学会视点

密切关注信息技术领域热点问题

中国电子学会　　第 3 期（总第 40 期）

2019 年 2 月 25 日

区块链与其他技术融合的趋势与挑战

编者按：区块链作为数字经济的一个重要技术在近几年已经有一定范围的应用，但是目前为止没有大规模服务于实体经济的落地应用。分析其中原因，我们发现除了区块链本身技术不够成熟以外，区块链与其他技术的融合是势在必行。区块链与其他技术的融合能够克服区块链本身技术的不够成熟，监管的困难性，安全问题，存储问题，数据上链的真实性问题等等企业级应用落地必须关心的问题。如何与其他技术融合，并且寻找真正服务于实体经济的应用，我们做了一些研究。围绕于此，中国电子学会汇报初步研究结果及对策建议如下：

一、ABCDSIS 技术的融合是大趋势

互联网发展从静态的内容发布的 Web 1.0 到目前的 WEB2.0。WEB 2.0 是技术的小融合，结合了 SoLoMoCo (Social, Location Based, Mobile App and Cloud Computing)，也就是社交，定位，移动 app, 云计算, 产生了非常大的经济效益，产生了像阿里巴巴，腾讯这样的巨无霸企业。我们看到目前技术正在从小融合进入到大融合。这个大融合产生的经济效益将会远远超过小融合带来的经济效益。我们看到的技术大融合是 ABCDSIS。

区块链作为一个单独的技术有一定的使用范围，目前比较多的 DAPP 应用是虚拟世界的游戏和数字货币。区块链服务于实体经济，必须与其他技术融合才能解决数据上链的真实性，安全，风险控制，监管等等难题。ABCDSIS 分别是 AI，区块链（Blockchain），云计算（Cloud Computing），数字化转型（Digital Transformation)，信息安全（Security），物联网（IoT）和分布式存储（Storage Decentralized）的英文首字母。

（一）区块链与人工智能

AI 可以帮助区块链在现实世界的应用程序中变得更加

智能。例如，在供应链金融中，为了控制风险，可以利用人工智能为区块链提供智能数据和 AI 运行结果。相比于传统人工智能应用，结合了区块链技术之后，通过共识机制保证了 AI 运算结果可验证，AI 算法的 hash 可以上链验证，保障算法和计算结果的准确性。区块链可以帮助 AI 提高数据共享能力，AI 运算需要大量的数据，通过区块链的去中心化存储以及零知识证明和 MPC（安全多方计算）计算解决数据孤岛问题的同时保证数据隐私性。通过使用智能合约和激励机制实现数据确权和交易，使得数据定价不再具有垄断性。区块链还可以帮助 AI 推广优化的 AI 算法，并为深度学习任务建立分布式的计算能力，有效使用闲散的计算资源。区块链智能合约可用于管理 AI 算法的行为，和规避 AI 算法不正当使用所产生的安全问题。

（二）区块链与云计算

自从区块链技术诞生之日起至今已经不再是简单的分布式账本的形式存在。区块链技术的去中心化计算，去中心化存储使得增加了区块链实现云计算的可能性。目前以亚马逊为主导的 I 层的云计算，真正被慢慢地被区块链颠覆。相比于类似亚马逊的 AWS 和阿里巴巴的阿里云的云服务，区

块链技术主要利用不可篡改性和可靠性提高云计算的服务性能。而这些正是传统云计算所不能实现的。目前的云计算服务虽然是分布式系统，但是以中心化形式进行计算，资源调度和利用都有一定的局限性。而利用区块链技术，比如去中心化存储 IPFS 协议，将云计算所需要的数据分片存储于物理层面的临近节点，在提高数据可靠性的同时提高了网络带宽利用率。而对于去中心化计算，对网络运算资源进行分片，自适应地使得网络在执行计算的过程中达到负载均衡，使得其相比于传统云计算达到更好的资源利用率。但是另一方面，区块链本身由于是基于共识机制，会导致所有数据都对外可见，而云计算往往涉及到大量的计算隐私问题，解决方案之一是通过联盟链的形式，数据在联盟中的节点中可见。另外一种解决方案是通过零知识证明、SGX 等的方式将计算数据进行加密计算，计算节点无法获得数据明文。不过由于计算复杂度较高，这种方式还正在发展之中。

