区块链应用研究进展

朱建明[1],付永贵[1,2]

1. 中央财经大学信息学院,北京 100081
2. 山西财经大学信息管理学院,太原 030031

摘要 区块链是基于去中心化的分布式账本技术,可以实现业务活动数据的隐私保护、安全存储及不可抵赖证明。自2009年产生以来,区块链技术逐渐被人们认可并在各行业得到重视和研究。本文总结了区块链的特点、技术,对区块链进行了应用、发展阶段及创业团队分类,对区块链与云计算的关联关系进行了分析。对区块链在世界各国及不同产业的应用研究现状以及目前区块链的学术研究进展进行了综述分析。结果表明,区块链在不同应用领域得到了广泛的探索,然而尚未形成成熟的可以推广的产品,学术研究多数为特点及价值分析,一些学者开发了具体领域的处于测试状态的区块链产品。区块链将颠覆传统的数据库体系及业务交互体系,成为"互联网+"时代信用建设的技术体系保障。

关键词 区块链;应用研究;云计算

信用是人、组织机构之间进行生产、维持社会关系的基础,目前人们主要采用规定、制度、法律、合同契约等来约束社会信用问题,这些方式由于人为主观因素较多是无法彻底解决信用问题的。

互联网的发展及其应用的普及给人们生活带来了很大的便利,然而伴随而来的网络诈骗事件也给人们生活带来了很大的困扰;因此,在目前各行业"互联网+"发展目标下,如何很好地解决"互联网+信用"则成了"互联网+"能否有效建设的前提,虽然学术界及产业界将网络交易信用寄希望于大数据体系,但由于数据获取困难,数据质量无法完全保证等问题,大数据依然没有很好地解决"互联网+信用"问题。

区块链是迄今为止第一个解决信用问题的技术手段,其使用严密的数据真实性证明机制实现了社会活动及交易活动的信用证明。

1 区块链

区块链(blockchain)是基于互联网的分布式账本技术,同时也是一个去中心化的数据库[1-2],区块链产生于2009年1月3日,创始人为中本聪,并于2009年1月9日发布。区块链本身不是产品,它是随着其产品比特币提出来的,因此最初的区块链是比特币区块链,即比特币是区块链的第一个成功应用,然而区块链并不是金融科技,仅仅是一个协议体系,因此,区块链技术不会随着人们对比特币热情的消退而受到冷落,反而由于自身鲜明的特点及技术优势使得其在智能合约、投票选举、冲突解决、健康公证、身份验证、股权众款等广泛领域得到关注和研究。事实上,区块链技术几乎可以应用于人们生活的每一领域,并将在未来产生颠覆性的革命。

区块链的主要特征有去中心化、开放性、自治性、信息不可篡改性、匿名性等。区块链的去中心化使得所有加入区块链的用户都可以参与其数据真实性证明,摒弃了传统认证体系单一认证中心的不足,事实上区块链的去中心化更多的是指区块链的"多中心化认证体系",而不是"无中心化";区块链的开放性是指区块链数据资源及管理隶属于加入区块链系统的所有节点,而对区块链系统以外的主体则是屏蔽的;区块链的自治性是指区块链由其系统节点自己维护,其数据证明机制由计算机通过协议作出,是在无人干预的情况下实现的;加入区块链的每个节点都是分布式记录区块链数据,这就保证了数据的不可篡改性;在区块链中每个节点的身份都是通过其发布的密钥哈希值表示的,这种不公开身份的隐匿身份数据交换模式可以有效地实现节点的隐私保护。

区块链的技术包括哈希算法、数字签名、时间戳技术、工作量证明机制等,这些技术可以在对区块链数据进行加密保护的情况下确保数据的源头、时间、涉及的主体,证明其真实可靠。区块链系统中各节点不需要掌握这些计算机信息安全领域的技术细节,只需要了解具体的系统操作规范,同时具有公开、透明性,既实现了网络对节点应用的公开性,又能将信息安全技术与经济管理结合起来,是人类信用领域的伟大创举。

目前,学术界及产业界在比特币区块链技术原理的基础上对其技术及应用进行了很多改进,形成了不同应用领域的

收稿日期:2016-12-16;修回日期:2017-02-18

基金项目:国家自然科学基金项目(U1509214)

作者简介:朱建明,教授,研究方向为网络与信息安全、区块链,电子信箱:zjm@cufe.edu.cn

引用格式:朱建明, 付永贵. 区块链应用研究进展[J]. 科技导报, 2017, 35(13): 70-76; doi: 10.3981/j.issn.1000-7857.2017.11.011

