



区块链的产业现状、存在问题和政策建议

梅海涛¹, 刘洁²

(1. 中国移动通信集团设计院有限公司, 北京 100080;

2. 中国信息通信研究院, 北京 100191)

摘要: 区块链是一种去中心化、去信任的集体维护数据库技术, 其本质是一种去掉删除和更新操作的分布式数据库。阐述了区块链的技术原理, 梳理了区块链的产业现状, 分析了区块链存在的问题。最后, 从政府、行业协会和学术机构 3 个角度提出了相应的政策建议。

关键词: 区块链; 去中心化; 拜占庭将军问题

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016299

Industry present situation, existing problems and strategy suggestion of blockchain

MEI Haitao¹, LIU Jie²

1. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China

2. China Academy of Information and Communications Technology, Beijing 100191, China

Abstract: Blockchain is one kind of collective and decentralized database technology without trust among the nodes. In essence, it is a distributed database which has no delete and update operations. The technical principles of blockchain was introduced, its industry situations and existing problems were discussed, and related policy suggestions were proposed from government, industry association and academic institution.

Key words: blockchain, decentralization, Byzantine failure

1 引言

一直以来, 账本是商业活动的核心要素, 用于记录金钱、产权等资产信息。记录账本的介质依次经历了泥板标记、甲骨刻字、竹片刻书、布帛记账、纸张写字、电脑记录、数据库存储等阶段, 这都属于集中式的记账方式, 需要机构信用或国家信用背书。如今, 区块链首次实现了协作维护的分布式总账技术, 在让所有人都有机会参与记账的同时, 降低了信任构建成本和交易成本, 加速演进互联网治

理模式, 创新商业合作模式, 提高协作流通效率, 正如超文本传输协议引领全球跨入信息自由传递时代一样, 区块链开创了价值自由转移的互联网“众证共识”时代。

(1) 技术本质: 一种集体维护的分布式数据库

区块链是一种基于密码学原理构建的分布式共享数据库, 其本质是通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案允许系统内的所有节点都备份当前区块链的一个完整副本, 每隔一段时间, 系统选出这段时间记账最快最好的节点, 由其利用密码学

技术计算和验证,将这段时间内的所有有效交易信息和当前区块链的“数字签名”记录到一个新区块(block)上,并将新区链接(chain)至当前区块链副本的末尾,形成新的区块链副本。区块链的任何变动,都会向整个系统进行消息广播,实现全网区块链副本的更新。如上所述,区块链技术具有分布式对等、去信任、集体维护和无法篡改四大特点。

(2)组织形式:分布式对等端,从阶层关系向扁平化平等关系演变

区块链由众多节点共同组成一个端到端的网络,整个网络没有中心化的硬件或管理机构。任何节点具有相同的权利和义务,都有机会参与总账的记录和验证,将计算结果广播发送给其他节点,且任一节点的损坏或者退出都不会影响整个系统的运作。传统支付系统几乎必须借助可信赖的第三方机构来处理电子支付信息,无法避免“基于信用模式”带来的高成本交易和效率低下等弊端。区块链系统基于密码学原理,而不是基于信用,使得任何达成一致的双方都能直接支付,不需要第三方中介的参与,从而促使系统拓扑逐渐从星状拓扑演变成扁平化的网状拓扑,具有良好的系统顽健性。

(3)通信机制:无需信任系统,基于数字签名的加密技术确保信息安全

依托公开透明的系统运作规则和数据传输内容,系统中节点之间的数据交换通过数字签名技术进行相互验证,形成一种基于密码学算法的共识信用。只要按照系统既定的规则进行,就可以确保节点之间的通信安全。其中,数字签名涉及一个散列函数、发送者的公钥、发送者的私钥。在密码学中,公钥和私钥成对出现,公开的密钥叫公钥,只有自己知

道的叫私钥。用公钥加密的数据只有对应的私钥可以解密,反之,用私钥加密的数据只有对应的公钥可以解密。

(4)共识机制:对拜占庭将军问题的一个现实实现

拜占庭将军问题是指在整个网络中的任意节点都无法信任与之通信的对方时,如何能创建出共识基础来进行安全的信息交互而无需担心数据被篡改。单纯地依赖投票机制,以少数服从多数来达成共识,容易引发“共谋串通”的账本篡改(Sybil 攻击)。区块链技术在信息传递的过程中加入了大量计算成本,即工作量证明,通过解决一个数学难题来限制发送信息的权利,并用数字签名和散列验证的方式来解决拜占庭将军问题中的溯源和验真难题,以数学加密作为其信用背书,确保整个系统的所有节点能在去信任的环境下建立信任,达成共识。

