如下：

⑴ 每笔新交易被广播到区块链网络的所有节点的时间 T0，与网络节点多少以及网络大小有关，因为是广播消息，其时长与节点个数并不是线型，而是到达最远节点的时间, 即

$$T0(N) = Max\ T0(i),\ i = 1, 2, 3\cdots.N; \qquad (3\text{-}11)$$

⑵ 为了构建新的区块，每个节点收集自前一区块生成以来接收到的所有交易，并根据这些交易计算出区块头部的 Merkle 根。节点消耗自身算力尝试不同的随机数，如将区块头部的随机数Nonce 从 0 开始递增加 1，直至区块头的两次 SHA256 哈希值小于或等于难度目标的设定值为止。这个过程俗称“挖矿”。 这个过程时长为 T1：每个节点进行随机数的计算的时间，和难度有关。

$$T1(N) = Min\ T1(i),\ i = 1,2,3\cdots N; \qquad (3\text{-}12)$$

T1(i) = T1 (Diff, i ），其中Diff 为每次计算的复杂程度。

⑶ 全网节点同时参与计算，若某节点先找 到了正确的随机数，生成区块信息 （块头+块身）。该节点将获得新区块的记账权及奖励（奖励包括新区块中的创世币及每笔交易 的交易费用），并将该区块向全网广播。 T2: 建立新块并广播时间，与T1相类似，但应该比T1长，取决于传输时间最长的那个。

$$T2\ (N) = Max\ T2\ (i),\ i=1,2,3\cdots N \qquad (3\text{-}13)$$

⑷其它节点接收到新区块后，验证区块中的交易和随机数 Nonce 的有效性，如果正确，就将 该区块加入本地的区块链，并基于该块开始构建下 一区块。 其时长T3为本地验证的时间。

$$T3(N)= Max\ T3\ (i),\ i=1,2,3\ldots N \qquad (3\text{-}14)$$

总的时长为： $T\ total\ (N) = T0\ (N) + T1\ (N) + T2\ (N) + T3\ (N)$ （3-15）

其中只有T1 是复杂度 Diff 的函数，其它都是节点数的函数，所以原等式可以变形为：

$$T\ total\ (N) = F\ (Diff, N) = MinT1(i) + T'(N) = Min\ T1\ (Diff, i) + K\ (N) \qquad (3\text{-}16)$$

其中K(N)是N的增函数。 所以输入的总能量为：

$$P\ in = F\ c\ (P\ total\ (N), T\ total\ (N)) \qquad (3\text{-}17)$$

在输出不变的情况下，输入功越大，其效率越低。效率是决定区块链技术是否能用到应用当中的决定性因素，面临诸多挑战，如:

1) 分布式记账的数据量问题[12]：为了保证区块链数据的不可篡改性和可追溯性，账本记录了整个链从开始到目前的所有交易记录，数量巨大。每个新节点加入都要同步所有的数据，同步的数据量和时间严重影响了工作效率。

2) 交易效率问题：以比特币为例，一秒只能处理7笔交易，平均十分钟处理一个区块。这种效率无法满足需求。

3) 单节点性能影响全局性能：比特币、以太坊 和 Hyperledger Fabric 目前都采用全网节点共享一 条区块链的单链方案，网络上的每个节点需要处 理、存储全网的所有交易和全部数据，整个区块链 系统的处理能力实际上受限于单个计算节点的处 理能力。

综上所述，随着节点数的增加，系统整体处理能力不但未随之升，整体效率还会降低。

3.4 不同共识机制下的研究

区块链系统的去中心化是依赖共识机制来保持其一致性，系统的安全性也是依赖于共识机制，而区块链的效率瓶颈主要在于共识算法。所以我们有必要研究不同的共识机制对这个三特性的影响。

本文已经以POW为例，对共识机制的原理进行了介绍，下面介绍下另外两种主流的共识机制并加以对比研究说明。

1） 权益证明（Proof of Stake，PoS)