区块链产品。

1.1 区块链分类

按区块链应用来分可以分为私有链、联盟链和公有链。

1）私有链。专门服务一个组织或某一简单业务的区块链,私有链有很大的封闭性和排他性,通常在一个较小的范围实施,由于其目标单一,所以构建相对简单。

2）联盟链。多个组织为了一个共同目标而组成的区块链,一些相关组织在获得联盟同意也可以加入联盟链。这种形式的区块链将会成为未来区块链的主流。

3）公有链。任何组织或个人都可以通过申请加入区块链,区块链没有排他性,这种区块链由于对用户扩展性无限制,可能在未来用户维护方面会有困难。

1.2 区块链的发展阶段

从进化的角度对区块链进行描述,可以分成3个阶段,这3个阶段代表了区块链的技术进展,也代表了区块链应用的发展,目前全世界处于第一阶段与第二阶段之间,为了表述方便,将这三个阶段分别定义为区块链1.0、区块链2.0、区块链3.0。

1）区块链1.0——数字货币。

这一阶段最具代表性的产品是2009年1月9日的比特币。随后,又相继出现了大量的基于区块链的数字货币或服务于比特币的交易平台。

比如:2013年7月,Mastercoin(Omni)通过meta-protocol拓展比特币功能,成为最早的数字加密货币;2013年12月NXT(未来币),成为首个完整的PoS区块链;2013-2014年,Bitshares(比特股)产生,与NXT和CounterParty组成"数字资产二代币三剑客";以及2016年3月产生的Lisk,2016年5月产生的TheDAO等,这些数字货币都是以区块链作为底层技术的。另外,国内比较有代表性的以区块链技术为基础的数字货币还有莱特币、OkCoin、BTCC等。

数字货币是区块链最初始应用领域,在这一领域区块链用于交易记录的证明,然而由于数字货币交易平台信息安全的脆弱性,数字货币价格波动大,交易时间长,政府对数字货币监管不力,用户对区块链技术原理理解困难等问题,导致基于区块链技术的数字货币在运行过程中出现了大量的操作问题及安全事件,基于区块链技术的数字货币在经历了盲目过热后而走向市场低迷。

2）区块链2.0—数字资产与智能合约。

这一阶段的典型特征是区块链突破数字货币应用的局限,逐渐扩展到数字资产与智能合约,在这一阶段区块链逐渐体现出其技术特征的生命力,体现出其去中心化、不可抵赖证明的价值。这一阶段比较有代表性的产品有:2014年7月,Ethereum(以太坊),将智能合约理念推进到极致;以及2015年3月的Factom(公正通),国内的太一系统等。

数字资产与智能合约是以数字形式存在的,随着互联网的出现与发展而更加普及,区块链技术应用于数字资产与智能合约可以更加有效地追溯其内容生成的途径,证明内容的归属及真实有效性。

3）区块链3.0——DAO、DAC(区块链自治组织、区块链自治公司)→区块链大社会(法律、健康医疗,银行,区块链+人工智能,区块链+能源等)。

这一阶段是区块链发展的第3个阶段,是区块链技术广泛应用于人们生活、生产的各个方面,区块链被人们广泛接受并应用,其产品比如国内的万向区块链实验室、布比、安存正信等。

在这一阶段,区块链将彻底改变人们生活的方式及交往形式,而且各个领域的区块链系统将会由私有链、联盟链逐渐发展为公有链,不同功能的区块链系统会进行无缝对接,甚至还会出现不同功能的用于租用的区块链平台。

1.3 创业团队

随着全球对区块链的关注,各行各业产生了大量的区块链创业团队,从团队目标进行分类,区块链创业团队大致可以分成底层技术团队、底层技术+应用团队和纯应用团队3类。

1）底层技术团队。比如布比网络、Chain、以太坊,这些团队基本上由高学历的技术专家组成,他们为很多第3类应用团队提供技术开发平台。目前因为技术要求较高,这一类创业团队较少,但这一团队发展的空间还很大;

2）底层技术+应用团队。例如Ripple,DAH等,国外早期的区块链创业团队基本采用这种模式。目前这一类团队多是有其名无其实,很多业务的底层技术还是成型业务技术上的转型;

3）纯应用团队。比如纳斯达克的Linq团队,国内的阳光积分、格格积分等,这些团队专注于应用层的开发,而在区块链底层他们分别采用了Chain提供的底层和布比提供的底层平台。这一类团队的发展空间最大,因其目标是面向领域应用,故其特征可以概括为"区块链+"。

目前,全世界对区块链的研究成果尚处于初级阶段,具体表现为概念炒作,具体场景应用的价值分析,应用探索,还没有形成比较有生命力的可以推广使用的区块链产品。按区块链的研究成果分类,区块链的研究成果可以分为应用研究和学术研究。

2 区块链与云计算

区块链是一个数据库,而且随着时间的推移,区块链数据库容量会快速达到大数据的量级,因此区块链系统是离不开云计算的。区块链与云计算的结合一方面表现在区块链数据在云平台的存储、计算、管理,另一方面表现在区块链系统会为云计算提供其所需要的计算机及其他网络设备硬件资源,还可以为云计算提供所需要的软件资源。

区块链由于使用了哈希算法、工作量证明机制等技术,其涉及的数据量会非常巨大,单机系统的计算能力是无法满足区块链系统运行要求的,大数据的管理需要云存储实现,若没有云平台及云环境实现区块链数据的存储区块链最终会走到数据管理瓶颈的状态。

