doi: 10.12052/gdutxb.180033

赛博智能经济与区块链

徐　恪，姚文兵
（清华大学　计算机系，北京 100084）

摘要: 互联网已经和经济系统深度融合形成了新的“赛博经济系统”. 本文探讨了赛博经济系统的主要特征，分析了当前赛博经济发飞速发展的原因. 从信息的角度出发，赛博经济是信息增长更快的经济，而信息有序与快速增长的核心原因是算法，进而以算法为基础提出了赛博经济的新形态——赛博智能经济. 认为区块链技术有望成为赛博智能经济的信任基础设施，使赛博智能经济迈入新时代. 同时，详细分析了区块链技术的特点，给出了当前区块链发展过程中面临机遇与挑战.

关键词: 区块链；赛博经济；智能经济；比特币
中图分类号: TP 393　　**文献标志码:** A　　**文章编号:** 1007–7162(2018)03–0001–09

Cyber Intelligent Economy and Blockchain

Xu Ke, Yao Wen-bing
(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Abstract: The Internet combines economic system forming the innovative cyber economic system. The principal characteristics of cyber economy are discussed and the reason of its rapid development analyzed. From the perspective of information, cyber economy is of faster information growth, and the core reason of the growth is algorithms. As the foundation, algorithms prompt the new form of cyber economy i.e. cyber intellectual economy. Analogously, blockchain is expected to be the reliable infrastructure of cyber intellectual economy and consequently to innovate it. Furthermore, the characteristics of blockchain are also analyzed, pointing out the future opportunities and challenges.

Key words: blockchain; cyber economy; intelligent economy; bitcoin

从1969年ARPANET诞生至今，互联网的发展经历了不到半个世纪，但其影响却是以往任何一个发明所不能比拟的. 网络加速了世界各地文化的融合、知识的传播，将世界紧密地联系到了一起. 3G、4G、大数据、云计算、人工智能、量子计算、天地一体化网络，这些新的概念近年来不断涌现，对传统行业造成了巨大的冲击，对工业、农业、商业带来了深远的影响，世界经济也逐渐摆脱了以往交流不畅的桎梏，得以飞速发展. 三次工业革命，不断地将人类从重复劳动中解放出来，不断释放人们的创造力，特别是第三次工业革命，直接将人类带入了科技时代. 计算机的产生是人类对机器智能研究的真正开始. 自计算机诞生以来，其是否可以具备思维能力这个话题从未淡出过人们的视线. 虽然现如今仍然没有一个可以思维的机器，但人工智能的发展成果喜人，特别是在计算机视觉、自然语言处理等领域，计算机的优势可见一斑.

互联网的诞生使得计算机如虎添翼，如今更是将人类推入了赛博时代[1]. 我们称以信息和知识为主导资源、以信息与网络产业为主导产业的新经济形态为“赛博智能经济”[1-2]，它是信息增长最快的经济，是可信任的经济. 在赛博智能经济时代，算法和机器智能高度自动化、自主化. 当前，赛博智能经济仍然处于雏形阶段. 在赛博智能经济孕育的过程中，信任问题不断凸显出来. 至美国次贷危机，信任问题全面爆发. 银行都不可信，那么谁可信？

2009年，比特币诞生[3]，比特币的诞生开辟了一个新的基于区块链的时代，它是对传统中心化信任

收稿日期： 2018-03-02
基金项目： 国家自然科学基金资助项目(61170292，61472212)
作者简介： 徐恪(1974–)，教授，博士生导师，研究方向为大数据、区块链.

体系的一次挑战. 比特币目前并没有被所有国家认可，但它所带来的影响不可忽视. 它改变了人们对建立信任的一贯认知，其设计运用了计算机科学、经济学甚至是心理学，其底层技术就是区块链. 区块链的诞生为解决信任问题提供了一个全新的思路，虽然其本身仍然存在许多问题，但赛博经济却有望在其帮助下得到飞跃.

1 赛博世界与计算思维

1948年，诺伯特·维纳发表的《控制论》一书中最先出现了以cyber为前缀的单词cybernetics，该词源于希腊语kubernetes，意为精于掌控. 如今cyber在被用于前缀时，如：cyber-space、cyber-security，通常都是为了说明此概念与互联网或者计算机相关，国人有将其简单译为“网络”. 实际上cyber一词的含义远超网络，它包含了物理网络和在其上承载的数据，以及基于这些数据所作出的分析、决策、控制.

在赛博时代，原有系统中的生产、消费、金融、市场等环节和领域被打破或颠覆. 互联网让一些诸如资金、资源、信息等要素更加高效的流通，让经济网络覆盖更广、耦合程度更深、效率更高，信息的增长也随之更快. 在生产中，数据先行，大数据分析已成为生产之前必不可少的环节. 网购、外卖已成为人们的习惯，消费不再需要面对面. 赛博经济是信息更快增长的经济，其推动力主要有两个：一是信息的增长，二是社会信任.

1.1 信息的增长

信息的增长是赛博世界的重要特征，赛博提供了信息快速增长的路径. 信任塑造了经济社会，它直接影响了赛博智能经济的发展速度. 区块链为原有的信任体系注入了新的血液，将为赛博智能经济的加速发展作出重要贡献. 进一步来看，增长的本质是什么？塞萨尔·伊达尔戈在他的《增长的本质》一书中写道：“经济是一个更深邃东西的世俗表现，它是信息生长的社会表现”，同时也指出经济是一个通过实体化拥有特定性质的信息来增强人们实际应用知识技术的系统. 可见经济的增长和信息的增长有着密切的关系. 在赛博世界中，信息的增长呈现出爆发式的特性，图1展示了近十几年的网络流量的状况.

