区块链技术对人工智能的影响

潘吉飞 黄德才
(浙江工业大学计算机科学与技术学院 杭州 310023)

摘 要 区块链是比特币的支撑技术,具有去中心化、不可篡改、可追溯的特点,在金融、数字版权、公证、物联网、文档存储等领域开始逐步应用并取得了较大成果,已成为与人工智能、大数据、云计算等比肩的热门技术。人工智能建立在海量数据和强大计算力的基础上,区块链技术的特点可以很好地融入到人工智能应用中,从而推动人工智能的进一步发展。文中在介绍了区块链基本概念与工作机制的基础上,重点介绍区块链技术的发展对人工智能的影响,分析了区块链技术应用于人工智能领域的可行性,最后提出展望。

关键词 区块链,比特币,挖矿,AI,Atmatrix
中图法分类号 TP315 **文献标识码** A

Impact of Blockchain Technology on AI

PAN Ji-fei HUANG De-cai
(College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract Blockchain is the technology behind Bitcoin, with the characteristics of decentralization, non-tampering and retrospective. Blockchain has been gradually applied in financial, digital rights, notarization, networking, document storage and other fields, and obtained great achievements. Blackchain has become a more and more popular research area like AI (Artificial Intelligence), Big Data and Cloud Computing. AI bases on massive datasets and powerful computing ability, and Blockchain can be well integrated into AI to promote it's rapid development. On the basis of introducing the concept and working mechanism of Blockchain, this paper mainly introduced the influence of Blockchain technology on AI, analyzed the application feasibility of Blockchain in AI, and finally put forward the prospect.

Keywords Blockchain, Bitcoin, Hyperledger, AI, Atmatrix

1 引言

区块链(Blockchain)[1-2]和人工智能(Artificial Intelligence,AI)是当今全球范围内的两大技术前沿热点。两者作为目前金融科技 Fintech 的最热门话题,已经引发了无数投资者的关注。

图 1 显示的是百度指数对于"区块链"和"人工智能"两个关键词在 7 月 21 日—10 月 18 日的搜索统计。从趋势上看,数据变化基本保持同步,体现出了两者紧密的联系。

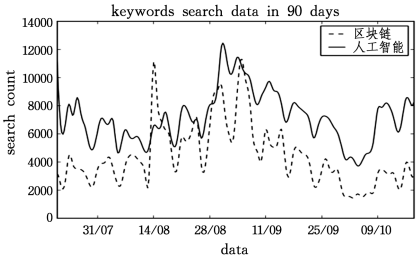

图 1 "人工智能"与"区块链"的搜索对比

"人工智能"一词在 1956 年美国达特茅斯(Dartmouth)大学召开的学术会议上提出,被认定为全球人工智能研究的起点。人工智能引爆全球、深入人心的事件是 2016 年 3 月 AlphaGo 4:1 战胜世界围棋冠军李世石[3]。2017 年 10 月 19 日,DeepMind 发布新版本 AlphaGo 程序,经过 3 天的训练,成功击败 AlphaGo Lee,经过 40 天的训练,AlphaGo Zero 完胜 AlphaGo Master。如今,机器学习、深度学习等人工智能相关技术遍地开花,各行各业都纷纷加入进来。智能机器人[4]等人工智能产品的出现,已经极大地解放了劳动力,为生活带来了极大的便利。

相比于人工智能,区块链是一门比较年轻的技术。区块链起源于数字加密学,虽然数字加密学的研究以及应用由来已久——早在 1983 年 David Chaum 就首次把加密技术运用在数字货币上,但是大众广泛了解和接触到区块链是因为比特币的出现。

1991 年,Haber 和 Stornetta 提出了区块链的概念并将其运用在时间戳上[6]。2008 年,比特币白皮书[5]发布,描述了基于比特币的虚拟货币系统,其底层技术就是区块链技术。比特币的出现,极大地推动了区块链的发展,至今比特币依然是区块链最大的应用项目。随着以太坊等一系列基于区块链技术项目的诞生,区块链技术逐渐火热起来,应用领域进一步拓宽,发展潜力巨大。

2 区块链的概念和相关术语

2.1 区块链的定义

区块链技术正处于飞速发展阶段,业界目前暂无统一的

本文受水利部公益性行业科研专项基金(201401044)资助。

潘吉飞(1993—),男,硕士生,主要研究方向为数据挖掘、人工智能,E-mail:2809956575@qq.com;黄德才(1958—),男,博士,教授,博士生导师,主要研究方向为数据挖掘、人工智能等,E-mail:hdc@zjut.edu.cn(通信作者)。

