

江苏可信区块链

(电子月刊)

2020年第2期 总第2期



江苏省互联网协会



江苏可信区块链

苏州黑云信息科技有限公司协办

2020年4月10日

编 辑：刘湘生 于苏丰 张东风 王 锋 谢绍蕴

王梦原 葛九丽 李正豪 尹 珺 周新月

美 工：王 雪

地 址：江苏省南京市建邺区新城科技园创新综合体A区5号楼

联系电话：025-83343696

➤ 征稿启事

为搭建知识普及、行业交流、政府沟通，促进江苏区块链产业健康持续发展的平台，2020年3月10日起，江苏可信区块链专委会推出《江苏可信区块链（电子月刊）》，从行业动态、场景应用、技术交流、项目展示等多个视角介绍区块链行业发展的最新情况，现面向从事区块链的企事业单位征集在区块链场景探索、行业赋能、产业发展、技术研发、国内外动态、投融资对接等方面的稿件。欢迎从事区块链业务的企事业单位积极参与，踊跃供稿。来稿请发送邮箱：jsiaorg@126.com，联系人：李正豪，15365059600。

版权说明：

《江苏可信区块链（电子月刊）》，仅供学习参考，不涉及商业用途，内容均来自江苏省互联网协会、江苏可信区块链专委会成员单位、个人原创以及互联网转载和摘录。媒体或个人转载请注明出处和链接，否则属于侵权行为。

卷首语

抗击新冠肺炎疫情的战斗进入最后决战阶段。疫情期间，强化信息资源开放共享的区块链技术与大数据应用相结合，在排查疫情相关密切接触人员上大显身手。后疫情时代，区块链和大数据的应用将成为加速社会数字化转型、推进企业组织方式变革的重要契机。

区块链被认为是继大型机、个人电脑、互联网、移动互联网之后计算范式的第五次颠覆式创新以及下一代云计算的雏形，有望像互联网一样彻底重塑人类社会活动形态，并实现从目前的信息互联网向价值互联网的转变。

基于区块链的我国信息基础设施建设的意义不仅在于中短期的稳增长、稳就业，更在于长期的促发展、促转型：新型信息基础设施建设将为智慧经济、数字经济等绿色型、创新型经济模式奠定坚实基础，从而有效促进我国经济高质量发展。

区块链是一种全新的信息网络架构，是新一代信息基础设施的雏形，是新型的价值交换方式、分布式协同生产机制以及新型的算法经济模式的基础。它具有难以篡改、可追溯、可溯源、安全可信、异构多活、智能执行等优点，是应对疫情和经济下行的有效手段，符合产业升级要求，既代表着经济高质量发展的未来方向，也成为数字经济发展的新引擎。

在互联互通、共享协同、安全与监管中，区块链技术的应用必不可缺，起到基础性支撑作用。它是互联网的再升级，将信息传递升级为价值传递，用新技术驱动，通证驱动，数字经济驱动解决生产关系的再改造，商业模式，商业业态的再创新，迎接“可信时代”的到来。

《江苏可信区块链（电子月刊）》以“搭建政府、企业、网民沟通的桥梁”“助力政府决策，促进行业发展，服务会员需要，普及网民知识”为办刊宗旨，探索利用区块链建立可信数据的协同网络，基于协同网络实现个人业务、行政业务、金融业务等数据融合，从而对包括民生、政务服务、工商业活动在内的各种需求提供智能化响应和辅助决策，进一步对传统企业进行赋能，探索技术、资本等更多层面的战略合作，促进建立区块链产业集群，引导区块链行业健康、有序发展。打造推动人才培养、培训及成果转化，打造合作生态，挖掘需求，引导建立系统化、专业化的服务体系，搭建知识普及、行业交流、政府沟通，促进江苏区块链产业健康持续发展的平台。以场景驱动实现区块链技术的应用落地，以价值驱动推动区块链技术的普及。