权益证明要求用户证明拥有某些数量的货币（即对货币的权益），根据这些权益来决定挖矿的难度。PoS(Proof of Stake)算法最早由 Sunny King 在 2012 年 8 月发布的 PPC (PeerToPeerCoin 点点币)系统中首先实现，针对 PoW 机制低效、耗能的缺陷，PoS 机制无需矿工购买矿机、消耗电力及进行无意义的计 算，而是根据矿工在区块链中拥有的股权(即数字 货币量)来决定其挖矿的难度:

$$H(n||h) \leqslant s(M).t\ (2) \qquad (3\text{-}18)$$

M 为某矿工; 函数 s 返回该矿工拥有的股权; 当矿工 M 拥有的股权越多，挖矿的整体难度就会越低，其越容易找到合适的 n。太坊系统一直有计划引入PoS 。PoS 及其变种算法可以解决 PoW 算法一直被诟病的浪费算力问题，但其本身尚未经过足够验证。

2）PBFT （实用拜占庭容错算法）

PBFT是Practical Byzantine Fault Tolerance的缩写，意为实用拜占庭容错算法。该算法是Miguel Castro (卡斯特罗)和Barbara Liskov（利斯科夫）在1999年的OSD99会议上提出来的，解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。该论文发表在1999年的操作系统设计与实现国际会议上（OSDI99）。Loskov就是提出著名的里氏替换原则（LSP）的人，2008年图灵奖得主。

PoW 机制依靠算力竞争来保障区块链数据的 一致性及安全性，但算力竞争毫无意义地消耗了大量计算资源和电力能源，并不适合于针对企业级应 用的联盟链。联盟链更适合应用无需消耗计算资源 和电力能源的 PBFT 算法。PBFT 算法可容忍恶意节点不超过全网节点数量的 1/3，即如果有超过 2/3 的正常节点，就可保障数据的一致性和安全性。 假设系统中共有 N 个节点，那么 PBFT 算法可以容忍系统中存在 F 个恶意节点，并且 3F+1 不大于 N。PBFT 在区块链网络中的共识流程如下:

⑴从全网节点选举出一个主节点，新区块由主节点负责生成。

⑵每个节点把新交易向全网广播，主节点 把从网络收集到需放在新区块内的多个交易排序 后存入列表，并将该列表向全网广播。

⑶每个节点接收到交易列表后，依据排序 模拟执行交易。所有交易执行完后，基于交易结果计算新区块的哈希摘要，并向全网广播。

⑷如果一个节点收到的 2f(f 为可容忍的恶 意节点数)条其它节点发来的摘要都和自己相同， 就向全网广播一条 commit 消息。

⑸如果一个节点收到 2f+1 条 commit 消息， 即可正式提交新区块及其交易到本地的区块链和 状态数据库。

PBFT 共识过程中的每个区块都由唯一的主节点生成，所以不存在分叉的可能。但在节点数为N 的网络中，该算法有两个阶段需要传输的网络消息 为 O(N^2)，其会造成很大的网络开销。PBFT 共识算法虽然随着系统中节点数增多而可以容忍 更多的拜占庭节点，但其共识效率却是以极快的速率下降，这也是我们能看到的应用 PBFT 做共识算法的系统中很少有超过 100 个节点的原因。目前基于 PBFT 算法的区块链的系统性能并不高。另外，如何支持共识节点的动态加入和退出也是有待 解决的问题。

通过对下图的对比我们可以看出PoW 与PBFT 两类不同的共识机制的性能差别：

1）去中心化方面：PoW所承载的网络节点远远高于PBFT，所以它的去中心化程度远高与后者。

2）在工作效率方面：当节点数比较少的情况下，基于PBFT的确认时间比基于PoW的系统提高10万倍，交易的吞吐量也提高了近100倍。在资源消耗方面：PoW 主要消耗的是计算能力和相关的解题时间。而PBTF消耗的是网络通信的资源。

3）安全性方面：因为PBFT系统本身不是完全去中心化的，并且它对于恶意节点的容错只有1/3，其系统安全性远低于PoW。

	PoW	POW	PBFT
链名称	比特币	以太坊	Fabric
节点准入机制	公链	公链	联盟链
交易吞吐量	7TPS	20-30TPS	200-2000TPS
节点量级	10万	10万	小于100
系统安全容错	< 50%的算力	< 50%的算力	< 33%的投票
资源消耗	大（哈希计算）	大（哈希计算）	中等 （广播）

图3.2 共识机制比较

实际测量结合原理可知，PBFT本质上是牺牲了去中心化和系统安全性来提升了系统的效率。其安全性要依赖于区块链以外的准入机制，它适合运用到规模较小的联盟链和私有链中。由此可见，无论是上图中哪种共识机制，都无法同时满足安全性、去中心化和高效低能同时存在。