标准，引用 Wikipedia 给出的定义[7]：区块链本质是一个不断增长的使用加密技术进行链接和保护的记录列表。记录的单元称为块，每个块包含哈希指针（作为前一个块的链接）、时间戳和事务数据。区块链具有天生抵抗数据篡改的特性，可以作为一个开放的分布式帐本，能够有效地永久记录双方之间的交易，所有交易记录都可追溯、可验证。

对于区块链，可以简单地将其看作是一套协议、一组规范，而不是具体的代码或项目。基于这套协议，可以利用现有的编程语言开发各类去中心化产品，并将产品应用在金融、物联网、供应链等领域。表 1 列出了区块链当下的应用生态。

表 1 区块链应用生态

行业	具体应用
金融	支付（跨境支付）保险、证券 股权登记、众筹
互联网	区块链物联、租赁
供应链	供应链金融、供应链追溯
公益慈善	区块链捐赠平台
公共服务	文化、教育、产权、医疗

2.2 区块链的工作原理

区块链是一个个区块连接在一起形成的链条。数据通过区块（block）的文件，永久记录在区块链网络上，新的区块追加到区块链末端。区块的结构如表 2 所列。

表 2 区块的结构

字段	大小	描述
区块大小	4 bytes	表示该字段后区块的大小
区块头	80 bytes	组成区块头的几个字段
交易计数器	1～9 bytes	交易的计数
交易	可变	记录交易信息

区块头由 3 组区块元数据组成：一组引用父区块哈希值，将本区块与前一区块相连接；一组包含挖矿竞争相关的数据，即难度、时间戳和随机数；最后一组是 merkle 树根数据，是一种用来有效地总结区块中所有交易的树形结构[8]。区块头结构如表 3 所列。

表 3 区块头结构

字段	大小	描述
版本	4 bytes	用于软件/协议的更新
父哈希值	32 bytes	引用父区块哈希值
难度目标	4 bytes	区块 PoW 算法的难度
时间戳	4 bytes	区块产生的时间
nonce	4 bytes	PoW 算法的计数器
merkle 根	32 bytes	区块 merkle 树根的哈希

以比特币为例来具体解释区块链的工作流程：客户端发起一项交易后，会广播到网络中并等待确认；网络中的节点会将一些等待确认的交易记录打包在一起（此外还要包括此前区块的哈希值等信息），组成一个候选区块；随机产生 nonce 串放到区块里，使得候选区块的 hash 计算结果满足给定条件，一旦条件满足，这个区块在格式上就被认定合法，可以进行全网广播；网络中的其他节点接收到提案区块后进行验证，若确实符合约定条件后就承认这个区块是一个合法的新区块，并将其添加到链上。

2.3 去中心化

首先解释什么是中心化。常见的 C/S（Client/Server）结构[9]中，1 个 Server 提供服务，n 个 Clients 调用服务，整个系统的可靠性和安全性主要依赖 Server，即所谓的中心化。中心化的弊端显而易见，如果服务提供方的机器宕机、被黑客攻击或数据被恶意篡改，将造成十分严重的后果。现有的分布式架构、异地多活容灾技术都不能完美地解决这些问题。

区块链使用 P2P 网络实现去中心化的目标，网络中每一个节点都是对等的，没有专门的 Server 和 Client，或者认为所有的节点都既是 Server 又是 Client。P2P 节点之间交互运作、协同处理：每个节点在对外提供服务的同时也使用网络中其他节点所提供的服务。P2P 网络具有可靠性、去中心化和开放性的特点。

如图 2 所示，去中心化的区块链架构主要分为 3 个层次：协议层、扩展层和应用层。

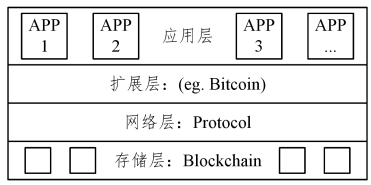

图 2 区块链去中心化的结构设计

协议层可细分为存储层和网络层，运用了数据存储技巧、密码学、分布式算法和网络协议等。

扩展层服务于不同类型的应用，起到适配器的作用。根据应用类型的不同，可以将扩展层分为两大类：一类是应用在智能合约的交易系统，针对各类数字代币，如比特币；另一类是应用在基于区块链技术的扩展应用中，如数字版权认证。