云计算的实现需要大量的软、硬件资源,区块链系统中包含着大量的节点计算机,这些节点计算机承载着区块链运行任务,使得其很容易被集中调度而形成一个云硬件资源环境,这些节点计算机中的软件资源也可以为云计算提供软件服务。区块链系统中的节点计算机既可以实现区块链系统的云计算服务要求,也可以满足其他系统对云资源的服务外包要求。

因此,区块链系统与云平台之间是互相依托的,区块链系统既需要云平台的服务,又可以依托区块链系统而构建云平台。区块链系统与云平台之间的关系如图1所示。

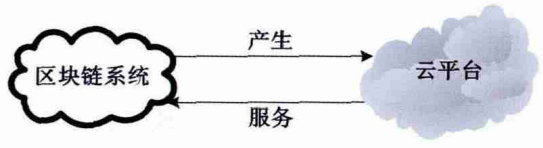

图1 区块链系统与云平台关系

Fig. 1 Relation between blockchain and cloud computing

3 区块链应用研究进展

3.1 区块链在世界各国的发展状况

目前,对区块链最为关注的当属英国。2016年1月19日,英国政府发布了重要报告《分布式账本技术:超越区块链》,旨在探索类似于区块链的账本技术,用于记录物品所有权和知识产权,保障政府隐私等。英国央行发布数字货币RSCoin代码并进行测试,与比特币底层区块链技术不同的是RSCoin由中央机构控制,是完全基于央行的需求而设计的全新的理论框架。

另外,区块链技术在其他国家政府也受到了高度关注。比如:全球区块链联盟委员会于2015年11月在迪拜成立;在美国,总部在纽约德勤Rubix已经成为区块链行业的领头人,具有行业领先水平的区块链架构,目前已经升级为企业级区块链应用开发平台,美国BTC公司使用区块链技术构建了用于大选的投票机;日本于2016年4月成立了区块链联盟(BCCC);荷兰央行正在致力于开发一种被称为基于区块链技术的原型币——DNBCoin;韩国、俄罗斯央行也表示密切关注区块链技术;等等。

3.2 区块链在中国的发展状况

目前,区块链在我国产业界受到了高度关注。比如:中国央行对数字货币持积极态度,逐步加强对数字货币的研究力度;2016年2月3日,中关村区块链产业联盟正式成立,同时中关村创业公社区块链国际孵化中心成立;2016年5月31日,中国金融区块链合作深圳联盟(FBSC)正式成立;该联盟成员包括31个金融机构或金融科技公司;2016年8月21日,中国区块链产业大会在北京召开;2016年8月25日,中国区块链技术应用研讨会在北京召开;国内恒生电子极有可能凭借技术优势,携手蚂蚁金服,将区块链技术运用到移动支付、P2P、征信等多个领域;飞天诚信一直关注数字货币的发展,对区块链有一定的技术及研究成果。

区块链在受到中国产业界关注的同时,也受到了高校教学研究的重视,2016年7月5日中国第一个基于区块链的校企联合实验室在中央财经大学信息学院建立。

3.3 区块链在产业界的应用

3.3.1 区块链在金融行业、大型公司的应用

Magister Advisor分析结果显示,到2017年银行在区块链开发方面的投入经费将超过10亿美元,将成有现有企业软件中发展速度最快的一项软件。2016年5月25日,世界交易所联合呼吁明确区块链应用监管政策。目前区块链在全世界金融行业得到了高度关注,一些大型有实力的金融机构或者金融公司、计算机公司着手进行区块链在具体领域的应用研发。具体表现在以下几个方面。

1) R3 CEV。总部位于纽约,是目前最为知名同时规模最大的传统金融区块链联盟组织,R3 CEV放弃了比特币区块链完全开放性的、任何组织和个人都可以加入的"公有链"特性,形成专门服务于银行机构的"私有链",从2015年9月成立以来截至2016年8月4日,迅速吸引了全球最大的55家金融机构(中国平安保险(集团)股份有限公司于2016年5月24日加入R3),这些金融机构包括西班牙对外银行、桑坦德银行、美国银行、巴克莱银行、花旗银行、德意志银行、汇丰银行等,涉及中国、西班牙、美国、英国、加拿大、法国、瑞士、丹麦、日本、德国等国家,另外也有其他一些非金融机构也加入了R3,比如IBM公司通过自身的区块链服务机构加入了R3;R3 CEV目前处于开源形式,加入R3 CEV的所有成员金融机构都可以参与这一区块链联盟组织提供的测试及广泛应用,内容包括互操作性、支付、结算等;2016年4月,R3 CEV公布了首个与比特币区块链技术架构不同的分布式总账应用Corda。