相信这些内容有助于您对区块链行业有更加深入的了解，《江苏可信区块链（电子月刊）》与您共同进步。

CONTENTS

目 录

一、专家特稿	1
1.积极探索区块链技术在政务领域中的应用	1
二、复工复产	5
1.构建疫情防控信息化长城，助力江苏企业复工复产	7
2.江苏迪普思：“战疫数字员工”公益行	4
3.江苏银行供应链云平台 支持企业复工复产	4
4.苏州相城：区块链技术保障口罩公平供应、助力企业复工复产	8
5.区块链新技术为企业复工复产“保驾护航” 杭州下城“1Call链”上线	9
三、高端访谈	10
1.Moshe Vardi——科学家眼中的区块链	10
2.蔡维德——学者眼中的区块链	11
3.王嘉平——技术大拿眼中的区块链	15
4.王岳华——知名投资人眼中的区块链	18
四、专家视点	21
1.马小峰：区块链将带来消费者数据保护“革命”	21
2.于佳宁：“区块链+”未来发展需要完善的数字金融体系支撑	22
3.谢绍韞：“代码智能化”是区块链的重要发展方向	22
五、项目展示	23
1.江苏银行：区块链可信存证的应用与落地	23
2.黑云科技：区块链与人工智能的完美结合	25
3.南京翼太源：签书区块链电子证书服务平台	27
六、技术交流	29
1.三类常见跨链方案以及 Cypherium 跨链机制	29
2.Wanchain 4.0 通用跨链框架 T-Bridge	32

七、江苏动态	34
1.江苏省委书记娄勤俭：大力发展区块链等前沿产业和新业态新模式	34
2.区块链技术为江苏优质农产品写“日志”	34
3.江苏省将加快区块链等新技术研发应用	35
4.江苏常州市委书记：加强区块链、5G通信网络等互联网经济项目引进	35
5.江苏省推“文化业态创新十条”支持区块链技术在文化领域的创新应用	35
八、国内讯息	36
1.“人民链”搭建信用体系，缓解中小微企业融资难	36
2.杭州将为加快区块链、5G商用等产业布局创造有利条件	36
3.工信部谢少锋：区块链等技术在疫情防控和复工复产中发挥了重要作用	37
4.支付宝：依靠支付宝区块链等技术 消费券可实现“公平可追溯”等特点	37
5.央行持续推进法定数字货币研发	38
九、国际简讯	38
1.国际证券委员会称全球稳定币计划可能受证券法监管	38
2.意大利两所高中开始使用区块链发行文凭	39
3.Bitbank首席运营官：日本关于加密资产的修订法案将于5月生效	39
4.美国商品期货交易委员会对新冠病毒相关的加密货币欺诈发出了警告	40
5.分布科技将为加拿大开发者区块链基金会提供 WaaS 解决方案	40
十、术语解析	40

一、专家特稿

1.积极探索区块链技术在政务领域中的应用

2019年10月24日，中央政治局就区块链技术发展现状和趋势进行专题学习，习总书记在讲话中指出，要探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。这次专题学习，意味着区块链技术在我国的应用上升为国家战略；习总书记的重要论述，为区块链技术指明了新的应用场景，即由目前的跨境交易、金融创新、供应链整合等经济领域，延伸到民生需求、城市治理和政务服务等社会政策和公共服务领域。



王兴亚：江苏省城市发展研究院副院长、智慧政府建设推进中心主任、江苏可信区块链专委会特聘顾问

一、数字政务内涵及基本特征

数字政务，通常是指以新一代信息技术为支撑，以“业务数据化、数据业务化”为着力点，通过数据驱动重塑政务信息化管理架构、业务架构和组织架构，形成“用数据决策、数据服务、数据创新”的现代化治理模式。也可以表述为，政府机构借助网络等线上信息化渠道，推进政务的实施、控制、查询、评估等功能，以便公众利用数字化手段了解政府相关政策实施情况的技术手段。第44次《中国互联网络发展状况统计报告》显示，截至2019年6月，我国在线政务服务用户规模达5.09亿，占网民总数的59.6%。政务“上线”已经成为广泛认同、普遍接受的政务服务方式和模式。数字政务基本特征，可以用动态化、数据化、精准化、移动化、平台化、协同化和智能化等“七化”来描述。