应用层就是各种用户终端应用，如各类电子钱包等手机或电脑软件。

区块链的协议层和扩展层使用加密算法和共识机制确保数据不被篡改、节点信息一致。即使在少数节点宕机的情况下，仍然不影响整个网络的运行。

2.4 共识机制

区块链技术为拜占庭问题[10]提供了新的解决方案。P2P 网络中有成千上万个节点，每个节点都保存了数据库的一个备份，协调和确保节点间的一致性。共识机制的本质是少数服从多数的原则[11]，即如果有 51%或以上的节点确认了某笔交易，那么这笔交易就是真实可靠的，其余节点需要同步这笔交易的信息并将其写入区块。如果要篡改某一区块信息，那么必须至少同时攻击 51%或以上的节点，其付出的代价必然是巨大的，虽然理论上可行，但实际上很难实现。

共识机制包括：PoW（Proof of Work 工作量证明机制）、PoS（Proof of Stack 股权证明机制）、DPoS（Delegated Proof of Stack 授权股权证明机制）等。表 4 对比了这 3 种共识机制。

表 4 3 种共识机制的对比

名称	优点	缺点	代表项目
PoW	自动调整机制；奖励机制吸引较多用户参与，节点网络扩展迅速	挖矿耗费大量电力；算力趋向集中；挖矿的积极性随奖励减少而减小带来的网络安全性能下降	比特币
PoS	相对节能；更加去中心化；避免后期紧缩	信用基础不够牢固	以太坊
DPoS	能耗更低；更加去中心化；更快的确认机制	采用投票方式选举委托的决策者，但大多情况下投票积极性不高；对坏节点的处理不够合理	比特股

2.5 加密算法

2.5.1 hash 算法

hash（哈希或散列）算法是信息安全领域非常基础也非常重要的技术，能将任意长度的二进制值明文映射为较短的固定长度的二进制值密文（hash 值），并且不同的明文很难映射为相同的 hash 值。针对字符串“Impact of Blockchain Technology on AI”，32 位 MD5 hash 值为“cf3b7e7625db4ff76fcee66484a1d58b”。

区块链节点在运算过程中广泛使用了 hash 算法。以计算地址为例：公钥经过一次 SHA256 计算，再进行一次 RIPEMD160 计算，得到一个公钥哈希（20 字节\160 比特），添加版本信息，再通过两次 SHA256 运算、取前 4 比特字节，加上哈希公钥加版本信息，再经过 base58 编码，最终得到地址。

2.5.2 对称和非对称加密

公钥私钥体系是现代加密算法的核心。公钥一般是对外公开的，人人都可获取；私钥一般自己持有，避免他人获取。加密过程中，通过加密算法和公钥，对明文进行加密，获得密文；解密过程中，通过解密算法和私钥，对密文进行解密，获得明文。根据公钥和私钥是否相同，加密算法可以分为对称加密算法和非对称加密算法，两种模式有各自的适用场景，可以单独使用，也可以组合使用。两者的对比详情如表 5 所列。

表 5　对称加密和非对称加密的对比

名称	优点	缺点	代表算法	适用场景
对称加密	加解密速度快；空间占用小；保密强度高	密钥容易泄露；密钥分发问题	DES 3DES AESIDEA	大量数据的加解密
非对称加密	公私钥分开，方便管理	加解密速度相对较慢	RSA EIGamal	签名和密钥协商

对称加密和非对称加密也可以组合起来使用：先通过计算复杂度高的非对称加密协商一个临时的对称加密密钥（会话密钥），然后双方再通过对称加密对传递的大量数据进行加解密处理。这种方式综合考虑了对称加密和非对称加密的优缺点，在实际项目中被广泛采用。

3 区块链推动人工智能的发展

人工智能是计算机科学的一个重要分支，是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术以及应用系统的一门新的技术科学。目前，人工智能已经在智能机器人、语音识别、图像识别、自然语言处理、专家系统等领域取得了巨大成就。

人工智能是一门基于数据的科学；区块链的本质是一种数据存储方式，或者叫作“超级账本”（超级账本项目 Hyperledger[12]），体现了数据智能[13]。两种技术都与数据息息相关，可以进行有效结合。区块链去中心化、不可更改等特性，以及共识算法、智能合约等机制，都可以被应用到人工智能中，从而推动人工智能更好地发展。

3.1 去中心化带来数据新范式

最初人工智能的研究方法大多基于固定大小的数据集，通过设计或改进某种算法来提高运算性能或者结果的准确度。

针对获取到的数据集 $X=\{x_1,x_2,x_3,\cdots,x_n\}$，按照一定的比例将其划分成训练样本 X_{train} 和测试样本 X_{test}，X_{train} 和 X_{test} 都是 X 的子集。如果通过训练样本建立的模型在测试样本上能得到很好的测试结果，那么这个模型就被认定是可用的。