2) 证券行业。全美证券托管结算公司(DTCC)于2016年1月发布了区块链白皮书《拥抱颠覆-探索分布式总账潜力、改善交易后环境》一书,后于2016年3月召开全球研讨会,研究区块链及分布式记账对金融基础设施与金融行业的影响;纳斯达克于2015年10月率先推出区块链技术产品Linq,随后澳大利亚证券交易所(ASX)、伦敦证券交易所(LSE)、迪拜多种商品交易中心(DMCC)、日本交易所集团(JPX)等也关注区块链;2015年12月美国证券交易委员会(SEC)批准在线零售巨头Overstock通过比特币区块链发行自己股票的计划;国际跨境支付清算巨头SWIFT于2016年5月发布《区块链对证券交易流程的影响及潜力》报告,提出金融行业应该采取有适当访问权限的联盟式区块链形式,区块链首先会在没有中央托管的领域推广应用,而在中央托管的公开市场中规模化应用则会相对滞后,在一定行业中应用区块链技术可能涉及到制度的改造问题;欧洲证券及市场管理局(ESMA)密切关注区块链技术及其应用的发展,做好调整

监管框架的准备。

3）欧清银行(Euroclear)与奥纬咨询(Oliver Wayman)于2016年2月联合发布《资本市场上的区块链》研究报告,意在帮助资本市场加深对区块链及其应用的认识。

4）保险方面。伦敦保险市场大玩家劳合社开始了以区块链为技术基础的Target Operating Model(TOM)现代化计划项目。而德国安联保险集团已可以成功使用基于区块链的智能合约实现巨灾互换和债权交易的处理。

5）期货方面。美国商品期货交易委员会(CFTC)计划将比特币与其他电子货币作为监管对象,关注区块链在市场中的应用。

6）会计审计方面。普华永道开始组建区块链技术团队,分析客户对于区块链技术的潜在应用及可能需求。德勤、安永宣布进军区块链,尝试在客户端的自动审核功能使用区块链技术。

7）大型公司方面。IBM、Intel、Cisco等于2015年底加入受Linux基金会监督的Open Ledger Project开放账本项目,目前此项目称为Hyper Ledger(超级账本),Onchain是中国首家加入Hyperledger的区块链公司;IBM公司构建了企业级区块链的技术框架和标准,并将其主体部分贡献到Hyper Ledger项目之中。鉴于物联网是区块链未来应用研究的重要方向之一,IBM公司已经开始与芬兰Kouvola Innovation在这一领域着手进行合作;而在人工智能方面,IBM公司则尝试将区块链技术引进公司的人工智能计算机Watson之中;2016年1月3日,世界第一个成功上市的区块链投资公司Coincilium在伦敦ISDX交易所首次公开募股。

8）其他领域的应用。例如:区块链技术公司Factom与金融数据公司Intrinio达成合作,计划未来将华尔街金融系统纳入Factom区块链之中;2016年7月27日,来自纽约的全球区块链联盟Agentic Group宣布开设伦敦办事处,正式进军英国市场;GovCoin Systems Ltd.是一家区块链技术金融科技新兴公司,总部设在伦敦,被英国工作和养老金部选中进行以区块链为基础的福利支付试验。这项试验于2016年6月开始,目标是发展应用于福利系统更高效、防篡改能力更强的技术;Paypal在2015年12月举办了黑客马拉松活动。目的是找出利用Paypal使用比特币和区块链技术的新方法。

3.4.2 区块链在其他产业领域的应用研究

区块链除在金融领域及大型公司得到广泛关注以外,在通信、医疗健康、教育、知识产权等方面也得到了一定的进展。具体表现在:

1）通信领域。Bitmessage代表了区块链在通信领域的一个典型应用。

2）在医疗保健方面。区块链技术公司Tierion与飞利浦医疗保健集团合作研究如何使用区块链实现患者信息的安全、可靠保存。

3）在教育方面。索尼已经成功开发了适用于教育领域的区块链技术,而且其研究成果具有通用指导价值。

4）知识产权方面。美国知识产权律师事务所正在研发Monegraph应用程序,通过将个人的指纹数字化后上传区块链系统,证明对应数字信息的所有权,为数字化产品所有权的交易提供了技术保障。

综合区块链在产业领域的研究成果可以发现,目前金融领域、大型公司、通信、医疗健康等领域对区块链进行了高度关注,然而目前区块链在这些领域的应用研究尚处于探索阶段,现有的应用成果也处于试运行和产品调整、完善阶段,没有形成可以推广使用的产品。

3.4 学术研究进展

在学术领域区块链的研究成果包括理论概述、特点及价值分析方面的研究成果,从批判角度分析区块链价值的成果,以及理论技术探讨方面的研究成果。

3.4.1 特点、价值分析方面的研究

因为目前区块链尚处于初级阶段,所以现有区块链这一成果较多,这些成果涉及能源、金融、军事、法律法规等很多领域。其具体内容包括具体领域应用价值分析、区块链带来的社会影响及技术变革、区块链的特点等几个方面。

在具体领域应用价值分析方面,研究者根据具体应用领域的特点,分析区块链应用于这些领域会产生什么样的经济价值及数据质量保障价值,这些成果目前属于探索分析式的内容,一般没有涉及区块链的核心技术,只是结合区块链的特点进行分析。