二、加快建设数字政务是一个历史趋势

我国数字政务的三次迭代。近年来，现代信息技术推动传统政务服务加速向数字政务服务转型，大体上已经历三次迭代：数字政务1.0，通过Web技术将政府信息数字化，也就是电子政务；数字政务2.0，通过移动互联网技术将政府服务数字化，也就是“互联网+政务服务”；数字政务3.0，通过大数据、物联网、人工智能、区块链等现代信息技术将政府组织数字化，也就是智慧政府。数字政务是政务服务数据化、自动化、智能化、智慧化的高级阶段，是推动政府管理变革与创新的必然选择和历史趋势。

加快建设数字政务需要打通“痛点”。信息共享是建设数字政务的重要前提和基本要求。近年来，随着智慧城市建设、“互联网+政务服务”的普遍推开，我国政务领域信息公开、办事效率、民众体验等都有了长足进步，但“各自为政、条块分割、烟囱林立、信息孤岛、共享困难”等制约数字政务发展的诸多“痛点”还没有从根本上打通。

有分析认为，这些“痛点”大多不是技术问题，而是与之相应的制度机制和管理问题。在我国，政府机构或管理部门总体上还沿用着传统的管理模式和方式，“办事入口不统一、平台功能不完善、事项上网不同步、服务信息不共享”等，仍然是普遍存在的“正常”现象。3月10日，习近平总书记在武汉考察抗疫工作时强调指出，这次新冠肺炎疫情防控，是对国家治理体系和治理能力的一次大考，既有经验，也有教训。有学者认为，这次抗疫也是对我国智慧城市功能、数字政务效率等的一次大检验。3月2日，李德仁院士在“科技与产业的共振”系列公益直播讲座中，谈了他对此次疫情防控工作的一个看法。他说，这次重大疫情数据，有些在卫健委、在医院，有些在公安、人社等部门，有些在手机供应商手里，数据的开放权则在公安部门手里，这些数据没有直接连通和开放的渠道，于是才有了武汉“封城”的无奈决定。这种状况说明我国智慧城市建设还处在初期阶段，没有达到十分精细化、实时化、智能化管理的程度。

因此，加快建设数字政务，要从打通制约数字政务发展的“痛点”开始，从转变政府管理模式和方式开始，以国家治理体系和治理能力现代化总体要求为引领，科学谋划，整体推进。

三、积极探索区块链技术在政务领域中的应用

总体而言，区块链技术在各领域的应用目前还处于探索起步阶段，区块链技术推动政府管理变革还需要一个长期探索和积累的过程。当下重视区块链技术在各领域应用的态势已经明朗，我们要抢抓有利时机，按照习总书记“探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，为人民群众带来更好的政务服务体验”的指示要求，积极探索和大力推进“区块链+数字政务”建设，助力国家治理体系建设和治理能力提升。

1、区块链技术打通“痛点”的有益尝试

区块链技术的显著特性是去中心化、不可篡改、非对称加密、可追溯等，这在很大程度上契合了数字政务对于数据流通、信息共享、安全可信等方面的需求。

近年来我们已经看到，一些地方政府及相关部门在应用区块链技术推动数字政务建设方面进行了有益探索，并积累了一些成功案例。2019年10月27日“浙江日报”报道，同年6月浙江省依托浙江政务服务网上线了全国首个“区块链电子票据平台”，助推群众看病报销“最多跑一次”。2020年2月25日“区块链网”发布信息，近期全国首个“区块链政务服务平台”在重庆上线，在这个平台上注册一家公司的时间从以前十几天缩短到最快只要3天，办事效率提升5倍。2020年2月26日“人民日报海外版”发表文章《区块链应用助力疫情防控》，详细报道了区块链技术在防范新冠肺炎过程中的作用。包括