无论是 PoW 算法还是 PoS 算法，其核心思想都是通过经济激励来鼓励节点对系统的贡献和付出。公链系统为了鼓励更多节点参与共识，通常会发 放代币(token)给对系统运行有贡献的节点，因为Token的存在也引发了新的经济现象 — Token经济。而联盟链或者私链与公链的不同之处在于，它们之中的参与节点通常希望从链上获得可信数据，或者形成交易。在这样目的的激励下并且在组织的管理下，他们有责任去维护系统的稳定运行，并且通常参与节点数较少，PBFT 及其变种算法恰好适用于联盟链或者私链的应用场景。

对传统分布式一致性共识算法和PBFT的不足，结合公有区块链中的授权机制，重新[4]设计和实现了新的拜占庭容错算法，称为“动态授权拜占庭容错”共识算法，建成DDBFT。针对特定需求的共识机制：我们相信共识机制将发展为针对特定需求，其中包括特定用例的需求、技术执行可能性的需求或监管环境的需求。允许不同参与者根据角色需求不同，制定不同的节点类型，划分不同权限进行连接、发送、接收、发出、 挖掘、激活或管理等操作。

3.5 同一共识机制内的实验分析

用理论研究和试验相结合的方法，以以太坊[13]为例来研究在同一共识机制的区块链系统内，对去中心化、安全性及应用效率三者进行考察和分析。

实验环境：为了使实验更有针对性和可操作性并有利于进一步理论分析，实验采用比较一致的物理及软件条件：

1）软件系统配置：部署上采用以太坊及其POW共识机制。

2）硬件配置：每个节点的硬件配置保持一致。

- System Clock :33MHz
- Width:32bits
- OS Vendor: Red Hat, Inc

3）网络条件：局域网环境内，保障至少500M的点对点传输带宽。

测试方法：在上述的局域网环境下，给个主机部署以太坊开源软件后，构成区块链网络。从三节点的配置开始开启挖矿动作。开始采集一段时间内（24小时左右）生成所有新区块的个数，并用总时长去除，得到该段时间内平均生成一个区块的时长。然后从三节点每次增加一个节点，逐步递增到十个节点来逐步比较其新区块生成的平均时间。实验结果如图：