通过区块链进行去中心化的云计算技术目前仅处于起步阶段，不过谷歌、微软、亚马逊，IBM 等公司都已经开始着手研究，虽然具体细节没有公开，未来可以想象云计算因为有了区块链可以更加安全，稳定，高效，节省能源，更

加多的个人计算资源可以被有效地调用。云计算的商业模式和提供商的运营模式会因为区块链赋能而改变。

（三）区块链与数字化转型

数字化转型需要为区块链提供真实的数据。区块链使用 NuChain（一个加拿大公司的区块链项目）的 BNP（Blockchain Network Protocol: 区块链网路协议）和 POC（Proof of Contribution: 贡献证明，提供有效数据和优化的 AI 算法进行共识）可以帮助数字化转型，以弥合数字和物理世界之间的距离。为了实现从物理世界到数字世界的转型，其需要保证的有两点。一个是数据的真实性以及数据有效性。数据真实性是指物理世界产生的数据如何真实的进行上传和验证。为了实现真实性，单一的通过软件是难以达成的。一种有效的方式是通过硬件芯片，利用加密硬件芯片对数据进行签名，由于签名无法伪造的特性，可以在区块链节点上对签名进行验证。此外，还要保证传输过程的安全性。BNP 协议定义了硬件签名，传输协议，链上验证协议等来保证整个链下到链上的过程是安全的并且数据是真实的。数据有效性是指物理世界存在大量的噪声数据，使得所上传的有价值数据不高，并且不同的数据价值也不一样。由于区块

链的激励机制和智能合约，通过调用合约的频率和激励可以根据数据需求进行市场定价，从而从经济学层面对数据进行定价，这也间接的反应了数据的有效性。这种定价模型也可以通过 AI 的方式对数据使用频率，数据内容等客观参数拟合数据有效性并且进行全网共识。NUChain 通过 POC 算法把激励和上传数据有效性的判定通过上述方式进行结合，从而使得数字化转型过程更加客观有效。当获得真实、有效的数据之后，通过区块链对数据进行分析，可以实现包括监管，征信等应用场景。

（四）区块链与信息安全

区块链本身的不可篡改性是具有安全属性的，它有效地保证了数据的完整性。但是不可篡改性是一把双刃剑，当链上出现漏洞的时候这些漏洞往往无法弥补。当我们将安全性与区块链集成时，需要采用深度防御方法。区块链的一些顶级安全控制包括：智能合约安全，DAPP 安全，共识节点强化，加密交换安全性，身份和访问管理，节点到节点流量加密，链上和链下数据加密等。

智能合约由于一经发布无法修改，这样如果存在漏洞，往往会产生直接经济损失并且难以挽回，一个经典的例子就

是 DAO 事件。而智能合约的审计和验证费用高昂，就算经过审计也难以避免其中存在安全隐患。目前这个领域的研究方向大多希望通过形式化证明的方式来确保只能合约的安全性，虽然已经有大量研究人员进入这个领域，但是仍然在发展过程中还未成熟，对于复杂的合约逻辑依然难以满足。

共识安全，比如 POW 的 51%攻击，分叉等等情形正是因为 PoW 在某些情况下依然无法达到非常安全的情况。由于不可能三角的存在，安全性，去中心化和可扩展性不能同时兼得，极大的限制了区块链技术的发展。如何按照具体应用，在不可能三角找到最佳的平衡是区块链项目需要研究的课题。

节点安全涉及到区块链底层实现逻辑的漏洞，譬如 EOS 爆出过远程攻击漏洞，ETH 的 RPC 端口暴露，以太坊默认对 RPC 不做鉴权的设计引起资金被盗的问题等。这种安全隐患往往难以察觉，一般都是在区块链系统运行过程中爆出类似漏洞，这样需要在区块链上线前进行大量的重复测试和验证。