赛博时代，信息为何能够如此快速地增长？这可以从赛博经济的3个主要特征[1]来看：1) 小世界；2) 幂律与长尾；3) 信息级联. 小世界现象最早由Duncan Watts和Steven Strogatz在1998年提出，以高聚集系数及低路径长度为主要特征. 小世界网络的一个典型的例子是人际关系网络，相关的理论就是“六度分割”. 六度分割理论指出：在社会网络中，人们是紧密联系的，一个人联系到世界上任意其他人平均只需要6步，也就是经过5个中间人. 这种人与人之间的紧密联系性在互联网时代的表现尤为突出，让信息的传播速度更快，传播范围更加广泛. 幂律分布是网络中另一个常见特征，最直观的理解就是在网络结点中少量结点的度非常大. 为人们熟知的二八定律就是幂律分布的一种体现. 二八分布即20%的部分做出了80%的贡献. 因此传统观点认为20%的关键部分非常重要. 我们称前面做主要贡献的为“头部”，而后80%为“尾部”. 与传统观点不同的是，长尾理论认为在互联网高度发达的时代，“尾部”应该成为我们关注的重点，原因是在急剧变化的市场中，由于互联网信息传递的速度十分迅速，头尾会随时发生位置转换. 赛博小世界、幂率与长尾等特征的出现推动了信息级联，信息经过传播、重组、再传播、再重组……这个过程传播速度不断加快.

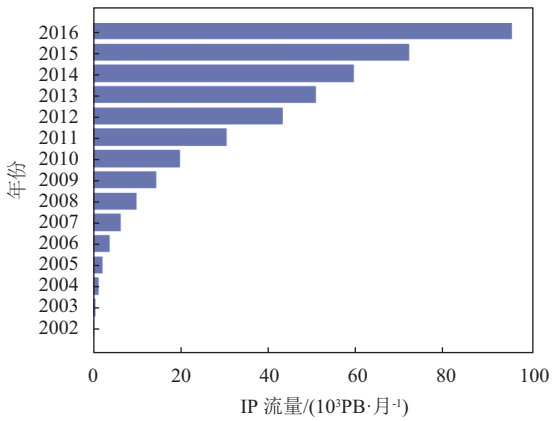

图1 全球网络流量增长

Fig.1 Global IP traffic growth

要把握赛博时代的经济，需要完成从传统经济思维到计算思维[4]的转变，加深对新的经济形态如：虚拟经济、平台经济、数字经济、共享经济的理解. 这种思维的转变会促进赛博经济的发展，给经济发展带来新的机遇. 人类的几次工业革命让生产力得到大幅提升，生产力提升的背后支撑是人类从机械的、拥有特定模式的劳动中解放出来，充分利用机器、计算机的优势来弥补人类自身的劣势，使人与机器的组合达到1+1＞2的效果. 赛博时代计算思维必不可少. 计算思维指的是利用计算机科学的概念进行求解问题、设计系统和理解人类行为. 它涵盖了整个计

算机科学的一系列思维活动. 计算思维通过将现实问题通过抽象、简约、嵌入、转化、仿真等一些列方法转化成计算机可以处理的问题，是一种递归思维. 赛博新经济形式下，计算思维应该是一种交叉思维，它将计算机科学与经济学相结合，将经济学的问题转化为计算机可以仿真、试验、解决的问题，或者转化为可利用计算机科学中现有的强大工具进行分析的问题，进而为解决问题提供新思路. 如图2中展示的那样，市场竞争中的一些规律在网络科学中也是有所体现的，而网络科学中的研究成果也可以为解决市场中的问题提供借鉴. 这种交叉思维在新经济形势下尤为重要，经济全球化大势下，世界各国经济犹如逆水行舟，不进则退.

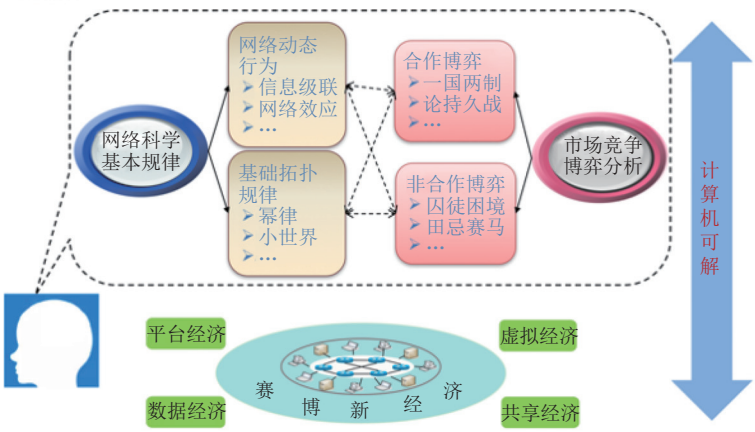

图 2　赛博时代的网络与经济

Fig.2　Internet and economy of the cyber era

1.2　社会的信任

诺贝尔经济学奖得主肯尼斯·约瑟夫·阿罗认为信任是经济交换的润滑剂. 信任是经济和社会系统得以正常运行的基石，越是发达的社会，人与人之间的信任程度越高.