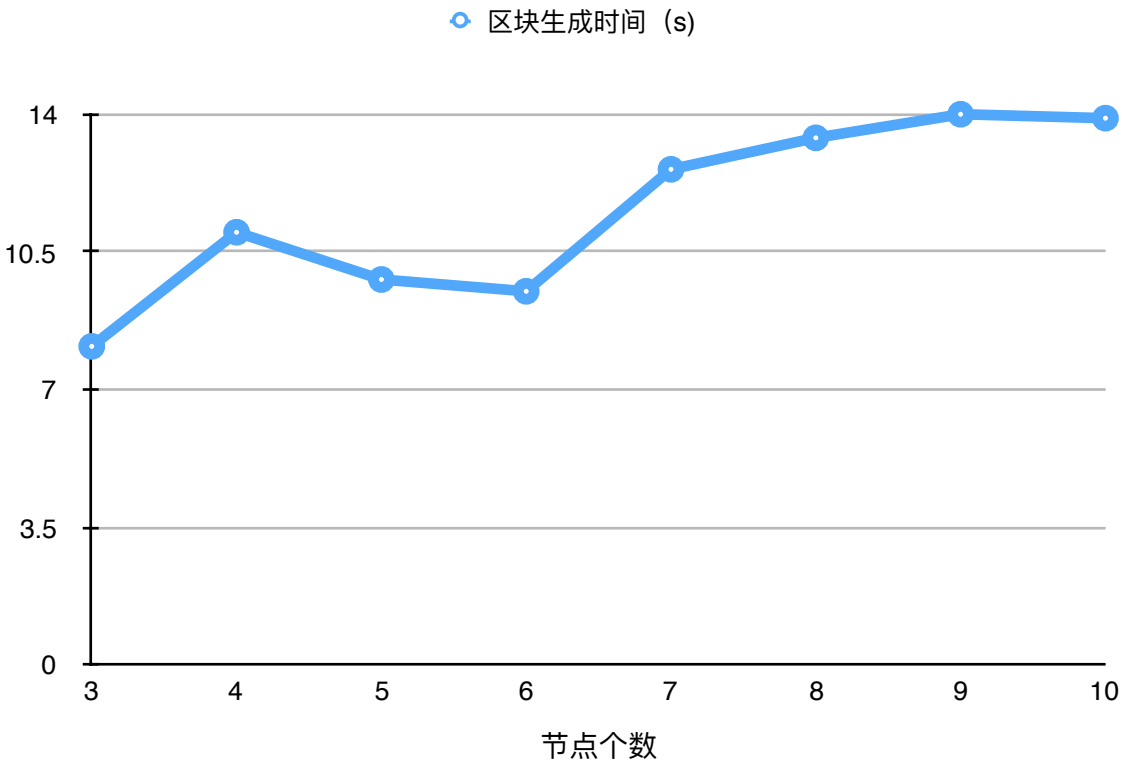

图3.3 节点数递增情况下区块生成时间

上图可知，随着节点数的增加，区块生成时间逐步增多，从三节点的8秒上升到了十节点的14秒左右，上升的态势还是比较明显的。根据之前的区块链生成块的总时长公式：

$$T\ total\ (N) = F(Diff, N) = MinT1(i) + K(N) = Min\ T1(Diff, i) + K(N) \quad (3\text{-}19)$$

下面研究MinT1(Diff, i) 与K(N)的内涵与逻辑。首先，在这部分的工作里面，有一个目标难度Diff计算，以太坊中采用了三种规则来计算目标难度，具体如下所示：

- calcDifficultyByzantium（Byzantium版）
- calcDifficultyHomestead（Homestead版）
- calcDifficultyFrontier（Frontier版）

这里将以calcDifficultyHomestead为例子，来讲解相关的计算算法，在计算难度的时候要注意四个输入参数，如下所示：

- parent_timestamp：父节点区块timestamp

- parent_diff：父节点区块难度值
- block_timestamp：本节点区块timestamp
- block_number：本节点区块序号number

根据这几个区块输入参数，可以得出当前区块难度的计算公式，具体如下所示：

block_diff = parent_diff+ (parent_diff / 2048 * max(1 - (block_timestamp - parent_timestamp) // 10, -99) + 2^((block_number // 100000) - 2)　（3-20）

（其中“//”是整数除法运算符，比如说x//y，先计算x/y，结果是不大于x/y的最大整数值）

这个计算公式保证了出矿的时间在10-19s之间，如果低于10s就增大难度，大于19就减小难度，当前区块的难度不会低于创世区块的难度。这些巧妙的机制保证了系统性能的稳定性和可预测性。也就是说MinT1（Diff，i）的取值是在一个常量范围内，理论上不随着节点数目N的变化而改变。

其次，研究下K(N)这个函数，包含了所有与节点数目相关的函数。以太坊采用POW公式工作工程中，在新区块计算的全网广播时长，各节点的验证时长，新区块的确认时长，区块数据更新时长等都受到节点数N的影响。也就是说T(N）在一定程度上随着N的数目增长而增大。由下图可知，区块的生成平均时间随着N的增长呈线性增长。

N代表的是节点个数，代表去中心化程度，由此可见，去中心化程度越高，系统安全性越高，在一定范围内区块生成的工作时长变长，区块链系统的效率变低。去中心化（包括隐含的系统安全性）与区块链效率存在着此消彼长的反比例关系。