2 区块链的产业现状

区块链是一个具有国家战略意义的新兴产业,如图1所示,截至2016年9月26日,基于区块链的加密货币一共有682种,总市值为11 962 051 199美元。其中,比特币占79%,以太坊占9%,瑞波币和莱特币分别占2%,并列前三。

2.1 全球高度重视区块链的发展

根据世界经济论坛的报告,全球已经有24个国家和地区正在投资区块链技术,80%的银行将在2017年前启动区块链项目,90多个中央银行加入了区块链讨论,90多个公司加入了区块链联盟。在过去3年里,区块链的风险投资超过了14亿美元,产生了2 500多个区块链相关专利。

从国际组织来看,联合国社会发展部(UNRISD)和国

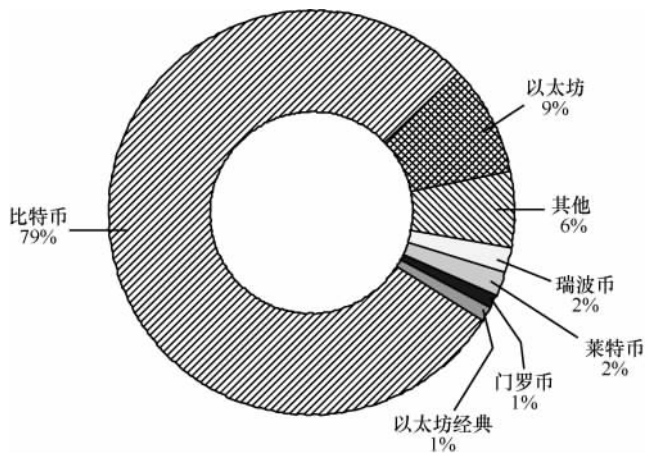


图1 基于区块链的加密货币市场份额



际货币基金组织分别发布区块链相关的加密货币报告,看好区块链技术在金融行业广阔的应用前景。从全球来看,美国司法部举行了数字货币峰会,证券交易所纳斯达克基于区块链开发股票交易平台;英国政府发布《分布式账本技术:超越区块链》研究报告;爱沙尼亚已经在税务和商业注册系统中使用了区块链技术;日本于2016年5月首次批准数字货币监管法案,将其定义为财产。从我国来看,中国人民银行于2016年1月20日召开数字货币研讨会,考虑争取早日推出央行发行的数字货币。2016年4月19日,由上海证券交易所牵头、中证机构间报价系统股份有限公司等11家机构共同成立的中国分布式总账基础协议联盟(China Ledger 区块链联盟),激发了各金融机构应用区块链的积极性。2016年7月,工业和信息化部(以下简称工信部)信息化和软件服务司印发了《关于组织开展区块链技术和应用发展趋势研究的函》(工信软函[2016]840号),并委托工信部电子标准院联合蚂蚁金服、万向控股、微众银行和平安保险等国内重点企业开展区块链技术和应用发展趋势研究工作。

2.2 区块链吸引了众多跨国巨头和创业公司

截至2016年年初,全球已经有917家区块链领域的创业公司,在区块链领域的累计投资已经超过了15亿美元。随着区块链潜在价值和巨大潜力的不断挖掘,重量级跨国行业巨头纷纷通过成立研究小组、投资区块链创业公司、开发区块链基础平台、研究未来的潜在应用前景等方式超前布局区块链领域,其示范与引领作用已经开始带动新一轮的区块链创业创新浪潮。

2.3 区块链加速向各行各业广泛渗透

从高科技行业来看,主要是围绕区块链技术,构建区块链技术开发和运行的一整套生态系统,提供底层分布式应用运行的协议,加速区块链和现有技术的集成创新,改变现有商业的运营模式和行业业态。科技巨头微软、IBM和亚马逊纷纷推出BaaS(blockchain as a service,区块链即服务)的解决方案,帮助中小开发者更快速地应用研发。此外,还有一些新兴创业公司针对某一行业特性提供某一专业领域的技术研发平台,如Counterparty、Chain都主要专注于为金融和资本市场的客户提供基于区块链的应用程序开发与运行平台。