1.2.1　信任塑造经济社会

日裔美籍学者福山在其著作《信任：社会道德与繁荣的创造》[5]一书中深入分析了社会信任程度及其范围对经济的组织形态、运行效率以及产业结构乃至国家竞争力的重大意义. 福山分析了低信任度地区和高信任度地区的企业的发展状况. 在其研究中，低信任度地区主要包括华人社会（包括中国大陆、台湾地区、香港地区）、法国、韩国、意大利. 这些国家和地区中的宗教或传统文化推崇家族主义，直接导致了人与人之间的信任被限制在家族甚至家庭范围内. 低信任度带来的一个后果就是在经济发展过程中，这些地区出现的大量小型家族企业由于社会的低信任度难以迈入现代化大型企业阶段. 排斥外人经营以及家族的财产均分继承制度导致家族企业富不过三代. 低信任度还迫使政府不得不干预以确保那些在国家竞争中处于重要地位的资金、技术密集型产业得以发展，而此过程则带来了资源的浪费与效率的损失. 在以日本、德国为代表的高信任度国家则以血缘关系的社团为基础构建信任体系，在其历史和文化上，相对较少的中央集权、较弱的家族力量加之相对强大的社会连署关系，促使人们将信任扩大至家族之外. 高信任度国家和地区的企业往往可以更加顺利地从小型家族企业转变为大型的现代化企业，这些大型企业之间还可以通过道德互惠或者互助的形式合作解决问题以及创造更大的价值. 相反，在低信任度社会中，为了堵住各种可能的漏洞，企业需要经常求助于法律或者制定冗长的契约来增加自身的安全感，这些都提高了交易的成本，结果就是全社会需要为之买单.

1.2.2　去中心的信任系统

无论是银行还是第三方支付平台，它们都是依赖中心化处理的机构. 中心化的处理模式成本可控、效率高，但是一旦中心结点出了问题，那么整个系统的可靠性都会受到影响. 中心化解决方案的这些问题促使人们去寻找一种新的不依赖于中心结点的分布式方案.

次贷危机之后，“比特币”诞生了，它率先被人们所知的是其电子加密货币的身份. 不久之后，它的底层技术区块链被挖掘出来，其影响远超比特币本身. 区块链利用去中心化的共识机制，构建了一个不依赖于中心化结点的、独立于任何国家、组织、企业的

系统. 它由全世界所有的运行该系统的结点共同维护，一旦出现错误、欺骗等不合理或违规行为，便会被系统中的结点检测出来. 一笔交易只有得到了一半以上（从总的哈希计算能力来讲）的比特币结点的认可才会被系统接受，单个、少量结点的欺骗或者失效不会影响到整个系统运行. 区块链的诞生为赛博新经济注入了新的血液，有望成为赛博新经济的信任基础设施，加速它向赛博智能经济的转变.

2 区块链的前世、今生与未来

区块链不是一个全新的技术，它所利用的技术都是已有的、相对成熟的技术，如：P2P、密码学、分布式共识等. 比特币为人们熟知之后，区块链很快被人们挖掘出来，并且针对不同的场景，派生出大量变体. 虽然区块链为解决信任问题提供了一个全新的思路，但是其本身依然存在着许多问题，比如：性能、隐私保护等等.

2.1 P2P技术与共识机制

2.1.1 P2P网络

P2P(peer-to-peer)是一种能够让计算机不通过中心化的设备就能够进行通信、资源和服务共享的分布式技术. 在P2P网络中所有结点都是对等的，结点间通过相互通信、协作来达到资源共享的目的[6].

P2P的发展经历了3个阶段. 第一代P2P系统以Napster为代表，它采用集中索引的方式来处理网络资源的共识问题. 本质上它还是一个C/S架构，整个P2P网络的性能受到了中心服务器结点的限制. 第二代P2P系统以KaZaA、Gnutella为代表，采用完全无中心的结构，所有的查询和响应都在分布式的P2P结点间完成. 用户拥有的资源以广播的方式发送给网络上的其他结点，容错性强. 第二代P2P系统解决了第一代系统中服务器结点的性能瓶颈问题，却引入了广播流量问题，这就给资源共享带来了时间、空间上的限制，同时它也无法避免中间结点对信息的恶意篡改. 第三代P2P系统以Chord[7]、CAN[8]等为代表，利用分布式哈希表技术，同时具备前两代P2P结构的优点，利用位于主干位置的多个超级结点来维护网络资源的共识. 不幸的是第三代的P2P网络仍然要求节点是可信的，如果有一个结点传播错误信息，整个网络的资源就无法达成共识.

EigenTrust[9]通过在P2P网络中引入信誉管理机制，让网络中的结点可以选择从它们信任的结点获取数据，而且该信誉管理机制使网络可以自动识别恶意结点并将其隔离出去. EigenTrust可以减少网络中不可靠文件的数量，但仍无法完全避免恶意文件的存在和传播. P2P网络的局限性使其只能被应用到一些不需要太多信任的场景下，比如说音乐、电影的分享等，而像一些需要高度安全、可靠的场景，如：电子支付无法从中获益.