2001 年，微软研究人员 Banko 和 Brill 发表了一篇论文[14]，指出大多数自然语言处理领域的工作基于小于 100 万字的数据集。针对这种规模较小的数据集，传统的经典算法，如朴素贝叶斯（Naive Bayes）和感知器（Perceptron）的算法，错误率为 25%，而最新研究出的基于记忆的算法（memory-based algorithms）实现了 19% 的错误率，如图 3 中最初的 4 个点所示。

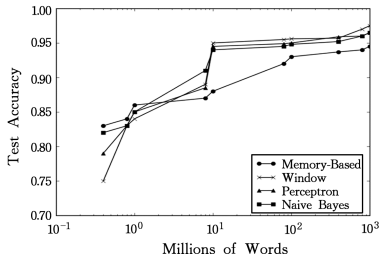

图 3　不同数据量下 4 种算法的效果对比

随着数据集的逐渐加大，所有方法的测试准确度会增大，且之前表现突出的 Memory-Based 算法开始落后于传统的、经典的算法。另一篇 2010 年 CoRR 的论文[15]则指出，如果给予较大规模的数据集，则来自 20 世纪 80 年代的反向传播神经网络甚至能与最新的方法抗衡。

如笔者在做关于糖尿病数据贝叶斯分类的实验中，当数据集为 700 多时，当预测的精确度只有 78%左右且当数据集增大一倍时，精确度上升到 85%；当数据增加到 5000 时，精确度达到 93%。

人工智能的关键不仅在于算法的先进性，更在于数据的质量和规模。有更好、更多的数据，才能建立更有效的模型来解决现实问题，这也是 Google、Facebook、阿里等数据巨头成为人工智能领跑者的关键。

然而数据在很多情况下都是独立的，尤其是大家开始重视数据的重要性后，数据壁垒成为人工智能新的阻碍。区块链技术为数据获取提供了更好的途径。去中心化/共享机制能够获取全球范围内更为健全、丰富的数据集，为人工智能带来了新的机遇[16]：

1）数据共享能够产生更好的模型；

2）数据共享能够诞生新的模型；

3）数据和模型可审计追踪，预测结果更加可靠；

4）可使用全球范围提供的数据集和训练模型；

5）将数据和模型作为 IP（知识产权）资产实现数据和模型交换。

3.2 共识机制培养更“友好”的人工智能

Elon Musk（特斯拉 CEO）认为未来最大的威胁，可能是人工智能的发展。毋庸置疑，人工智能促进了社会的发展，提升了的工作效率，然而，当机器通过大数据洞悉世间万物时，它不但可以识别、预测，更开始了创造：文本生成、语音生成（TTS）、图像和视频生成、二维图片 3D 建模等。会创造的人工智能让这个世界耳听不再为真，眼见不再为实，有图不再代表真相，视频也不再比图片有更强的说服力，因为极有可能是智能生成的。人工智能容易被不正当使用。

Musk 提出了几个关键问题：1）在实施人工智能时应该如何监管？2）如何规范和监督这项技术？一种有效的解决方案就是采用区块链技术。

智能合约是一套以程序形式定义的承诺(promises)协议,协议一旦制定好,将会自动执行,不受干扰。智能合约可以应用到人工智能的实施,避免了过程的监管。

共识机制通过群体投票确认、少数服从多数的原则对外提供一致的数据结果,这个过程需要每一个个体的参与,或者由个体选出代表代为参与(DPoS 共识机制)。可以基于这种机制创造一整套完善的规则体系,用于规范和制约人工智能的实施[18],促进参与人工智能的每一位成员成为具备合作精神、遵从既定规范的个体。

任何数字智能体在执行一些关键的网络操作任务时,包括安全访问、验证、交易等,需要一个多方一致的签名,签名的获得取决于智能体本身是否"友好"(安全评定、信誉评判等)。将信息存储在区块链上,进行"存在性证明(proof of existence)",能够去伪存真,确保证据的真实性和依据的权威性。

2016 年 12 月,Google 人工智能 DeepMind 医疗保健项目宣布采用区块链的技术,以增强基础设施的安全性和透明性。

3.3 挖矿设备为 AI 提供算力

区块链的 PoW(Proof of Work)共识机制和核心理念是"按劳取酬",通过为网络提供计算服务(算力 * 时长)获得报酬(如一定量的比特币)。这种机制发展到今天,算力的提供已经不再单纯依靠 CPU,而是发展到 GPU、FPGA、ASIC(专用型集成电路芯片)矿机和集群[19]。