从金融行业来看,除了为比特币等数字货币提供交易平台以外,区块链技术可以大幅改善,甚至颠覆现有

数字货币以外的各种资产交易系统,在金融衍生品、外汇、私人股权、能源信用挂钩投资品等资产的清算结算程序中大显身手。区块链技术提升了金融机构的运行效率,以往美国证券市场的结算审核需要2~3天,运用区块链技术以后,结算审核时间将至分钟级,甚至是秒级,降低了系统性风险;区块链降低了金融机构的运营成本,根据奥纬(Oliver Wyman)的估算,目前数字证券全球每年的交易流程,共要浪费650亿~800亿美元的各种中间人手续费,区块链可以显著精简流程,从而节省大笔费用;区块链技术提升了金融市场的安全,基于智能合约的区块链可以处理复杂的衍生品交易,将清算变更为标准化、自动化,24 h不间断的运营特点也让数据互换变得更为稳定和值得信赖。

从公共管理、能源等行业来看,公共管理、能源、交通等领域的中心化特质也产生了效率低下的问题,可以借助区块链技术,改进客户体验,提升服务效能。LO3 Energy和区块链技术开发企业ConsenSys合资成立公司,基于区块链技术,让居民可将自家太阳能板产生的过剩电力出售给对面街道的家庭。德国电力公司将区块链技术应用于电动汽车充电,基于智能合约和分布式总账,按时租赁充电桩。

3 区块链存在的问题

(1)“代码即标准”将产生新的中心

区块链技术虽然实现了运行时的“去中心”,但是强化了设计时的“中心化”。根据比特币的核心源代码分析,从2010年中本聪将项目控制权移交给Gavin Andresen至今,比特币的核心代码主要由6个国外程序员持续贡献。尽管代码贡献团队成员多于200人,但其中几乎没有中国程序员的身影。一旦区块链代码形成规模,成为行业标准,必将形成决定软件修复更新、未来发展决策的另一个中心化的组织。

(2)区块链耗费了大量资源

一是体现在区块链需要耗费大量的计算能力。截至2016年初,比特币区块链的全网计算能力已经达到了 8×10^{18} 次运算/s,而当前世界运行最快的计算机——美国用于核武器研发的蓝色基因超级计算机的计算能力为 2.8×10^{14} 次运算/s,从这个数据来看比特币区块链的计算能力已经是世界上最快的单台计算机的计算能力的28 571倍。

二是全网算力无法像云计算一样协同互动。区块链的特性决定了每次只有一个矿工能获得记账权,那么其他矿工的计算都被浪费。区块链技术的全网算力无法像云计算一样通过协同合作的方式对外输出,产生价值。此外,挖矿能力的比拼进入白热化,带来了高额电费的支出。据报道,东北一家挖矿工厂拥有 2 500 台矿机,每个月矿机运行的电费就达到了 40 万元。

三是底层的传输机制耗费大量网络带宽。由于采用工作量证明机制,在耗费大量全网算力的同时,交易速率被限制在 6~7 笔/s,不能处理的交易只能排队等待。由于区块链通过广播进行消息交互,排队消息的广播容易带来广播风暴,对底层网络的带宽资源带来大量消耗,导致网络性能下降甚至瘫痪。

(3) 技术的集成创新需谨防“多症并发”

区块链是私钥加密算法、P2P 网络、工作量证明机制 PoW 等多种已有技术的集成创新成果,这些技术从诞生至今已经发展了十余年。虽然在发展过程中,多个缺陷已经得以完善,但仍存在很多难以解决的问题,需要谨防这些缺陷综合起来产生严重后果。

第一,从密码学来看,加密算法的安全通常定义为在当前技术水平下,加密信息在相当长的一段时间内(例如 100 年以上)无法被解密。但是,随着新的数学算法的出现以及计算能力的提高(例如,量子计算机),以往安全的加密信息可能在较短时间内被解密。

第二,从 P2P 网络的稳定性来看,当前大量节点的参与维持了网络的顽健性。一个重要原因是比特币自身的价格处于高位,且电费便宜,成本可以覆盖收益。中国绝大部分高计算能力的比特币矿机为了降低成本部署在小水电站周边。但是,如果有一天因为成本、政治或其他因素,大量节点开始退出网络,则要防范由此可能带来的区块链网络的不稳定性。