2.1.2 拜占庭将军问题

拜占庭将军问题由图灵奖获得者LesileLamport[10]于1982年提出，目的是为了解决如何在一个互不信任的分布式群体中达成共识的难题. Lamport在其论文[10]中描述了拜占庭将军问题：几个拜占庭将军率领军队围住了一座城市，将军们之间只能通过通信兵联络，在观察过敌人的城池之后，他们必须决定攻击或者撤退. 其中的问题是一部分将军可能是叛徒，他们会阻止其他将军们达成共识.

共识算法必须保证：1) 所有忠诚将军们的决定必须一致；2) 少量的叛徒不能让忠诚的将军们达成一个坏的共识. 拜占庭将军问题是容错性问题中最难的问题之一. Lamport在论文中指出在同步环境下，叛徒个数小于将军总数的1/3时，将军们可以达成共识. 如果同步通信是可认证防篡改的，任意多叛徒都存在解决方案；在异步通信环境中，只要有一个叛徒存在，拜占庭将军问题就是无解的. 2014年，清华大学王君行[11]提出了一种简单的拜占庭容错协议，利用简单的循环代替复杂的递归，简化了算法. 在Lamport之前，Pease[12]也提出过一个解决方案，他们的共同的特点就是都使用了递归算法，较为复杂. Barbara Jane Huberman于1999年在其论文[13]中第一次提出了一种实用的解决拜占庭将军问题的协议PBFT[13]，减小了共识算法的复杂度，改善了性能. 继PBFT之后，又有许多拜占庭容错协议（BFT）协议被提出来，如用于提升效率的Q/U[3]，HQ[14]，Zyzzyva[15]，ABsTRACTs[16]，用于加强健壮性的Aardvark[17]和RBFT[18]，以及其他一些改善PBFT的论文，如：A2M-PBFT-EA[19]、MinBFT[20]、Adapt[21]等.

网络容错技术的发展和拜占庭将军协议的不断改进解决了信息共识问题，也就解决了如何在P2P网络中进行可靠通信的问题. P2P技术和网络容错技术的发展为区块链的出现奠定了基础.

2.2 区块链——信任的基础设施

2008年11月，中本聪关于比特币的白皮书[22]发表，比特币开始进入人们的视野. 对于电子加密货币人们早有研究，但直到比特币的诞生才真正出现了一个为大众熟知、被许多人接受的加密货币. 比特币是一个去中心化的加密货币，它不依赖于单个结点

或服务器来运行，全球任意一台计算机都可以运行比特币的客户端，加入比特币的网络，为其作贡献. 人们对比特币的信任来自于3个方面：1) 密码学；2) 去中心化；3) 基于PoW(Proof-of-Work)的共识机制. 密码学中的SHA256和椭圆曲线[23]加密技术是比特币安全性的基础. 密码学技术确保在比特币系统中未知他人密钥的情况下无法盗取比特币，并且可以防止双花（double-spend）问题. 去中心化是比特币获取信任的前提. 正是因为比特币结点不依赖于网络中的任何单个服务器，它的可靠性才得以保证. 而共识机制是比特币作为加密货币的先决条件，没有共识就没有比特币. 共识包括两方面：一方面是数据的共识，另一方面是对比特币的价值达成共识.

2.2.1　区块链的基本结构

比特币是一种电子加密货币，区块链最初就是为了存放比特币交易信息的，是一种为存放交易数据而设计的数据结构. 区块链可以从区块和链两方面来了解，其基本结构如图3所示.

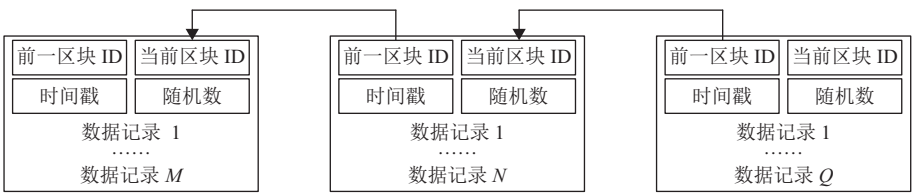

图 3　区块链基本结构

Fig.3　Basic structure of blockchain

区块中包含头部和交易实体数据. 头部中包含了当前区块的哈希值以确保区块的完整性. 链将区块以特定的顺序连接起来，区块头部中包含了一个作用类似指针的字段，这个字段中存储了前一个区块的哈希值. 区块的实体中包含了许多交易，这些交易逻辑上以默克尔树[24]的形式来组织，结构如图4所示.

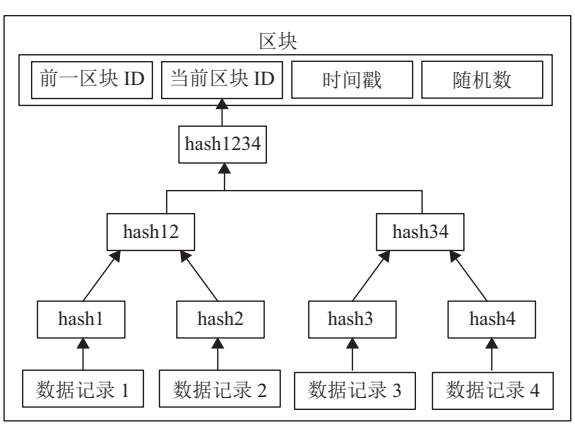

图 4　比特币区块基本结构

Fig.4　Block structure of Bitcoin

默克尔树是一棵二叉树，叶子结点是每个交易的哈希值. 每个父结点的值为两个子结点组合起来所计算得到的哈希值. 最终的默克尔树的根哈希会被记录到区块的头部中去. 通过默克尔树这种数据结构，在添加一笔新的交易时，无须遍历整个交易记录以更新根哈希，只需要以复杂度log(n)更新一次每一层的哈希. 同时，默克尔树的可以保证任意交易数据被篡改了，默克尔树的根哈希一定会改变，否则区块无法被验证通过.