“区块链+慈善”。由多家企业联合倡议发起的一款基于区块链技术的慈善捐赠平台“善踪”，实现了捐赠流程全部上链公开，防篡改、可追溯，接受公众的监督；“区块链+政务”。上海静安区开发并使用“人员登记系统‘临小二’”，完成了全区20多个社区、688个商户及2万余人次的口罩预约、回沪登记、健康打卡、访客登记、社区关爱等服务；“区块链+生产”。武汉东湖新技术开发区的“东湖大数据复工智能管理系统”，助力实现“穿透式监管”“精细化治理”，有效帮助开发区向复工复产过渡；区块链+金融。国家外汇局跨境金融区块链服务平台试点工作范围扩大至22个省区市，平台累计完成融资放款159亿美元，服务企业近2500家，其中中小企业占比75%。此外还有：2018年10月广州开发区建设“政策公信链”区块链政策兑现平台，旨在提高政府政策兑现业务处理效率。2019年4月，北京市海淀区推出基于区块链等技术的“不动产登记+用电过户”同步办理的新举措，实现以二手房交易为主题的各项服务的联动办理。

从这些探索中，我们已经看到了区块链技术在数字政务建设中的价值与效用，看到了这方面的潜力和希望。

2、“区块链+数字政务”的实践预期

总的方向和趋势是，“区块链+数字政务”将向全方位、多层次、宽领域的流程发展，向完整程度更高的政务一站式服务方向发展，服务效率更高、成本更低、社会满意度更好。

“区块链+数字政务”办事领域拓宽。据统计，2018年，我国政务服务交通查缴、气象、人社、生活缴费、医疗、公共交通、车船票、教育、加油、出入境等，是用户量最大的前10类服务。有数字显示，其中的“区块链+数字政务”使在线查询办理交通缴罚变得方便快捷，服务了全国247个城市超5200万用户。除了交通查缴、天气查询、生活缴费等民生领域，“区块链+数字政务”已经开始向专业性更强、流程更复杂的司法、税务等垂直领域拓展。

“区块链+数字政务”办事成本降低。目前数字政务比较理想的状态，是大幅简化企业与个人办事手续，压缩社会经济体系在行政事务上的时间成本。“区块链+数字政务”将有效推动办事信息数据化和线上办理，大幅度减化办事流程，提高政务服务透明度，进而降低政务成本。

“区块链+数字政务”办事效率提升。目前政务服务的现状是，一部分事项仍需要线下办理，时间成本很高；一部分事项因为部门之间事实上存在的信息孤岛、资源共享困难等，彼此之间需要提供信息数据佐证，也加大了时间成本。“区块链+政务服务”，将进一步推动“网上办事”、“一站式服务”等，通过打造可信的政务环境，缩短政务办理手续，提高办事效率。

“区块链+数字政务”社会满意度提高。从大体上始于2018年的试点实践看，我国区块链技术在政务民生领域的应用，已经取得较好社会认同度和服务效益。第43次《中国互联网络发展状况统计报告》显示：截至2018年底，预约挂号、诉讼服务、交通缴罚、出入境、公积金、户政治安、车船票、文化场馆预约等公共服务，用户满意度均在96分以上；通过微信、支付宝城市服务平台获得政务服务的使用率达

到44%，为网民使用最多的在线政务服务方式。

“区块链+数字政务”最大预期是提升政务业务协同能力。近年来在“互联网+政务服务”和“放管服”改革的推动下，我国各级政府的政务服务水平显著提升。但跨地区、跨部门和跨层级的数据交换和信息共享还没有完成，很多政务服务面临“最后一公里”的有序衔接问题，业务协同无法发挥最大效力。区块链技术分布式数据结构，可以让所有部门都参与“记账”且数据公开透明，所有数据的交换都有迹可循，数据交换的容错率也较高，这就为建立和维系政府部门之间的信任和共识、提升业务协同能力等提供了技术条件。

3、“区块链+数字政务”面临的挑战

区块链技术作为一项新兴技术，在政务服务领域的应用，目前仍然存在一些亟需破解的难题。

技术成熟度有待提升。有分析认为，总体而言目前区块链技术系统稳定性、应用安全性、业务模式等还不够成熟。从性能上看，区块链技术还无法同时满足“高效率”“去中心化”和“安全”三项要求，高频次业务需求难以得到满足；从能耗上看，信息数据证明等共识算法，所需能耗大、成本高；从生态上看，目前缺乏相关的开发、集成和运维体系，我国在区块链开源平台上缺少话语权和影响力；从监管上看，加密技术对合法监听、客户识别、反恶意行为等监管手段带来不小挑战，多方协同治理也对监管提出更高要求。