第三,从工作量证明机制来看,系统在仅拥有少数节点的时候,使用工作量证明机制存在一定的风险。由于这时的攻击者算力很容易超过全网算力的 50%,进而轻松实现 51% 攻击,导致整个系统的瘫痪和失效。

(4) 区块链自身存在的问题

首先,区块链的工作量证明机制,限制了交易速率只能是 6~7 笔/s,不能像现在成熟的支付系统一样快速高效。例如,VISA 的交易处理峰值为 1.4 万笔/s。其次,区块链目前已经生成了 40 多万个区块,约 60 GB 数据量。很多区块

链的应用,为了实现物品溯源和证书公证等目的,在交易附言里添加物品和验证信息,进一步加快了区块链的膨胀速度,以致于区块链的读写操作日益缓慢。第三,区块链技术在高效低耗、安全和去中心化三者之间,存在“不可能三角”问题。

4 区块链产业的政策建议

(1) 政府超前布局区块链,加强顶层设计和统筹谋划

一是针对区块链能耗投入产出比低、“去中心化”替代成本高等弊端,政府应发挥统筹协调作用,组织专家研判区块链和分布式总账技术的发展趋势,把握区块链技术潜在用途、成本收益及其技术本质,商议区块链可能带来的个人隐私、伦理和社会影响,通过设立专项基金和出台政策等方式,引导产业健康发展;二是重点挖掘区块链在“一带一路”国际产能合作方面的潜在价值,促进国际合作,打破地缘政治,共同构建合作共赢的新型国际关系;三是加快制定区块链的相关法律法规,通过立法将区块链技术纳入合适的监管框架之内,控制数字货币发行数量,加强金融等行业的市场监管,防范系统性风险。其中,尽可能在维护系统参与者利益与维护更广泛的社会利益间达成平衡,避免固化的架构阻碍技术创新。四是加快区块链在金融、公共服务等行业的试点应用,加速形成以点带面、点面结合的示范推广效应,鼓励政府部门、企事业单位作为区块链的主要节点参与网络运营,发挥“干中学,学中做”的精神,积极积累一线实战经验;五是建议由分管信息化的中央部门牵头,会同发改委、商务部、公安部、一行三会等部门,联合商议区块链技术引发的安全问题,加强安全监管,维护公众利益,确保社会稳定。

(2) 产业联盟积极引导,提升我国行业标准的话语权

一是发挥产业联盟在国家标准、行业标准的“抢跑”优势,针对区块链实现语言不一致、智能合约标准不统一等存在问题,先行先试联盟标准,引导产业集群优化升级,提高企业竞争力。二是针对“代码即标准”的产业现实,积极培育中国特色的区块链开源生态,构建区块链开源社区,汇集国内精英和全球智慧,提高我国在区块链开源项目中的代码贡献量,增强我国在区块链领域的话语权和影响力。三是针对区块链和共享经济的高度融合性,建立区块链技术研发的公共服务平台,提升产品研发和产业化能级和水平,构建“双创”良好格局,鼓励区块链和“互联网+”深度融合,打造新的经济增长极,助推共享经济。四是积极引



导企业进行专利布局,预防专利“陷阱”,做好知识产权保护,维护企业的合法权益,提升企业的国际竞争力,加快实现企业的“走出去”。

(3) 科研机构夯实基础研究,保证人才和知识供给

一是针对缺乏区块链技术和垂直行业复合型人才痛点,鼓励学校开设区块链的相关教学课程,加大学校和企业的合作力度,通过订单式培养,培养学科交叉、知识融合、技术集成的复合型人才,构建领军人才、高端人才、专业人才的人才梯队,形成人才集聚效应。二是探索建立区块链技术的国家重点实验室,夯实区块链的基础研究,增强密码学、P2P网络、重叠网、人工智能等方面的相关研究,跟踪量子计算机等前沿研究,搭建基础研究和交叉学科研究的创新平台,增强原始创新能力,唱响中国声音。三是依托高校、研究机构和企业自主创新平台,形成产学研用相结合的开发联合体,加大核心信息技术的投入,严格

管理研究资金,推动科研成果转化。

[作者简介]



梅海涛(1959-),男,中国移动通信集团设计院有限公司技术部资深经理,主要研究方向为大数据分析。



刘洁(1979-),女,中国信息通信研究院产业与规划研究所电信行业研究工程师,主要研究方向为行业数据分析、运营商科技创新管理等。