数据的完整性通过哈希算法来保证，而共识协议则依赖于工作量证明(PoW)算法. 区块的头部中包含一个32位的nonce字段，比特币网络中的结点（矿工）通过改变这个32位的整数以计算出不同的哈希值（256比特的整数），在哈希值小于一个特定的值target（256比特的整数）时，区块被认为是有效的. 由于哈希值的随机性，如果target值非常小，找到一个有效的区块会非常困难. 区块产生后向全网广播，其他矿工在收到并且验证区块的有效性之后，在这个新的区块上继续寻找下一个区块. Nonce字段只有32位，而正常情况下target值却非常小，即使使用普通的PC也可以很快将这32位的整数遍历一遍却无法发现有效的区块. 区块中还有其他数据可以改变区块的哈希值——交易. 显然，不同数量或者同样一组交易但顺序不同产生的哈希值也不同. 此外，每个区块的交易中可以包含一个非常特殊类型的交易——coinbase交易，比特币就由此产生. 每个coinbase交易输出一定数量的比特币，作为对矿工的奖励. 由于coinbase交易无需输入（交易有输入和输出），它的输入字段可以写入任意数据，这是改变区块哈希值的一个非常便利的途径. Target的值是随着区块链全网的计算能力而改变的，网络中的结点根据区块的产生时间动态调整target值，使整个网络维持在每

10 min产生一个区块.

区块的主体部分由交易组成,交易中主要内容是交易的输入和输出. 交易的输入指明交易金额的来源,交易的输出指明交易金额的去向. 输入输出的个数可以是多对多的,其中使用最多的是1对2,即一个输入两个输出,类似于用100元纸币去买了80元商品,找零20元,这里输入就是100元,输出就是80元和20元. 交易的输入中包含了发送者的签名,交易的输出中包含了接收者的地址(哈希值,比如用户公钥的哈希). 交易过程如图5所示.

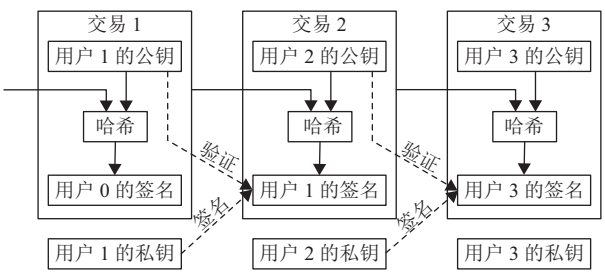

图 5 比特币中的交易

Fig.5 Transaction in Bitcoin network

交易有效性的验证是通过脚本进行的,比特币区块链的脚本是一种基于栈的简单脚本,它并不是图灵完备的,支持的脚本命令很有限. 输入和输出中都包含了脚本片段,将这两段脚本连接在一起就组成一个完整的脚本,执行此脚本即可验证交易的有效性.

2.2.2 区块链的共识协议

比特币区块链以一种极其巧妙的方式给出了一种拜占庭将军问题的解决方案. 比特币网络中的节点在挖到一个区块后,就会向全网广播,比特币协议规定了工作量最大的链(一般为最长链)为主链,只有主链才会被认可. 由于网络传播存在延迟,如果在传播过程中,另一个结点也挖到了一个区块,这样网络中的结点就会收到不同的区块,并且基于不同的区块寻找下一个区块,这就会产生分叉,如图6所示.

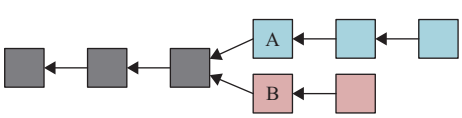

图 6 区块链分叉

Fig.6 Forks in blockchain

在同一区块之后产生了两个区块A、B,此时结点的做法是选择在它们最先接收到的区块之后挖矿,直到其中一条支链的长度超过另外一条转变为主链. 可以证明,出现长度为N的支链的概率是随着N的增加指数递减的. 长度为1的支链在区块链网络中较为常见,但长度为2的支链在区块链诞生后几乎没有出现过. 由此可以看出区块链的高可靠性. 经过测量[25],一个新的区块大约需要经过40 s之后才能被全网90%的结点接收,在区块的传播过程中大概会产生1.69%的孤块(就是被抛弃分支上的区块). 这意味着全网大概有1.69%的算力被浪费了,算力的浪费会降低区块链的安全性和可靠性. 区块链网络的延迟主要是由两方面引起的:一方面是网络本身的延迟. 无论是区块链还是传统的网络,数据在其上传播都会产生延迟,这些延迟包括:传输时延、传播时延、处理时延、排队时延等等,时延的大小还与收发双方的网络带宽有关;另外一方面是区块有效性验证的时间. 为了防止恶意的攻击,结点在收到新的区块之后并不是立即告知其他结点,而是先要验证区块的有效性. 它包含两方面:(1) 区块头部的验证;(2) 区块所包含所有交易的验证. 在区块链诞生之初,区块链自身的体积(所占用的物理磁盘空间)还不大,交易量还很小,每个区块中最多包含几十或者上百的交易(2011~2013年),验证交易的时间消耗较小. 但是随着区块链的体积不断增大,UTXO(未花费交易输出即用户余额)越来越多,这样搜寻交易的输入所需的时间越来越大. 同时,每个区块包含的交易数量越来越大,至2017年末,每个区块包含的平均交易量已经超过了2 000笔,这样验证的时延就增加了. 区块传播路径上的每一跳都会进行有效性验证,这进一步扩大了时延.