业务基础设施有待健全。目前我国跨区域部门间的数据交互机制、共享数据库等基础准备尚未建立，一定数量的政务服务还未实现网络化电子化升级，部分政务服务即使已经电子化也没有得到大规模应用，App实际注册率并不高。

行政思维有待革新。数据共享难的最大难点在于政府部门作为天然的中心化管理机构，不太愿意接受完全去中心化的业务流程重塑。人民网曾发表评论：“若想做活政府App，使其真正成为民众生活的助手、公众舆论的容器，功夫在App之外，在于激活运营、管理、制作App的一个个政府部门，激活政府僵化的工作机制，提升政府‘以人为本’的服务意识，根本转变政府职能。”因此，未来“区块链+数字政务”能否真正实现，主要取决于政府是否愿意以及多大程度上愿意接受去中心化改造，升级新的行政思维。

四、小结：

区块链作为一项新兴技术，为数字政务服务的改革和创新打开了一扇窗。加快推动“区块链+数字政务”建设，已经成为政府管理部门及机构的普遍共识，而要真正将“区块链+数字政务”建立起来，使其发挥独特功能和效用，主要取决于两方面的努力和突破。一是区块链技术的应用创新及完善。区块链技术服务商本身要提升技术的成熟度，同时要对政务服务、系统运行、机构之间相互关系等的使用场景有深入的理解，并据此设计出务实、管用的技术业务架构和服务系统，成为数字政务坚强有力的技术支撑。二是政务服务机制与流程再造。政务机关要主动打破权责不清、各自为政、数据割据传

统模式，破除信息资源不敢分享、也不想分享等落后思维，借助区块链技术重构政务组织架构和服务流程，提升政务服务能力和效能。我们相信，利用区块链技术的共识机制和可追溯功能，我国的数字政务建设的痛点一定会被打通，适合我国管理体制和特点的数字政务机制一定会建立起来。

（投稿邮箱：jsiaorg@126.com，联系人：李正豪，15365059600）

二、复工复产

1.构建疫情防控信息化长城，助力江苏企业复工复产

江苏省面对疫情的发展和全省企业全面复工的高峰，保障疫情防控物资生产、加强复工后企业疫情防控工作任务变得越来越繁重。为保证企业防控组织和复工复产工作的有力、有序、有效，紫光软件基于江苏工信大数据支撑服务平台，利用大数据、移动互联技术，建设疫情防控专班信息系统，为江苏省工业和信息化厅成立的防控物资生产保障、企业疫情防控、防控物资协调和材料信息统筹等四个专班提供信息化支撑，助力江苏企业复工复产，构建疫情防控信息化长城。

依托该平台，相关人员通过手机可以随时随地查看即时更新的防疫政策信息，企业复工复产实时情况分析，防控物资情况的实时汇总分析，在线完成疫情防控问题的追踪和互动。

同时，基于目前全国都面临后疫情时代防控新形势，紫光软件基于自身在大数据、云计算、区块链、人工智能等新一代信息技术的积累，以及十多年丰富的行业应用经验，开发出“基于大数据的行业安全复工复产支撑平台”。该平台可以实现：

1. 依托大数据底座支撑，建立企业员工健康管理档案，并与政府大数据平台、企业行业大数据平台快速实现对接；
2. 在线完成复工复产政策推送，采集企业运营状况信息，完成产业行业经济运行以及复工指数分析，有效指导供应链上下游协同；
3. 以企业为中心，通过工业企业复工备案、复工巡查数据全景视图，构建企业员工、企业所在区域政府各部门的多级联动调控；
4. 通过物资供需对接撮合、产业行业复工指导等方式，以数据说话，以事实呈现，切实解决企业的问题、困难，提升企业的获得感。

紫光软件开发的安全复工复产支撑平台可快速与政府大数据平台、行业大数据平台实现安全对接，构建疫情防控数据围栏，助力企业复工复产有序开展，为江苏省提供持续发展的动力和政企联动保障。