数据加密安全和之前提到的漏洞不太一样，由于区块链本身是公开透明的，很多隐私数据无法在链上流转，这个时

候可以通过多种密码学算法譬如零知识证明，MPC 等技术达到在不暴露信息的情况下进行验证。

其他一些信息安全包括私钥管理、通信安全、加密算法、钱包多签名漏洞等等也是区块链技术所要研究的方向之一。

（五）区块链与物联网

物联网可以利用区块链来管理机器到机器的通信和支付。物联网部署中使用的边缘计算可以帮助区块链构建大量的共识节点和处理能力。例如 Nuchain 利用边缘计算来训练数据模型，找到最佳的 AI 算法和从 IoT 设备收集到的真实数据。

（六）区块链与分布式存储

对于区块链未来发展，存储是一个必不可少的功能，很多应用场景中比如 AI、IOT 等都需要大量的数据接入，而这些领域需要和区块链结合就不可避免的需要解决存储问题。另一方面，由于存储是有成本的，需要占用大量的存储资源，这样区块链的激励机制可以将存储的成本进行量化。目前主流区块链是无法直接存储大规模数据的，因为全节点需要同步所有区块链数据，如果大量的数据存在于链上会导致节点负载过大，从而区块链效率变低。目前比较流行的数

据上链的方式是将数据放置在 IPFS 等去中心化存储中，并且将例如哈希，上下文数据，数据地址等等小量数据存储于区块链上。但是这种存储方式是无法通过真实性和有效性进行数据验证的。此外，数据存储激励也难以通过这种方式实现。为了实现激励机制，著名的 filecoin 项目提出了复制证明（Proof of Replication）和时空证明（Proof of Space Time），复制证明和时空证明通过激励机制保证了矿工存储数据的真实性和延续性。但是这种机制是否成熟稳定依然还需要工业界的验证。

总的来说，重要的是要注意个别技术的实际应用范围非常有限。技术的融合可以提供大范围的实际应用，从而实现融合应用中使用的每种技术的快速成熟。

二，区块链技术和落地应用面临的挑战

当前区块链技术和落地应用的主要挑战是隐私保护，可扩展性，共识算法，数据上链的真实性，程序缺乏模块性等等问题。

（一）隐私保护

从隐私角度来看，目前的区块链项目还不够成熟。在隐私保护方面，零知识证明，安全多方计算，同态加密，环签

名，BLS 签名，Schnorr 签名，Mibble Wimble 等等隐私算法值得研究。具有访问控制的状态通道，可信计算环境（TEE）等的研究一直非常活跃，也有助于隐私保护技术的发展。研究人员面临的难题是满足欧盟通用数据保护条例（GDPR），隐私法，HIPPA 等法规规定的隐私要求，并满足 KYC / AML 的要求。隐私和 KYC / AML 的监管要求之间需要保持平衡。这个也是我们应该研究的课题。

（二）可扩展性

从可扩展性的角度来看，有 3 层解决方案。顶层（称为第 2 层技术）使用侧链，子链或跨链技术来分流从主链到子链的大量交易请求。例如，三个众所周知的项目：以太坊 Plasma，Polkadot 和 Cosmos 正在采用不同术语的主链和子链技术（CosmosZone 或 Polkadot 的平行链都是子链）。以太网的 Raiden 网络和比特币的闪电网络也采用了类似的交易分流的思想，以减轻主链的负担，减少瓶颈，从而提高可扩展性。中间层又称为第 1 层技术。在这一层中，想法是使用分片（Sharding），隔离见证（Segwit），增加块的容量，使用有向无环图（DAG）或改进主链上的共识算法来提高主链本身的可扩展性。底层也称为零层技术。在该层中，主