区块链的共识并不是全网大部分结点的共识,这可以从两方面来讲. (1) 共识是通过哈希计算能力来保证的而不是结点的数量. 全网只有对某一区块认可结点所拥有的计算能力超过了50%,网络才可能达成一致. (2) 打破公平性远不需要拥有50%以上的计算能力. Ittay Eyal等[26]的研究指出只要拥有超过1/3的算力,采用他们论文中提出的自私挖矿(selfish mining)的策略,就可以获得超过其所占算力比重的奖励.

比特币的共识协议是基于PoW的,之后,又出现了其他机制如:PoS (proof of stake / proof of storage), PoR (proof of retrievability), PoB (proof of burn)等等,并且随之出现了很多其他加密货币.

2.2.3 区块链的特点

首先区块链是去中心化的,网络中的结点的权利是对等的,这是区块链成功的前提. 密码学技术给区块链带来了安全性. 如果区块链底层的密码学技

术被攻破，那么现有的基于SHA256或者椭圆曲线算法的应用都将失去安全性. 身份对等和安全性带来的是信任. 只要产生交易就必然伴随着信任，区块链的出现将这种信任由对交易双方的信任或者第三方的信任转移到了区块链技术本身，区块链成功运行9年之久也一定程度上证明了其可信性.

区块链的另一个重要特征就是匿名性，也有人称伪匿名. 之所以被称为伪匿名，是因为通过一定的方法有一定的概率可以追踪交易的来源. 理论研究[27]虽然说明比特币可以通过一定的方法溯源，但是这些手段在实际中应用的准确率并不能保证，并且这些溯源手段都可以通过一定的方法来规避. 在实际应用中，伪匿名性带来的问题并不大.

此外，在加密货币的应用上，区块链也给电子货币带来了传统法币所不具备的特点. 传统交易需要使用政府发行的货币，那就必须要相信政府，可是印刷货币的成本可以忽略不计，而大量印刷货币就会造成通货膨胀. 传统的硬通货黄金的储量也是有限的，但其一，个人无法私自采矿；其二，地球上黄金虽然有限，但总量也是巨大的. 而比特币的挖矿任何人都可以参与，并且它的发行量有限（2 100万个），减少了通货膨胀的风险.

2.3　区块链的前景与挑战

比特币为全世界提供了一种不依赖于第三方的转账的手段；以太坊将图灵机从线下搬到了线上，智能合约在区块链的帮助下真正开始进入人们的视野；The DAO（分布式自治组织）项目借助以太坊成为第一个完全去中心化的风险投资基金，为去中心化组织的管理探索了一条新的道路；IBM的超级账本为高性能、可扩展区块链积极探索着新的方案. 近年来，包括美国、日本、韩国、法国、俄罗斯等国政府纷纷表示支持区块链的创新，放宽加密货币的政策.

区块链的应用早已不再局限于加密货币，而正在逐渐成为信任的基础设施. 可以想象不久的将来，个人的信用将与区块链不可分离；重要数据的可靠性、安全性、隐私保护将借助区块链来实现；人与人之间可以自由转账而无需担心安全问题；产品的质量可以借助区块链来保证；企业之间的合同执行都在线上进行，大大减少了人力物力. 所有这些都在逐步成为现实.

如何构建一个在性能、安全性、可靠性、隐私保护、可监管方面都表现都优秀的区块链，如何打造一个良好的区块链发展的生态，如何将现有的区块链技术服务于赛博新经济，如何发展赛博智能经济，这些仍然是开放的、等待解决的问题.

区块链的性能一直为人们所诟病. 比特币区块链每秒可处理的交易量在十这个数量级，以太坊在百数量级. 超级账本项目在2016年初成立，该项目联合构建了一个开源的、企业级的分布式账本框架. 它旨在通过实现一个跨行业的、开放的、标准的分布式账本来转变全球商业交易的方式，以推动区块链的发展. Fabric[28]是超级账本的核心项目，它的性能虽然比比特币、以太坊等要好，但是是以联盟链或授权链（不再是完全分布式的，链在一定范围内达成共识）为代价的.

在安全性方面，虽然区块链本身的安全漏洞较为罕见，但是在实际的应用中，却会出现各种各样的问题，如MtGox事件、the DAO事件、Poloniex比特币被盗事件等. 这些问题有的是由于中心化造成的，有的是由于智能合约代码的漏洞造成的. 这就类似于加密算法本身的漏洞十分罕见，但是实际应用中却经常出现问题，系统被黑客攻陷一样. 这个问题将会伴随着区块链甚至互联网的存在而一直存在.