平台的主要功能有：

1. 疫情防控数据围栏：

通过对企事业单位员工自身的活动轨迹，人际接触，身体健康以及对员工密切接触人员进行数据化追踪，结合企事业单位主体疫情防控措施的监控，构成安全可视可靠的数据围栏。构建安全可靠的复工复产环境和对外接触网，切断疫情传播途径，结合政府和社会防控措施，形成全面的防控体系，确保本单位无风险，提高复工率，服务大局。

2. 惠企政策精准推送：

通过对惠企政策的结构化分析，根据企业填报的各项条件，自动计算出符合企业申请的资金项目、疫情补贴减免、政策激励和扶持信息，主动推送给企业。

解决企业政策解读难的问题，同时也解决了企业需要中介协助申报的问题。构建政策智能推荐算法模型和自动学习能力，让政策真正落实到每个最需要的企业手中。

3. 政务服务秒批办理：

简化复工复产审批和条件，全程网上办理、优化审批流程，自动识别和校验身份信息，例如采用人脸识别校验身份、自动识别和校验上传证件的文本信息、自动识别银行卡信息等，完成秒批审核。同时，实现政务服务审核“无人工干预”模式减少因办公时间限制及人为审批因素导致的审批结果差异。

4. 诉求服务在线解答：

企业经过身份验证进入“诉求服务”后，随时可以找到服务空间提供的专业咨询，线上建立1V1的虚拟诉求解答室，进行全程指导。通过线上实时沟通，企业随时随地跟踪进度和掌握情况，最终解决后进行评价。

5. 复工复产一码一策：

与政府大数据平台对接，针对每个企业的登记信息生成一个特定的“二维码”，实现政府针对不同企业的“一企一策”，根据企业信息、企业上下游供应链信息、企业员工信息的动态变化情况进行快速的分类分析，协调解决好原材料供给、产品运输、员工返岗等问题，助力企业平稳安全生产。

6. 应急物资供求对接：

建立物资供求对接平台和机制，确保应急物资供应保障有序有力，帮助企业协调解决上下游协同，根据自身库存情况、加工能力构成应急事件应急物资的社会需求，通过政府的公共服务平台发布物资现货、物资加工能力、物资原材料等供应信息，形成社会协同应急的物资保障。

7. 项目申报科学有序：

实现项目申报、审批信息等无缝衔接，全流程线上操作、无接触式审批；对接各部门资源，包括法人库、电子证照库、社会信用库等数据资源，整合相关部门涉企基础数据，建立十重维度预警规则，有效防止同一项目多头重复虚假申报，实现对项目建设按区域、行业、时间等多维度的可视化综合分析；实现项目全过程跟踪管理及效益分析。

8. 社会资源一键使用：

平台建立社会资源应用入驻的模式与机制，包括云计算资源、云会议资源、云教育资源、云配送资源、云医疗资源等，一键免费开通，及时为企业随时服务、特别是市域内的企业资源和能力，真正调动一切社会力量参与到社会治理中，切实提升企业的获得感与责任心。

9. 信用监管联合奖惩：

对接信用平台数据，实现线上信用修复材料提交、申请，审批后办理信用修复手续，实现信用修复“0跑腿”。平台将收集重点防疫保障企业参与防疫相关信息，作为守信信息纳入企业信用档案，为企业获得融资信贷、财政补贴、通关便利和评先评优提供增信支持；同时，对于失信企业，平台提供开放校验接口给平台内企业，助力行业企业在生产经营活动中的防范和警惕。

10. 经济运行分析监测：

应用可视化技术、地理信息技术、数据挖掘、智能分析等手段，在不改变原有业务模式的基础上，以“后台一张表”的方式统一相关数据，逐步向“企业一套表”过渡，统一采集指标、频次、样本等数据基本要素，实现经济运行的动态描述、历史分析和在线监控。为领导决策研判提供全面、准确的数字化支撑，为行业企业提供科学的经济恢复与趋势分析报告。