曹寅[3]介绍了区块链在能源领域应用的意义;吴健等[4]分析了区块链技术应用于数字版权保护领域的价值;李绍民等[5]提出将区块链应用于多媒体数据版权保护;廉蔺等[6]分析了区块链技术在情报工作绩效激励、武器装备全寿命管理和军用物流等军事领域中的潜在价值;王和等[7]分析了区块链技术应用于互联网保险领域的价值;袁勇等[8]提出区块链是社会物理信息系统(CPSS)平等社会的基础架构之一,而计算实验和平行执行(ACP)方法可以自然地与区块链技术相结合;de Meijer[9]提出英国政府在数字货币方面的关注度在世界居于领先地位,英国政府不仅在诸如比特币这样的加密货币领域投入资金,而且在其底层技术区块链方面投入资金,意在改变金融世界;区块链技术受到中央银行、金融机构和技术公司的关注;该论文讨论了区块链在不同领域应用的潜在价值以及案例,区块链不仅局限于数字现金支付,而且在智能合约等其他领域也有很大的应用价值;Trevor I. Kiviat[10]综合当前研究领域杰出的计算机科学家与密码学家思想以提升立法领域对区块链的理解,最终告知决策者与从业者考虑不同的监管方案,对区块链基于货币的经济属性的测试说明技术的正确价值在于其潜在的更有效地促进数字资产的转移,比如法律界更有效的文件和著作权验证,所有权转让和合同执行;虽然围绕虚拟货币的监管已经开始形成,但其替代应用仍有很多的不确定性。Peters[11]讨论了数据货币理论及其价值,对其在世界不同领域的监管状态进行概述。

在区块链带来的社会影响及技术变革方面的研究成果

方面,研究者从区块链对社会生活、生产及其他信息领域带来的变革入手进行研究,分析区块链的技术地位,目前这一方面的成果尚处于初级阶段,没有形成实际的区块链社会地位架构或技术影响机制,对其未来发展分析的也不够。

王立仁[12]以清算记账、云存储、改造能源产业等为例说明区块链对各行业生产力的推动和促进作用;冯珊珊[13]提出随着区块链数据库时代的来临,大数据的质量、可信度会上升到不容置疑的程度;杨东[14]提出区块链会变革目前现有的法律法规;高航等[15]提出随着区块链算力的提升,将加速大数据行业发展,促使未来区块链计算机从致富工具向智能机器发展,促进区块链网络生态发展,促进区块链技术及应用的创新。Goertzel等[16]提出基于区块链技术的货币可以做到透明开放交易,这在人类全球经济一体化、开放协作、网络互联环境下是有发展潜力的,有助于最大化个人和社会的经济利益。

在区块链特点分析方面,研究者更多注重区块链去中心化特点分析,强调区块链去中心化更多侧重于"多中化",而不是"无中心化",这些研究从区块链原理入手,阐述其在具体应用中的模式。

谌麒艳[17]分析了区块链应用于金融行业业务活动的价值,分析区块链未来应用于金融业更可能是"多中心化";穆琳等[18]提出,未来金融可能不会是完全的去中心化,而是多中心化与弱中心化,体现了在金融系统构建私有区块链的思想,体现了弱化传统主体话语权的思想;杰基·海兰等[19]提出区块链与比特币是两个完全不同的事物,在比特币名声不太好的现实情况下,区块链在未来反而会体现出创造新产业机遇并且颠覆现有技术与工艺的巨大潜力,它将成为未来的主流;蒋海[20]提出区块链是构建价值互联网的基础,是有史以来第一个使用技术构建信用体系的,区块链的去中心化更多体现在多中心化,而不是完全没有中心;Steven[21]对比特币区块链的起源以及其去中心化、点对点服务等特点进行了分析。Greenspan[22]介绍了3种类型的分类账:中心化数据库、以太坊区块链、比特币区块链,对比结果得出以太坊区块链在存储程序方面与中心化数据库有很多相似之处,而比特币区块链在分类账与交易水平方面与中心化数据库有根本性的不同。Birch[23]建立了一个简单的共享分类账分类和分层结构便于金融服务领域技术人员、业务人员和管理者之间进行交流,并介绍了其中的技术原理。Feld等[24]对比特币的底层区块链技术工作原理进行了分析。

特点、价值分析方面的研究成果体现研究者对区块链的关注程度,这些研究将成为区块链应用研究、推广使用的前期成果,促进区块链的发展。

3.4.2 批判分析角度进行的研究

有些研究成果是从批判的角度对区块链进行分析的,这些研究从辩证的角度入手,在肯定区块链价值、发展的基础上,提出区块链发展应用尚需面对的问题。

程华等[25]从技术、监管政策、生态体系等方面对区块链的局限性及不足进行了分析;庄基良[26]针对目前对区块链过度迷信崇拜的现状,指出区块链从技术到应用仍处于最初级阶段,要想实现区块链革命性的潜力需要政府、企业和标准制订组织等的通力合作与不懈努力;蒋润祥等[27]在肯定区块链取得进展的前提下指出区块链在应用研究过程中会受到现行法律、观念、制度等的制约,技术上还需要进一步完善,还受到类似量子技术等的挑战。