要思想是改进对等网络（P2P）路由和节点发现算法以获得更好的可扩展性，或者在未来，利用 5G 技术来获得更好的网络带宽。总的来说，所有三个方面的改进都是必要的，并且正在研究中，以提高区块链的可扩展性。

（三）共识算法

从共识算法的角度来看，异步通信领域的 FLP 不可能性定理已经证明在完全异步通讯的分布式环境下,如果有一个节点出错，整个网络是没有办法取得共识的。所以共识算法研究人员试图绕过 FLP 不可能性，因此大多数共识算法都假定了网络节点的诚实多数和部分或完全同步。例如，在比特币工作证明算法中使用的 POW 算法假定 51％诚实节点和响应时间的上限（部分同步），各种类型的 POS 算法也假设多数诚实节点和不同程度的同步性。POS 算法的关键问题是所谓的“无利害关系”（Nothing at Stake）攻击。所谓的无利害关系是指由于 POS 投票成本几乎为 0，如果区块链存在多个分叉,每个验证者都会在所有分叉上进行投票实现攻击的目的。此外，POS 还会面临长程攻击等情况。可见目前的 POS 共识还不够成熟。我们最终还是无法避免使用 PoW 共识。PoW 的问题是其计算的内容是无意义的，

浪费能源。我们认为节点需要执行实际有用的计算，例如在 Nuchain 的 POC 共识算法节点提供最佳的机器学习算法或有效的深度学习训练数据可以获得奖励。

（四）上链数据的真实性

从数据真实性的角度来看，为了使区块链技术对现实世界的应用有用，迫切需要向区块链提供真实的数据。虽然区块链具有链上数据的不可篡改性。但是缺少将现实世界物理对象的属性映射到链上的第一英里问题。如果没有数据真实性，区块链上的智能合约可以对假数据，垃圾数据进行操作，因此执行智能合约的结果将可能导致资产损失或其他严重后果。

受到网络的 OSI 协议启发，NuChain 定义了五层区块链协议，这个包含

物理层:通过 RFID、二维码、传感器、生物识别等技术实现物理世界数据化;

接入层:通过支持 BNP 协议的区块链接入设备将数据上链;

网络传输层:解决区块链网络通用协议及传输协议，实现多节点、多链、跨链的互联互通;

数据层:支持各种共识协议及激励机制、存储、加密以及账本存储等;

应用层:支持各 DAPP 及商城 Stores 等应用。

其中 BNP 定义接入层对数据真实性进行保证。

接入层主要功能之一是数据确权。NUChain 为每个接入层设备安装一个硬件芯片，芯片包含一个保密的私钥。每次数据产生后，会对数据进行签名，这样在链上验证的时候进行确权。

此外，BNP 定义了数据报文的格式如下:

通过校验码、哈希值和签名确保传输过程中数据无法被篡改。

（五）程序缺乏模块性

目前绝大部分区块链项目代码质量非常差,缺乏模块性和层次性。代码基本上是意大利通心粉，牵一发而动全身，因此很难经过修改用到企业级的应用。NULS 团队在区块链

模块化设计非常有创新。NULS 由微内核和功能模块组成，以弱化主链的全新思维，通过事件和服务的剥离，实现高度模块化的底层架构，提供智能合约、多链并行、跨链共识等运行机制，降低开发和使用的成本，推动区块链商业应用进程。作为一个基础链，NULS 提供了智能合约、多链并行、共识机制、P2P 网络、存储、加密、多级账户等功能模块。我们认为区块链设计和代码的模块化是区块链落地必须解决的问题。

三、措施建议

一是监管创新和吸引出海的区块链团队回国发展。目前国内很多区块链团队出海在新加坡，瑞士，澳大利亚等等国家建立区块链公司，这个对于我们国家来说失去了税收权，监管权和一定的话语权。目前区块链行业处于一种鱼龙混杂的状况,很多的区块链项目在没有得到一个有效技术和商业模式验证的就进行立项，技术含量非常低，在国内仍然大量存在。而有些区块链技术创新经过国际会议和专家肯定，但是因为国内监管环境不得不出国。我们需要有效的监管机制使得那些传销，空气，欺骗的区块链项目没有藏身之地。同时鼓励优秀的区块链项目在国内发展。所以我们的监