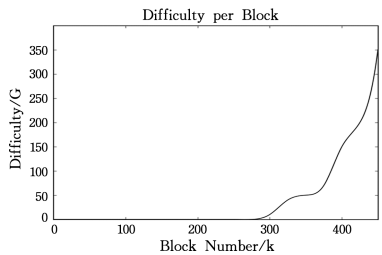

图 4 比特币挖矿难度的增长

如图 4 所示,从创世块到 260k 块,挖矿难度几乎没有增长,从 260k 块左右难度开始增加,380k 块左右开始剧增。比特区块难度的增加,要求算力更强大的机器才能挖矿,于是诞生了专门为挖矿机器设计的用型集成电路芯片 ASIC[20]。

为了推动人工智能继续向前发展,必须满足对更高阶处理能力的需求。摩尔定律随着计算机芯片微处理器发展到今天,已经开始面临失效,随着晶体管越来越小,晶体管电路逐渐接近了性能极限,通过提高集成度来提升芯片性能变得愈发困难。美国国防部高级研究计划局(DARPA)认为,突破摩尔定律的可能性方法是开发专用电路或专用型集成电路芯片 ASIC。

比特币挖矿设备早已跨入了 ASIC 时代,而使用 ASIC 芯片来进行人工智能相关的基础计算才刚刚兴起。如果能将区块链挖矿设备算力的一部分提供给人工智能,或者将闲置或淘汰的矿机资源应用在人工智能上,不仅能够推动人工智能的飞速发展,在倡导可持续发展、资源重复利用的今天,也是一种伟大的实践。

为了将人工智能更好地融入区块链,应该满足 3 个必要条件[22]:

1)挖矿算法能够支持现有的 AIASIC 芯片,并且可以极大地提升挖矿效率;

2)挖矿过程采用人工智能应用较为广泛的算法,能够适用于较广泛的人工智能计算场景;

3)区块链是去中心的,但是 AI 计算场景中需要一个中心来负责数据分发、任务调度和结果的汇总,新的挖矿算法需要解决这个矛盾。

条件 1)有两种满足方式,一种是直接使用现有的 AI 芯片(如寒武纪芯片),设计针对性的挖矿算法,这种方式的成本较低,但受限于 AI 芯片的设计;另一种是针对现有的 AI 芯片进行功能扩展,使其本身就具备挖矿的能力,这种方式需要设计和生产全新的芯片,成本较高,但是适用性更广。条件 3)在共识机制中采用 DPoS 的方式,通过节点投票选举代表的方式产生一个临时中心,负责 AI 作业的开展。

比原链(Bytom)[21]是一种多元比特资产的交互协议,在 PoW 共识机制中引入了矩阵运算与卷积运算,使其能友好地支持人工智能 ASIC 芯片。比原链采用定点优化的策略,针对具体的 AI ASIC 芯片设计算法,可以在使用 AI ASIC 芯片挖矿的同时进行人工智能的分布式加速计算。

为了更好地使用区块链加速 AI 运算,需要有一种机制将矿机的算力导出。导出的 AI 算力相对独立于主链功能,这部分算力的使用不会影响主链的运行,不会降低整个网络的安全性。AI 算力模块通过事先预留的编程扩展接口嵌入主链,可以与主链产生互动,满足可插拔的特性。

格雷德币(Gridcoin)[22]将全网算力一分为二,一部分用来维护网络的安全,另一部分输出到 BOINC 平台(伯克利开放式网络计算平台,目前是世界上最大的分布式计算平台)进行科学计算。

Gridcoin 采用 Scrypt-sleep 的加密策略(Scrypt 加密策略的延伸),根据 base58 钱包地址和对 BOINC 的贡献值来决定哪些钱包睡眠,而另一批钱包被唤醒参与到 hash 求解中来。Scrypt-sleep 算法能在保持 block chain 安全性的前提下,让区块链加密的算力需求降低一半。这些算力可以投入到科学计算中。

矿工可以自行选择如何分配自己的算力,如果矿工选择将全部算力用于传统挖矿,那么得到的奖励会较少;当矿工将一部分算力用于科学计算时,会得到较多的额外奖励。通过这种方式,格雷德币鼓励更多的矿工贡献算力到科学计算上。

3.4 共享 AI 时代的到来

人工智能发展到今天,已经涌现出了一批优秀的开发框架,如 Google 的 TensorFlow、BAIR(Berkeley Artificial Intelligence Research)的 Caffe、Facebook 的 Torch、IBM 的 SystemML 等。然而,框架之间彼此独立,在一个框架上训练好的神经网络模型无法直接在另一个框架上使用。