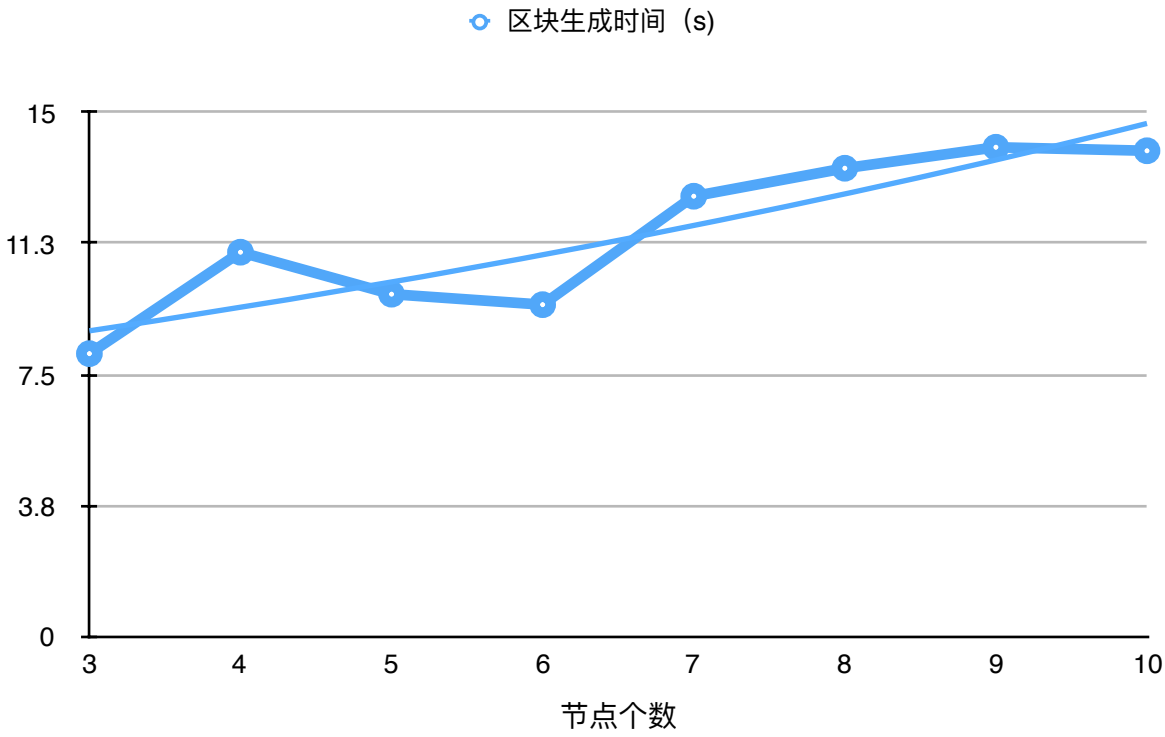

图3.4 生成区块量的点拟合

连接各点拟合，可以看出是一条线型向右上方倾斜的曲线。即类似于 Y = a+bX 的一次曲线。对应到公式 T total (N) = Min T1 (Diff, i)+K(N)， Min T1 (Diff, i)基本为常量a，K(N)近似于等于bN, 即 T total (N) = a + bN , 与上面结论相同，总时长与N成正比，效率与N成反比。

由此可见，经过实验与数据的分析验证了区块链功耗的重要指标总时长Ttotal (N)是在一个基本恒定值之上叠加了一个节点数N的增函数，在一定范围内，随着节点数N增大系统消耗也增大。也就是说中心的程度越高，系统安全性越高，系统消耗就越高，其系统效率就回降低。

3.6 区块链不可能三角分析

在之前的章节我们把将三个特性量度的数学表达做了定义，并结合实验分析了之间的关系印证了原理性分析。结合“不可能三角”和量化特征进行讨论和总结。

首先，确保区块链系统的高安全性和高度的区中心化程度的情况下，必须牺牲其系统效率。原理上很容易理解，高安全性所要求的难度较高的加密算法，即S data = H (Diff)，从而需要更多的算力解决。同时，高等级的去中心化意味着系统的节点数目N增多，根据 P total (N)= $\sum$ P (i) , i= 1,2,3…N，而这直接导致了系统所消耗的算力增多。

事实上区块链系统主要基于数字签名与验证来确保数字货币的所有权以及交易的不可伪造、不可否认; 依靠每次交易使用不同的数字证书和账户地址来保障交易的隐私性。也就是数据的安全与开放的分布式之间是有矛盾的，而为了确保两者的兼顾，用了密码学即更消耗算力的方法与弥补。也就是说牺牲了系统的效能来满足去中心化与安全性。从上可知，为了保证这两个方面的要求，区块链系统的效率下降。从系统安全角度来说，区块链节点组成

的网络越分散，节点数量越多，去中心化程度越高，其系统安全性越高，即很难对其形成占多数的51%攻击。但这个规模下区块链共识所需的成本太高！但所需要消耗的算力自然就越多，系统的效率越低。在实际应用中应避免一味的考虑系统的规模，去中心化水平即安全性而忽视了系统效率，即影响了用户体验，也起不到区块链价值传递的核心价值。