区块链的可靠性较高. 以基于PoW算法的比特币区块链为例，只有拥有超过全网50%的算力才可以操纵比特币区块链. 鉴于目前比特币区块链全网的哈希计算力非常之大，截止2018年1月21日比特币的哈希计算能力已经接近2^{63} 次/秒. 如果这些算力都被用于寻找SHA1的碰撞（生日攻击[29]），那么三四天就可以找到了，由此可见比特币挖矿的算力有多么强大. 正因为如此，要想控制全网超过50%的算力非常困难. 另一方面，如果有人控制了超过50%的算力，比特币的安全性、可靠性将面临巨大威胁，这就意味着比特币可能变得一文不值，这将对控制着比特币50%以上算力的攻击者造成巨大的经济损失. 这也是区块链可以发展的重要原因. 现有的基于区块链的加密货币基本上都是基于理性经济人模型的，一旦这个条件不成立，区块链的可信性将面临巨大挑战.

区块链上的隐私问题正在不断被新的方案解决. 现在已经出现了一些带有隐私保护特性的加密货币，如：Zerocoin[30]、Zerocash[31]、Monero、Dash等等. 比特币使用得当在很大程度上已经可以保护用户的隐私，而之后的的加密货币使用密码学中的零知识证明、环签名等技术以及匿名的P2P网路等等手段进一步加强了隐私保护.

但我们也必须看到，隐私保护带来的另一个问

题就是难以监管. 由于区块链上的交易是点对点的交易，加上匿名性，区块链几乎是黑市交易的最佳工具. 典型的例子是专门用于进行毒品等违禁物品交易的网络平台Silkroad、Agora等等，它们都支持比特币交易. 加密货币的匿名性一方面可以隐藏罪犯的身份，另一方面，在犯罪分子被抓之后，这些非法盈利所得的资金也很难追回. 如何在不丢失区块链保护隐私的优点的情况下，进行有效监管仍然有待探索.

3 赛博智能经济与区块链

近年来，智能家居、智能交通、智慧城市等概念不断传入人们耳中，万物互联正在从一个虚构的蓝图逐渐变为现实. 万物互联带来信息爆炸式增长的同时，网络安全问题也日益严峻，限制着网络的发展. 区块链的出现有望解决这一问题. 它作为一个可信的基础设施，在其上可以搭建智能合约系统，从而可以运行各种各样安全、可靠的应用，不但可以保护用户数据的隐私、完整性等，还可以简化各种流程，降低成本. 智能合约在20世纪90年代[32]就已经有人提出，但是苦于没有一个安全、可信的执行环境，一直发展缓慢. 直到区块链产生后，智能合约才再次火热起来.

赛博经济将在智能合约的推动之下进入赛博智能经济时代. 在智能经济时代，人们可以通过设计特定规则的智能合约，让物与物之间可以直接进行安全、可靠交易. 这将进一步加快资金的流动、推动信息的增长，最终使经济更加快速的增长.

从传统经济到赛博经济，经济系统中的各个组成部分不断升级，形成了新的生产、交换、消费、金融子系统. 这些子系统有序运行的基础是8类算法[2]：推荐、分配、匹配、动态定价、区块链、大数据处理、数据交易、隐私保护算法，其结构如图7所示. 区块链作为这8类算法中的一员，它的位置与其他7类又有所不同，它有可能发展成为算法层与数据层之间的一个子层，以保障算法所获取数据的可靠性. 杂乱无章的信息不能创造任何价值，从信息到价值，区块链可以作为保障，而算法在这个过程中起到的是桥梁的作用. 一方面，信息的增长不断加快，这种增长不是无序的，它在算法的指导下有序地运行着. 另一方面，算法可以从看似杂乱无章的数据中，提取有用的信息. 算法这只“看不见的手”将在赛博新经济、赛博智能经济系统中推动信息有序增长、保障经济系统运行、促进经济系统不断创新变革，从而推动经济不断快速、持续增长.

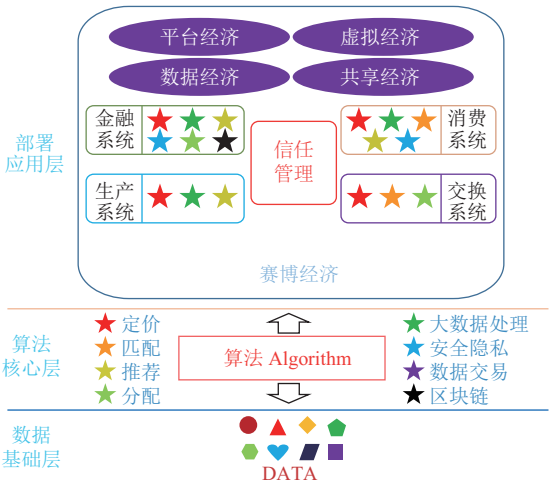

图7 算法支撑下的赛博经济结构

Fig.7 Architecture of the cyber-economy supported by algorithms

参考文献：

[1] 徐恪, 王勇, 李沁. 赛博新经济[M].北京: 清华大学出版社,2016:1-49

[2] 徐恪, 李沁. 算法统治世界[M].北京: 清华大学出版社, 2017:324-339.

[3] ABDELMALEK M, GANGER G R, GOODSON G R, *et al*. Fault-scalable Byzantine fault-tolerant services [C]//Twenti-eth ACM Symposium on Operating Systems Principles. Brighton: ACM, 2005: 59-74.

[4] WING J M. Computational thinking [J]. Acm Sigcse Bullet-in, 2006, 49(3): 3-3.