2017 年 9 月,Facebook 和微软共同面临了一个重大挑战——如何在机器学习不同框架之间进行切换,如 PyTorch 和 Caffe2。

区块链有加密技术和代币体系,有望实现各类 AI 核心算法的有效保护和快速的商业获利,并促进最大程度的技术共享。区块链搭建的人工智能共享平台,由矿机提供算力支持,通过免费或代币付费的方式提供 TensorFlow 和 AlphaGo 等其他人工智能产品的使用。平台能够鼓励更多的人投入到 AI 的研究中,同时将研究成果在全球范围内共享。

Atmatrix[24]是一个类似于以太坊的的项目,致力于搭建共享的人工智能平台。Atmatrix 提供了一个基于共识的、分

布式虚拟的 AIaaS(人工智能即服务)云基础设施，借助区块链经济系统，调用全球 AI 技术力量，打造世界人工智能。代表技术是 AIaaS 人工智能即服务技术、DBot 分布式机器人技术(DBot 账户、DBot 平台、DBot 主链)和 Oracle 跨链互操作技术。

图 5 给出了 Atmatrix 的框架结构。智能合约为了确保各个节点最终执行结果的一致性，在执行过程中无法直接访问外部数据或调用外部的 AI 服务接口，因为会引入不确定性。Atmatrix 在区块链网络和外部 AI 服务之间引入了 DBot 平台，使得智能合约和外部接口的通信是异步的。智能合约对外部 AI 服务的调用首先触发 DBot 平台中的节点，DBot 节点将请求信息发送给外部 AI 服务，并将外部 AI 服务返回的数据信息通过链下共识机制达成一致后，以交易的形式发送到区块链对应的智能合约上，使得这些信息成为区块链账本数据的一部分，从而消除非确定性。

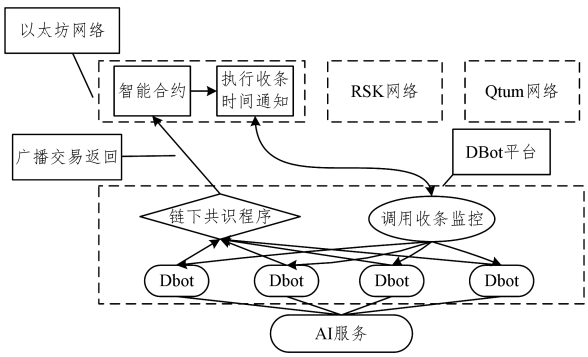

图 5　Atmatrix 框架结构

DBot 平台设计了服务注册合约以及对应的 DBot 账户管理策略，在被调用合约的区块链网络中存在收条证据和 Merkle 记录，因此也可以无需链下共识过程即可证明调用过程的可靠性和确定性。通过设定多个 DBot 账户来竞争执行该调用，以支撑在可靠性竞争执行的过程设定经济激励。

智能矩阵区块链包括主链和支持与其他区块链网络(如以太坊、量子链、元界、小蚁股、超级账本等)互操作的服务，主链是基于兼容 EVM 智能合约的石墨烯技术，并利用 Oracle 提供 AIaaS 和互操作服务的区块链。

Atmatrix 旨在构建具备人工智能能力的下一代区块链平台，为各个区块链网络的 DApp 服务，使各个区块链网络的 DApp 具备人工智能能力，使智能矩阵网络的 DBot 生态繁荣，同时促进人工智能成果在全球范围内实现共享。

4　面临的挑战

为了更好地结合人工智能，区块链技术需要克服自身存在的不足[25]。

4.1　提升交易吞吐量

目前，公有链和大部分私有链的吞吐量十分有限，比特币交易网络最令人诟病的一点就是交易性能：最初的全网交易速度只有 7 笔/s，远远低于传统的金融交易系统。同时，等待 6 个块可信确认导致约需 1 h 的最终确认时间。闪电网络[26]虽然提升了交易效率，但是不具备良好的对外扩展能力，这样的性能无法支撑“世界电脑”需求。

4.2　自主进化能力

区块链平台应该根据需求变化不断进行升级完善。目前，大部分区块链不具备自我变更能力，而只能通过硬分叉或软分叉的方式启用一个新的网络，并要求所有用户进行迁移。这种方式成本高，且存在很大的风险。

分叉的本质是，共识机制的失败，会造成区块链的分裂。在 2013 年 3 月 12 日，Bitcoin-qt 0.8.0 版本软件发布，该版本软件采用了一种新的数据库 level db。有的矿工节点及时升级了 Bitcoin-qt 0.8 版本，有的矿工还继续使用 Bitcoin-qt0.7 版本。双方各自生产区块，由于软件的 bug 导致 Bitcoin-qt 0.8生产出的区块被qt0.7版本节点拒绝掉，因此在区块高度 225430，比特币区块链分成了两条链，一条是包含大于 800kb 区块的链，另一条是拒绝承认这些包含更大区块的链，这就发生了硬分叉。这次硬分叉导致交易受到了很大影响。