其次，在确保系统高效低能与安全性同时存在的情况下，必须牺牲其去中心化。系统消耗的能耗为 T total (N) = Min T1 (Diff, i)+K(N) 和P total (N)= ∑ P (i) , i= 1,2,3…N都是 N的增函数，即随着N的增大，输入的能耗增加，整体效率随之降低。所以高效低能一定意味着节点数目N限制在一定范围内。在N比较小的时候为了确保安全性系统借助其它安全鉴权机制保证区块链上的内容隐私受到保护。而因为N取值小，即整个区块链的规模较小，其去中心化受到了影响，上文提到的PBFT就是这个情况。

另外，在保证去中心化程度高与高效低能的条件下，必须牺牲其安全性。去中心化程度高意为着节点数N相对较高，保持高效低能意味着P值较小。由公式 P total (N)= ∑ P (i) , i= 1,2,3…N， 可知，在保证N较大值而P total不变或者减小的情况下，只能降低每个节点的功耗P(i)。 而决定P(i) 的是安全难度 Diff，只能降低系统的安全算法难度，以牺牲其安全性来保证相对较高的去中心程度和高效低能。

由此可见，用原理推导和定量分析可知，区块链系统中的重要特性：“去中心化”、“安全”与区块链应用中“效率”三者不可能同时满足，被称为区块链应用的不可能三角。

4. 结 论

区块链是一场伟大的技术革命，它综合了密码学、分布式存储、共识机制、智能合约等技术,实现了在互不了解的交易双方间建立了可靠的信任，去中心化地实现了可信的价值传输，达成了对等的直接交易。合理的将技术有效的应用到合适的场景中能提高整个社会的效率和发展水平，因此区块链被称为价值互联网或第二代互联网。本文通过大量的收集现有的文献和研究成果，结合应用对区块链系统的主要特性“安全”、“去中心化”与其应用必须要考虑的“效率” 因素 进行了深入的研究、分析。并设计实验方案进行了实施与相关的数据分析。利用经济学的原理、方法和思维结合技术研究与实验，对区块链三个重要因素的属性进行量化分析并对三者的关系即区块链不可能三角的分析研究。为区块链技术合理的运用到实际当中提供了基础，希望能对区块链的发展起到积极的作用。

主要参考文献

[1]Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL].www.bitcoin.org
[2]Blockchain [EB/OL].https://en.wikipedia.org/wiki/Blockchain
[3]杨龙飞. 区块链的关键技术、应用与挑战[J].中国计算机学会通信，2018(6):43-50.
[4]荆林波 . 信息通讯技术、生产率悖论与各国经济增长[J].经济学动态, 2010(6):93-97.
[5]陈一稀.区块链技术的不可能三角及需要注意的问题研究[J].浙江金融，2016(2):17-20.
[6]邵奇峰，金澈清，张召等. 区块链技术：架构及进展.[J]计算机学报，2017, 40:1-21.
[7]Antonopoulos A M. Mastering bitcoin: Unlocking digital cryptocurrencies. Sebastopol,USA: O'Reilly Media, Inc., 2014）
[8]冯登国 网络安全原理与技术 北京：科学出版社， 2003
[9]刘岠，吕述望. 基于证书的多媒体信息客户端安全解决方案[J].电子测量技术，2007(11):中国人民大学出版社，2011:7.177-181.
[10]华为区块链白皮书[EB/OL].https://static.huaweicloud.com/upload/files/pdf/20180411/20180411144924_27164.pdf
[11] Burningoctopu. ELI5: The Difference between POS and POW ? [EB/OL].https://www.reddit.com/r/ethereum/comments/38db1z/eli5_the_difference_between_pos_and_pow/
[12] 沈鑫，裴庆祺，刘雪峰.区块链技术综述[J].网络与信息安全学报, 2016(11):14-20.
[13] Mining[EB/OL]. http://www.ethdocs.org/en/latest/mining.html

[作者简介]

刘岠，男，第一视频集团研究院院长，中国计算机学会区块链专家委员会委员，主要研究方向为信息安全，互联网.
荆林波，男，中国社会科学院社会科学评价院院长，主要研究方向为社会评价，经济学，电子商务.
王静逸，男，第一视频集团研究院研究员，主要研究方向为区块链，图形学.