2.江苏迪普思：“战疫数字员工”公益行

随着全国多省市陆续恢复企业复工复产，大多数企业将直接面临着针对于员工返程行程疫情风

险筛查防控压力，尤其针对人力资源集聚的大中型企业而言，通过有限的人工筛查手段无法实现对返程复工人员的行程风险进行实时筛查和防范。在病毒潜伏期内，一旦返程复工人员在使用公共交通工具过程中与确诊病患同行，将给企业复工生产直接带来不确定的疫情风险隐患。

作为一家勇担社会责任的金融科技新锐企业，江苏迪普思（DepthsData）科技主动作为，对于企业对返程复工人员的疫情防控重任难点痛点问题，凭借在数字员工领域的突出技术应用优势定制了一款公益“战疫数字员工”产品。据迪普思首席运营官汪祖刚介绍，通过机器人流程自动化技术可以帮助企业实现对返程复工人员的行程流动风险进行全面实时筛查、比对、跟踪、预警，形成人员流动风险筛查报告，及时发现疫情风险并调整优化防控工作，有效降低传播感染风险，同时减轻企业人力资源管理部门的工作压力，大幅提升企业疫情防控效率、减少重复劳动、降低操作风险，为打赢抗击新冠病毒肺炎疫情“没有硝烟”的阻击战做出积极贡献。

与此同时，江苏迪普思借助于江苏众享金联科技在区块链领域领先的研发实力，将“区块链+机器人流程自动化”两项硬核技术集成于“战疫数字员工”能力中，让此项战疫公益工作更科技、更高效、更安全。众享金联科技基于自身在区块链上领先的行业经验，依托上链数据可溯源的特性形成完整的、防篡改的责任链条能够完善追责机制，促使企业如实填报防疫信息，同时保证人员行程数据和筛查结果被篡改的风险，让疫情监控预警更及时。

3.江苏银行供应链云平台 支持企业复工复产

近日，江苏银行丹阳支行成功通过供应链金融云平台业务为丹阳一家企业落地1000 万元。据了解，江苏银行供应链金融云平台围绕核心企业供应链管理和资金结算，依托核心企业信用、真实贸易背景，将应收账款转化为电子支付结算和融资工具，大大提高了中小微企业融资效率。

受疫情影响，核心企业与上下游企业之间的账期延长，周转资金不足。为帮助企业盘活应收账款、加快资金周转，更好地服务实体经济，支持企业复工复产，江苏银行丹阳支行经过梳排，了解到丹阳一家企业有资金需求。

除了全力支持企业复工复产，考虑到目前业内对供应链金融、交易银行等业务的重视程度日益提高，并且该企业行业跨度大、产品定制化、施工工期长，资金垫付量较大，江苏银行丹阳支行便推荐了供应链云平台e融单业务。这项业务有签发、签收、流转、融资、清分等功能，全线上操作，供应商申请当天即可获得融资，得到了供应商的认可，也加深了企业与供应商的合作关系。

“江苏银行供应链云平台e融单业务可以恰到好处地解决企业的资金垫付问题，融资比例最高可达100%，高效又便捷，真真切切解决了中小企业融资难融资贵问题。”江苏银行丹阳支行相关业务人员介绍说，e融单是核心企业针对其应付账款开给供应商的电子付款凭证，其中约定了付款日期

和金额，到期后核心企业必须付款。e 融单对供应商而言，其付款时间确定，即核心企业必须按e 融单确定的日期和金额付款，免去了供应商催账的困扰；同时增加了融资途径，就是说供应商可根据自身资金需求向江苏银行发起融资申请，也可持有到期；此外线上融资快捷方便，所有融资操作在网上完成，半小时内到账，线上交易由江苏银行加密，安全快捷。

江苏银行供应链金融云平台是江苏银行采用大数据、区块链、物联网等前沿的金融科技手段自主研发的一站式供应链金融服务平台，使银行可以深入到产业链每一环的交易中去，大大提高了银行金融服务的效率，为供应链上下游的中小微企业提供了高效便捷的融资渠道。作为全球百强银行，江苏银行深入贯彻了国家对企业的金融扶持政策，尤其在新冠肺炎疫情的特殊时期，坚持服务实体经济，创新供应链金融等业务助力企业发展。