不管是社区还是开发者决定的分叉，都会在一定程度上导致部分用户的利益受损，区块链需要寻求更安全的自适应方案。

4.3　技术被广泛认可还需时日

以比特币为代表的是区块链 1.0，以以太坊为代表的是区块链 2.0。区块链技术目前还处于一个探索阶段，其应用领域主要还在金融行业，在其他领域的应用还处于尝试阶段。大多数人不理解区块链和比特币的机制，对两者持观望或抵制态度。2017 年 9 月 15 日，监管部门要求国内比特币交易平台全部关停，比特币在国内遭受重创，区块链的关注度也有所下降。可以说，区块链的发展任重而道远。

5　展望

区块链和人工智能是两门终将改变世界的技术。人工智能的应用，体现在智能的服务层面，让生活更便捷、更有乐趣、节约时间、解放体力，未来机器将替代人类进行更多基础性的劳作。区块链技术基于加密算法、共识机制、去中心化等特性，为金融、公证、数字版权、物流等行业提供了新的解决方案。越来越多的人开始研究区块链技术并将其应用到项目开发过程中[27]，一批基于区块链技术的创业公司应运而生。AI 使得世界更加智能，区块链使得世界更加紧密相连、更加诚信和更加安全。

2017 年“区块链＋人工智能”模式开始被提出，欲定义“区块链 3.0”，随着人工智能去中心化自治组织(AI DAOS)的出现，建立在区块链基础上的人工智能将是一个重要的研究领域。区块链的研究必将进一步推动人工智能的发展。

结束语　本文对区块链技术进行了阐述，包括基本定义、结构设计和工作机制等，并从 4 个方面介绍了区块链技术推动人工发展的可能性，论证了区块链技术对人工智能发展的巨大价值。如同 Web 流浪器拓荒者 Marc Andreessen 所说：“20 年后，我们就会像讨论今天的互联网一样讨论区块链。”区块链有望成为继蒸汽机、电力、互联网之后，下一代颠覆性的核心技术，将与人工智能一起改造世界，让我们拭目以待。

参 考 文 献

[1]　何蒲，于戈，张岩峰，等. 区块链技术与应用前瞻综述[J]. 计算机科学，2017，44(4)：1-7，15.

[2]　YUAN Y，WANG F Y. Blockchain：The State of the Art and Future Trends [J]. Acta Automatica Sinica，2016，42(4)：481-494.

(下转第 70 页)

ference on Very Large Data Bases. VLDB Endowment, 2006: 661-672.

[15] HUANG Z, JENSEN C S, LU H, et al. Skyline Queries Against Mobile Lightweight Devices in MANETs[C]// International Conference on Data Engineering. IEEE, 2006: 66.

[16] WANG S, VU Q H, OOI B C, et al. Skyframe: a framework for skyline query processing in peer-to-peer systems[J]. The International Journal on Very Large Data Bases, 2009, 18(1): 345-362.

[17] CHEN L, CUI B, LU H, et al. iSky: Efficient and Progressive Skyline Computing in a Structured P2P Network[C]// International Conference on Distributed Computing Systems. IEEE, 2008: 160-167.

[18] LI H J, TAN Q Z, LEE W-C, et al. Efficient progressive processing of skyline queries in peer-to-peer systems[C]// International Conference on Scalable Information Systems. DBLP, 2006: 26.

[19] CUI B, CHEN L, XU L, et al. Efficient Skyline Computation in Structured Peer-to-Peer Systems [J]. IEEE Transactions on Knowledge & Data Engineering, 2009, 21(7): 1059-1072.

[20] HOSE K, LEMKE C, SATTLER K U, et al. A Relaxed But Not Necessarily Constrained Way from the Top to the Sky[J]. Lecture Notes in Computer Science, 2007, 4803: 399-407.

[21] VLACHOU A, DOULKERIDIS C, KOTIDIS Y, et al. SKYPEER: Efficient Subspace Skyline Computation over Distributed Data[C]// International Conference on Data Engineering. IEEE, 2007: 416-425.

[22] VLACHOU A, DOULKERIDIS C, KOTIDIS Y, et al. Efficient Routing of Subspace Skyline Queries over Highly Distributed Data[J]. IEEE Transactions on Knowledge & Data Engineering, 2010, 22(12): 1694-1708.

[23] FOTIADOU K, PITOURA E. BITPEER: continuous subspace skyline computation with distributed bitmap indexes[OL]. http://zeus.cs.uoi.gr/~pitoura/distribution/damap08.pdf.