3.4.3 理论、技术方面的研究

这一方面的研究着手从区块链底层的技术出发对区块链进行研究,其研究结合具体应用需求,对区块链的技术原理进行改进,构建具体应用领域的区块链技术算法及架构,为区块链在具体领域的应用奠定基础;根据具体领域需求,构建具体的区块链产品,并对其工作原理进行介绍。

算法及架构方面的研究。这一方面的成果主要设计区块链的架构并对其性能进行分析。

朱建明等[28]分析了区块链的特点、局限性以及其链式结构散列原理,设计了多中心认证架构,并以煤炭行业为实例构建了相应的认证模型;Göbel等[29]研究了Bitcoin blockchain演化的通信延迟的影响;使用马尔可夫模型、空间泊松过程模型等进行了算法分析;Li等[30]提出一种基于禁忌搜索算法的鲁棒区块链,将其算法应用于动态产品退货与再制造的批量问题,并通过实证进行了分析;Zou等[31]针对云计算对服务执行的监控合同、责任分配和争议仲裁在问责方面的缺乏,基于区块链技术特征提出点对点环境中创新服务合同管理,用于监控服务合同的执行,基于此在一个真正分布式环境中即使在一个没有权威监管机构存在的环境中服务参与者也可以被追究问责;赵赫等[32]将区块链技术应用于采样机器人数据保护,设计了系统结构及实现技术。

产品设计及原理分析方面的成果成果以比特币区块链技术原理为基础,对区块链算法结构进行改进形成具体的产品,这一方面的研究成果决定着区块链具体应用的市场,表现了区块链在不同应用领域的存在形态,因此在具体应用过程中需要对比特币区块链的基础架构进行改进才能形成适宜具体领域的产品。

Ziegeldorf等[33]提出一种基于比特币区块链而改进的服务-CoinParty,进行了协议的算法设计和系统属性的讨论,最后进行了实证分析;基于区块链技术比较典型的产品Certcoin,Fromknecht等[34-35]在使用PKI查找或验证基于身份的公钥的技术环境下,提出一种去中心化系统-Certcoin,使用分布式字典数据结构实现关键字查找,针对目前互联网认证中证书权威认证必须依赖可信的第三方机构的不足,以及信任网认证实施的困难,提出将Certcoin应用于公共认证,并对Certcoin技术协议原理进行说明;Morselli等[36]针对信任模型PGP网络作为一个去中心化的认证系统,虽然在安全电子邮件中取得了巨大成功,但是其需要中心服务器对证书存储管理并对客户访问进行应答,提出一个在完全无结构网络中实施的点对点的检索认证链技术系统-KeyChains,KeyChains是一个去中心化的PKI系统,仿真实验证实了这一技术系统是有效

的和安全的;Kuo等[37]针对健康护理隐私保护需求,提出一种基于区块链技术的模型-ModelChain,并描述了这一模型的结构运行算法机理。

4 结论

近年来,区块链虽然未推广使用,但其价值得到了政府、研究人员及业界的肯定,人们期望区块链技术为15亿没有合法身份的人验明正身,解决身份问题;期望在区块链的推动下,迎来由信息互联网向价值互联网迈进的时代;期望区块链对现有生活模式带来的伟大变革等。热情之余,依然需要对区块链的现状及未来进行重新认识。区块链的发展要经过"技术萌芽→概念炒作→期望膨胀→泡沫破灭→稳步爬升→实质生产→推广使用"这样的发展阶段,目前比特币区块链本身的缺陷使得其不可能解决并适用于所有领域的数据保密及可靠性证明问题,而且区块链技术本身及适用场景还需要进一步进行考证,因此,"区块链泡沫"总有破灭的一天,届时人们需要正确面对区块链,停止盲目跟风,将区块链思想原理放到具体的环境中与具体环境进行结合,构建适用于具体场景的、具有一定约束的、与法律法规契合的"私有区块链"系统,并将其投入生产、推广使用,随着区块链应用的推广,区块链会面临着资源整合的问题,这时一些"私有区块链"会通过整合形成"联盟区块链",进一步发展会形成规模更大的"公有区块链",但需要说明的一点是,即使到了"公有区块链"阶段,隶属于各业务的"区块链"仍有其特性,包括权限、架构等,而且仍有一些区块链因为业务自身特性而停留在"私有区块链"或"联盟区块链"阶段。

本文在对区块链的特点、技术、发展等进行分析的基础上,从区块链的应用研究与学术研究两个角度对区块链的研究进展进行了综述;通过综述可以看出,目前区块链的发展尚处于初级阶段,但得到了产业界及学术界的广泛关注,尤其得到了金融领域的高度重视,这是因为一方面区块链的最初成果应用是比特币区块链,另一方面是因为区块链技术协议是用于实现数据可靠、安全、匿名存储及不可抵赖证明的,这恰恰是金融领域目前突出的信用管理问题所需要的;但区块链的强大兼容性和扩展性使得其在几乎所有的领域都有强大的生命力。

目前区块链从理论、技术、应用都不成熟,理论成果还处于探索阶段,产品还处于创业阶段,以后将继续关注区块链的发展,同时进行区块链技术创新研究,推进区块链的发展。

参考文献 (References)

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. [2016-11-30]. https://bitcoin.org/bitcoin.pdf.