[5] 弗兰西斯·福山. 信任:社会道德与繁荣的创造[M].桂林: 广西师范大学出版社, 1998.

[6] 徐恪, 徐明伟. 高级计算机网络[M].北京: 清华大学出版社, 2012: 354-384.

[7] STOICA I, MORRIS R, KARGER D, *et al*. Chord: A scal-able peer-to-peer lookup service for internet applications [C]//Conference on Applications, Technologies, Architec-tures, and Protocols for Computer Communications. San Diego: ACM, 2001: 149-160.

[8] RATNASAMY S, FRANCIS P, HANDLEY M, *et al*. A scalable content-addressable network[C]//Conference on Ap-plications, Technologies, Architectures, and Protocols for Computer Communications. San Diego: ACM, 2001: 161-172.

[9] KAMVAR S D, SCHLOSSER M T, GARCIA-MOLINA H. The Eigentrust algorithm for reputation management in P2P networks[C]//International Conference on World Wide Web. Budapest: ACM, 2003:640-651.

[10] LAMPORT, LESLIE, SHOSTAK, *et al*. The Byzantine gen-erals problem [J]. Acm Transactions on Programming Lan-

guages & Systems, 1982, 4(3): 382-401.

[11] WANG J. A simple Byzantine generals protocol [J]. Journal of Combinatorial Optimization, 2014, 27(3): 541-544.

[12] PEASE M. Reaching agreement in the presence of faults [J]. Journal of the Acm, 1980, 27(2): 228-234.

[13] CASTRO M. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transaction on Computer Systems, 2002, 20(4): 398-461.

[14] COWLING J, MYERS D, LISKOV B, *et al*. HQ replication: a hybrid quorum protocol for byzantine fault tolerance [C]//OSDI'06 Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation. Seattle: USENIX Association, 2006: 13.

[15] KOTLA R, ALVISI L, DAHLIN M, *et al*. Zyzzyva: speculative Byzantine fault tolerance[C]//ACM Sigops Symposium on Operating Systems Principles. Stevenson: ACM, 2007: 45-58.

[16] GUERRAOUI R. The next 700 BFT protocols[C].//International Conference on Principles of Distributed Systems. Heidelberg: Springer, 2010: 363-376.

[17] CLEMENT A, WONG E, ALVISI L, *et al*. Making Byzantine fault tolerant systems tolerate Byzantine faults[C]//Usenix Symposium on Networked Systems Design and Implementation, NSDI 2009. Boston: DBLP, 2009: 153-168.

[18] AUBLIN P L, MOKHTAR S B. RBFT: redundant Byzantine fault tolerance[C]//2013 IEEE 33rd International Conference on Distributed Computing Systems. Philadelphia: IEEE Computer Society, 2013: 297-306.

[19] CHUN B G, MANIATIS P, SHENKER S, *et al*. Attested append-only memory: making adversaries stick to their word[C]//Stevenson: ACM, 2007: 189-204.

[20] VERONESE G S, CORREIA M, BESSANI A N, *et al*. Efficient Byzantine fault-tolerance [J]. IEEE Transactions on Computers, 2013, 62(1): 16-30.

[21] BAHSOUN J P, GUERRAOUI R, SHOKER A. Making BFT protocols really adaptive[C]//Parallel and Distributed Processing Symposium.Hyderabad: IEEE, 2015: 904-913.

[22] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[M].[S.l.]: Consulted, 2008.

[23] KOBLITZ N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209.

[24] MERKLE R C. A digital signature based on a conventional encryption function[J]. Th Conference on Advances in Cryptology, 1987,293(1): 369-378.

[25] DECKER C, WATTENHOFER R. Information propagation in the Bitcoin network[C]//2013 IEEE International Conference on Peer-To-Peer Computing. Trento: IEEE, 2013: 1-10.

[26] EYAL I, SIRER E G. Majority is not enough: Bitcoin mining is vulnerable[C]//International Conference on Financial Cryptography and Data Security. Heidelberg: Springer, 2014, 8437: 436-454.

[27] ANDROULAKI E, KARAME G O, ROESCHLIN M, *et al*. Evaluating user privacy in Bitcoin[C]//International Conference on Financial Cryptography and Data Security. Heidelberg: Springer, 2013: 34-51.

[28] CACHIN, C. Architecture of the Hyperledgerblockchain fabric[C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers(DCCL). Chicago:[s.n.], 2016.

[29] BELLARE M, KOHNO T. Hash function balance and its impact on birthday attacks [J]. Lecture Notes in Computer Science, 2004, 3027: 401-418.

[30] MIERS I, GARMAN C, GREEN M, *et al*. Zerocoin: anonymous distributed E-Cash from Bitcoin[C]// 2013 IEEE Symposium on Security & Privacy. Berkeley: IEEE, 2013:397-411.

[31] SZABO N. Formalizing and securing relationships on public networks[J/OL]. First Monday, 1997, 2(9)[2017-12-18] . http://firstmonday.org/ojs/index.php/fm/article/view/548/469.DOI: http://dx.doi.org/10.5210/fm.v2i9.548

[32] SASSON E B, CHIESA A, GARMAN C, *et al*. Zerocash: decentralized anonymous payments from Bitcoin[C]// 2014 IEEE Symposium on Security and Privacy. San Jose: IEEE, 2014: 459-474.