[24] TAN K L, ENG P K, OOI B C. Efficient Progressive Skyline Computation[C]// International Conference on Very Large Data Bases. 2001: 301-310.

[25] PEI J, JIANG B, LIN X, et al. Probabilistic skylines on uncertain data[C]// International Conference on Very Large Data Bases. VLDB Endowment, 2007: 15-26.

[26] ZHANG Z, YANG Y, CAI R, et al. Kernel-based skyline cardinality estimation[C]// ACM Sigmod International Conference on Management of Data. DBLP, 2009: 509-522.

(上接第 57 页)

[3] Google Research Blog. AlphaGo: Mastering the ancient game of Go with Machine Learning[EB/OL]. (2016-01-27). https://google research. blogspot. com/2016/01/alphago-mastering-ancient-game-of-go. html.

[4] KUMAR A N. LEGO Robots and AI[J]. ACM SIGCSE Bulletin, 2005, 37(3): 418-418.

[5] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic CashSystem [EB/OL]. https://bitcoin. org/bitcoin. pdf.

[6] HABER S, STORNETTA W S. How to time-stamp a digital document[J]. Journal of Cryptology, 1991, 3(2): 99-111.

[7] Wikipedia. Blockchain[EB/OL]. [2017-10-17]. https://de. wikipedia. org/wiki/Blockchain.

[8] ANDREASM. Mastering Bitcoin: Unlocking Digital Cyrpto-Currencies [M]. Sebastopol, CA: O'Reilly Media, 2014: 160-170.

[9] SINHA A. Client-server computing [J]. Communications of the ACM, 1992, 35(7): 77-98.

[10] FAN J, YI L T, SHU J W. Research on the Technologies of Byzantine System [J]. Journal of Software, 2013, 24(6): 1346-1360.

[11] LOI L U U, NARAYANAN V, ZHENG C D, et al. A Secure Sharding Protocol For Open Blockchains[C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 17-30.

[12] HYPERLEDER. About Hyperledger [EB/OL]. [2017-10-17]. https://www. hyperledger. org/about.

[13] YUAN Y, ZHOU T, ZHOU A Y, et al. Blockchain: From Data Intelligence to Knowledge Automation [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[14] BANKO M, BRILL E. Scaling to very very large corpora for natural language disambiguation[C]// Meeting of the Association for Computational Linguistics. 2001.

[15] CIRESAN D C, MEIER U, GAMBARDELLA L M, et al. Deep Big Simple Neural Nets Excel on Handwritten Digit Recognition [J]. Neural Computation, 2010, 22(12): 3207-3220.

[16] MCCONAGHY T. How Blockchains Could Transform Artificial Intelligence[EB/OL]. (2016-12-21)[2017-10-17]. http://dataconomy. com/2016/12/blockchains-for-artificial-intelligence.

[17] MACCONAGHY T, GIELEN G. Canonical form functions as a simple means for genetic programming to evolve human-interpretable functions[C]// Conference on Genetic and Evolutinary Computation. 2006: 855-862.

[18] RICK OMAC G. AI on the Blockchain: Dystopian or Utopian Future? [EB/OL]. (2014-10-16)[2017-10-16]. https://www.cryptocoinsnews. com/ai-blockchain-dystopian-utopian-future.

[19] ZHU Z W. Node. js Blockchain Development [M]. Beijing: Mechanical Industry Press, 2017: 14-15.

[20] BITCOINWIKI. ASIC[EB/OL]. (2015-03-29). https://en. bitcoin. it/wiki/ASIC.

[21] BYTOM. BytomWhitePaperV1. 0[EB/OL]. http://bytom. io/BytomWhitePaperV1. 0. pdf.

[22] GridCoin[EB/OL]. [2017-10-17]. http://www. gridcoin. us.

[23] YEGULALP S. ONNX makes machine learning models portable, shareable [EB/OL]. (2017-09-08). https://www. infoworld. com/article/3223401/machine-learning/onnx-makes-machine-learning-models-portable-shareable. html.

[24] ATMATRIX. Atmatrix whitepaper[EB/OL]. https://www. atmatrix. org/ system/whitepaper-cn. pdf.

[25] SONG S Z, ZANG C. Calm Thinking Under the Blockchain Hot [J]. Chinese Banking, 2016(12): 33-35.

[26] POON J, DRYJA T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments[EB/OL]. (2016-02-14). https://lightning. network/lightning-network-paper. pdf.

[27] CAI W D, YU L, WANG R, et al. Blockchain Application Development Technical [J]. Journal of Software, 2017, 28(6): 1474-1487.