[2] Kavanagh D, Miscione G. Bitcoin and the Blockchain: A coup d'état in Digital Heterotopia?[C]. The 9th International Conference in Critical Management Studies: Is there an alternative? Management After Critique, University of Leicester, United Kingdom, 8-10 July, 2015.

[3] 曹寅. 能源区块链与能源互联网[J]. 风能, 2016(5): 14-15.
Cao Yin. Energy blockchain and energy internet[J]. Wind Energy, 2016 (5): 14-15.

[4] 吴健, 高力, 朱静宁. 基于区块链技术的数字版权保护[J]. 广播电视信息, 2016(7): 60-62.
Wu Jian, Gao Li, Zhu Jingning. Digital copyright protection based on blockchain technology[J]. Radio & Television Information, 2016(7): 60-62.

[5] 李绍民, 姚远. 区块链多媒体数据版权保护方法研究[J]. 科技资讯, 2015(12): 13-14.
Li Shaomin, Yao Yuan. Research on copyright protection of multimedia data in blockchain[J]. Science and Technology Information, 2015(12): 13-14.

[6] 廉蔺, 朱启超, 赵炤. 区块链技术及其潜在的军事价值[J]. 国防科技, 2016(4): 30-34.
Lian Lin, Zhu Qichao, Zhao Zhao. Blockchain technology and its potential military value[J]. National Defense Science & Technology, 2016(4): 30-34.

[7] 王和, 周运涛. 区块链技术与互联网保险[J]. 中国金融, 2016(5): 74-76.
Wang He, Zhou Yuntao. Blockchain technology and internet insurance [J]. China Finance, 2016(5): 74-76.

[8] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-493.
Yuan Yong, Wang Feiyue. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-493.

[9] de Meijer C R W. The UK and Blockchain technology: A balanced approach[J]. Journal of Payments Strategy & Systems, 2016, 9(4): 220-229.

[10] Kiviat T I. Beyond Bitcoin: Issues in regulating blockchain tranactions [J]. Duke Law Journal, 2015, 65: 569.

[11] Peters G W, Panayi E, Chapelle A. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective [J]. Journal of Financial Perspectives, 2015, 33: 92-113.

[12] 王立仁: 区块链对生产力的促进和推动[J]. 金卡工程, 2016(6): 5-6.
Wang Li Ren: The promotion of blockchain to productivity[J]. Cards World, 2016(6): 5-6.

[13] 冯珊珊. 区块链: 信任背书大数据时代的可能性[J]. 首席财务官, 2016(3): 14-17.
Feng Shanshan. Blockchain: Trust endorse the possibility of big data era[J]. CFO World, 2016(3): 14-17.

[14] 杨东, 潘婴东. 区块链带来金融与法律优化[J]. 中国金融, 2016(4): 25-26.
Yang Dong, Pan Zhaodong. Blockchain bring financial and legal optimization [J]. China Finance, 2016(4): 25-26.

[15] 高航, 俞学劢, 杨辉辉. 计算能力与区块链技术: 未来科技金融核心[J]. 中国经济报告, 2016(7): 106-110.
Gao Hang, Yu Xuemai, Yang Huihui. Computing power and blockchain technology: the core of future science and technology finance [J]. China Policy Review, 2016(7): 106-110.

[16] Goertzel B, Goertzel T, Goertzel Z. The global brain and the emerging economy of abundance: Mutualism, open collaboration, exchange networks and the automated commons[J]. Technological Forecasting and Social Change, 2016(4): 1-9.

[17] 谌麒艳. 区块链:金融业即将面临的一场革命[J]. 银行家, 2016(7): 14-16.
Chen Qiyan. The blockchain-another revolution of the financial industry[J]. The Chinese Banker, 2016(7): 14-16.

[18] 穆琳, 屈燕, 闵文文. 区块链:传统金融"攻城狮"[J]. 当代金融家, 2016(7): 104-108.
Mu Lin, Qu Yan, Min Wenwen. Blockchain: the traditional financial