管需要进行创新,需要把监管创新和风险管理作为同等重要的目标去实施。一些比较行之有效的方案包括

1. 设置准入门槛，发放牌照。所有项目需要进行审查、公示，并且对于未完成设定目标的项目需要进行惩罚和淘汰。
2. 为了吸引海外团队回国，国家可以进行技术性补贴等政策。
3. 设置沙盒监管框架，给予项目团队在一些试点城市平台对项目提出的区块链技术和落地应用进行验证等。

二是工信部牵头建立国家级的跨学科的研究机构包括区块链，人工智能，金融，经济学，博弈学，法律，物联网，云计算，信息安全，大数据。这个机构把区块链在供应链金融，政务，能源，交通方面，食品安全的落地应用作为主要目标。一个比较优秀的榜样是人工智能。目前大量的领域研究都会涉及到人工智能。区块链技术也可以复制这种成功模式,对于各个产业所提出的无论是和区块链结合的研究结果还是应用落地都可以得到政府或者学术机构、专家的肯定。

三是护持区块链初创企业，给予政策鼓励和优惠措施。目前最具挑战的是区块链企业融资的困难。目前出海的大多

数区块链项目融资渠道都是直接通过公募或者私募,并且在交易所等场所进行交易。交易所没有一个完善的准入准则和安全保障，对于项目方和投资者是非常不利。不管我们是否承认，这种风险对于在海外成立公司，在国内运营的区块链项目确实存在。我们建议对于初创的区块链企业，设置孵化器，辅助企业融资。相对应的给予初创企业进行税收以及政策上的鼓励。

四是重视教育培养区块链与其他技术融合的综合人才。目前部分高校已经专门开设区块链课程，将区块链设置为三级学科，鼓励高校设置区块链实验室等等。此外，设置专门的培训机构进行培训，鼓励区块链教育和技术普及。对于各个行业的企业介绍推广区块链技术,将区块链技术融入不同的行业中。

中国电子学会于 1962 年成立于中国北京，拥有个人会员 10 万余以上，团体会员 600 多个，专业分会 49 家，主要具备以下三大职能：

国家级前瞻性研究智库。中国电子学会是工信智库联盟副理事长单位，负责运营国内首家由中国科协授牌的智能社会研究所。拥有一支博士和高级工程师占比 75%的近 50 人的专业研究团队，以及由两院院士、长江学者、千人计划专家、杰青、青千构成的超过 300 人的顾问团队，主要围绕数字经济、人工智能、机器人、区块链、智慧社会等前沿领域展开深入研究，为指导科技和产业发展提供了大量智力支持和决策依据。

国际化产业技术交流合作平台。学会拥有具备全球知名度和影响力的品牌化行业组织及活动，并积极承担和参与地方重点行业活动，有效促进政产学研用金在数字化、智能化相关领域的对接，提供了技术、市场、政策、人才、资金等方面大量国内外交流合作渠道和发展机遇。

政府管理服务职能重要支撑。学会在专业技术资格认证、科技成果评价与转化、团体标准研究制定、科普及人才培训等方面持续开展大量工作，卓有成效地协助政府行使科技和学术领域的管理和服务职能，很好地发挥着政、产、学、研、用等多方对接枢纽及桥梁的作用。

本文作者：黄连金
联系方式：13068783860
电子邮件：M13068783860@163.com

编 辑 部：中国电子学会 研究咨询中心
通讯地址：北京市海淀区玉渊潭南路普惠南里13号楼
邮政编码：100036
联 系 人：陈濛萌
联系电话：010-88176360
传　　真：010-68219023
网　　址：www.cie-info.org.cn
电子邮件：chenmengmeng@cie-info.org.cn 欢迎关注“CIE智库”