"siege lion"[J]. Modern Bankers, 2016(7): 104-108.
[19] 杰基·海兰, 阿琼·卡帕尔, 朱莉娅·查泰莱, 等. 区块链: 颠覆还是服务?[J]. IT经理世界, 2016(5): 20-23.
Jackie Hyland, Arjun Kharpal, Chatterley Julia, et al. Blockchain: Subversion or service?[J]. CEOCIO China, 2016(5): 20-23.
[20] 蒋海. 区块链:开启价值交换新时代[J]. 金融科技时代, 2016(7): 27-29.
Jiang Hai. Blockchain: Open a new era of value exchange[J]. Financial Technology Time, 2016(7): 27-29.
[21] Steven L. Bankchain and itBit: Settling on the blockchain[J]. Modern Trader, 2016(5): 16-21.
[22] Greenspan G. Payment and exchange transactions in shared ledgers[J]. Journal of Payments Strategy & Systems, 2016, 10(2): 172-180.
[23] Birch D, Brown R G, Parulava S. Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis[J]. Journal of Payments Strategy & Systems, 2016, 10(2): 118-131.
[24] Feld S, Schönfeld M, Werner M. Analyzing the deployment of Bitcoin's P2P network under an as-level perspective[J]. Procedia Computer Science, 2014, 32: 1121-1126.
[25] 程华, 杨云志. 区块链发展趋势与商业银行应对策略研究[J]. 金融监管研究, 2016(6): 73-91.
Cheng Hua, Yang Yunzhi. Research on the development trend of blockchain and the coping strategies of commercial banks[J]. Financial Regulation Research, 2016(6): 73-91.
[26] 庄良基. 掘金区块链[J]. 互联网经济, 2016(7): 16-19.
Zhuang Liangji. Nuggets blockchain[J]. The Internet Economy, 2016(7): 16-19.
[27] 蒋润祥, 魏长江. 区块链的应用进展与价值探讨[J]. 甘肃金融, 2016(2): 19-21.
Jiang Runxiang, Wei Changjiang. Application progress and value discussion of blockchain[J]. Gansu Finance, 2016(2): 19-21.
[28] 朱建明, 付永贵. 基于区块链的供应链动态多中心协同认证模型[J]. 网络与信息安全学报, 2016, 2(1): 27-33.
Zhu Jianming, Fu Yonggui. Supply chain dynamic multi-center coordination authentication model based on blockchain[J]. Chinese Journal of Network and Information Security, 2016, 2(1): 27-33.
[29] Göbel J, Keeler P, Krzesinski A E, et al. Bitcoin Blockchain Dynamics: the selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation, 2016(7): 1-32.
[30] Li X Y, Baki F, Tian P, et al. A robust blockchain based tabu search algorithm for the dynamic lot sizing problem with product returns and remanufacturing[J]. Omega, 2014, 42(1): 75-87.
[31] Zou J, Wang Y, Orgun M A. A dispute arbitration protocol based on a peer- to- peer service contract management scheme[C]. IEEE ICWS2016, San Francisco, USA, June 27-July 2, 2016.
[32] 赵赫, 李晓风, 占礼葵. 基于区块链技术的采样机器人数据保护方法[J]. 华中科技大学学报(自然科学版), 2015, 43(增刊1): 216-219.
Zhao He, Li Xiaofeng, Zhan Likui. Data integrity protection method for microorganism sampling robots based on blockchain technology[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015, 43(Suppl 1): 216-219.
[33] Ziegeldorf J H, Matzutt R, Henze M, et al. Secure and anonymous decentralized Bitcoin mixing[J]. Future Generation Computer Systems, 2016(5): 1-19.
[34] Fromknecht C, Velicanu D, Yakoubov S. A decentralized public key infrastructure with identity retention[EB/OL]. [2016-10-20]. https://eprint.iacr.org/2014/803.pdf.
[35] Fromknecht C, Velicanu D, Yakoubov S. CertCoin: A namecoin based decentralized authentication system[R]. Massachusetts: Massachusetts Institute of Technology, 2014.
[36] Morselli R, Bhattacharjee B, Katz J, et al. KeyChains: A decentralized public-key infrastructure[EB/OL]. [2016-10-20]. https://www.researchgate.net/publication/228714967_Keychains_A_decentralized_public-key_infrastructure.
[37] Kuo T T, Hsu C N. ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks[EB/OL]. [2016-10-20]. https://www.healthit.gov/sites/default/files/10-30-ucsd-dbmi-onc-blockchain-challenge.pdf.

Progress in blockchain application research

ZHU Jianming[1], FU Yonggui[1,2]

1. School of Information, Central University of Finance and Economics, Beijing 100081, China
2. School of Information Management, Shanxi University of Finance and Economics, Taiyuan 030031, China

Abstract Blockchain is a distributed ledger technology based on decentration, and can realize business activity data's privacy protection, secure storage, and non repudiation proof. Since it was produced in 2009, the blockchain technology has been gradually accepted by people and received attention from almost every industry. In the paper we summarize the characteristics and technology of blockchain, and classify blockchain by application, development stage, and entrepreneurial team. We discuss the relation between blockchain and cloud computing. Moreover, we review the application research status on blockchain in the world and in different industry sectors, and summarize the current blockchain's academic research progress. It is indicated that blockchain has got extensive exploration in different application areas while it is still not mature or a popularized product, Although the current academic research results mainly focus on characteristics and value analysis, some scholars have developed concrete area's test status blockchain products. We believe blockchain will subvert the traditional database system and business interaction system and will become the technology system guarantee for the Internet plus era's credit construction.

Keywords blockchain; application research; cloud computing

(责任编辑 刘志远)