4.苏州相城：区块链技术保障口罩公平供应、助力企业复工复产

早前，苏州相城公证处联合苏州同济区块链研究院共同开发了全国首个“区块链公证摇号系统”。此摇号系统，利用区块链的“密码学随机算法”，对于摇号人员随机分组排序，实时公布摇号结果，不仅公开透明，还能保证结果不被人篡改，让买口罩在阳光下进行。

在相城渭塘镇，利用区块链技术开发出一款名为“战疫宝”的App，主要用于检测企业员工健康状况、监督企业抗疫防护措施。

该APP运用区块链思维，采取信息链技术开发，内设人员信息、体温测量、场所消毒、工作防护、用餐防护5个子模块。企业通过手机即可实时上传图片、视频，系统将自动记录好相关数据，所有数据保密、可追溯、不可篡改。

5.区块链新技术为企业复工复产“保驾护航” 杭州下城“1Call链”上线

近日，准备从安徽老家返杭复工的李师傅按照公司发出的通知，在“下城1Call移动办事平台”进行复工复产信息录入，并签署了一份“工地工作人员返岗承诺书”。全部录入完毕点击上传后，细心的李师傅还是不放心，他再次点击进入查看，页面显示已经通过审核可以返杭复工。而在承诺书的最上面，还多了五个字：信息已上链。

这是杭州市下城区数据资源管理局为了保证员工承诺书信息的真实性，让杭州城市大脑下城平台与区块链技术优势互补进行的探索。

三、高端访谈

导语：苏州黑云信息科技有限公司CEO谢绍韞日前就区块链的相关话题采访了不同行业的专家，请他们从各自视角出发，分享他们对区块链的看法：全球顶尖逻辑学家Moshe Vardi，分享了互联网的发展和存在的问题并给出了基于区块链的解决方案；国家特聘教授蔡伟德，从学术角度分享区块链助力中国梦的实现；技术大咖王嘉平博士，从技术角度分享区块链的核心、挑战以及中国自主创新技术在区块链领域的突破；著名投资机构德丰杰龙脉基金的投资人王岳华，分享了投资人眼中区块链行业的机遇与挑战。

1.Moshe Vardi——科学家眼中的区块链



谢绍韞：今天很高兴以主持人身份采访我们公司的顶级科学家。我看到一些杂志对互联网发展有非常多的担忧。那么这些担忧是什么？互联网存在哪些问题呢？

Moshe Vardi：第一个，互联网过于中心化。实际上开始时，互联网是一个分布的系统。美国的国防部最初想要建立的是一个有自由度并且是分布式的网络。但互联网的架构作为最关键的要素，它却是集中化的。比如，中央IP地址的数据库是由美国的Network Solutions进行维护的，我们从互联网公司获得信息的方式，也是经过两个公司来完成的，一个是谷歌，另外一个则是 Facebook。

如果我们看我们获得的信息，以及这些信息的来源，Moshe Vardi，全球顶尖逻辑学家、美国科学院、它们绝大部分是来自谷歌的检索，或者是一些发布在美国工程院、欧洲科学院、欧洲工程院等五院院士，黑云科技首席科学家。Facebook上的内容。这样的一种中心化会带来什么样的问题？万维网的概念是为我们提供信息，从世界各地都能访问任何信息，但是现在却由两个公司决定。谷歌作为一个搜索引擎，它决定了我们能够检索到的信息，有时候他们会向我们隐瞒不希望我们看到的一些信息。

第二个，互联网存在的问题是它的商业模式。我们怎么在互联网上赚钱？一开始的时候，人们认为信息是一种产品，我们会有一个信息的交易市场。但从互联网的起源看并不是这样的。

现在我们并不知道信息的价值是什么？因为没有人要求你对信息去支付费用。我们认为信息是免费的，但是并不是说，我们在为信息付费，我们看了他们的广告从而去购买相应的东西，但并没有一个公开市场来对我们的购买行为“论斤计价”。

谢绍韞：现在这种数据很大程度上都侵犯了用户隐私，那么我们要怎样去解决这些问题呢？区块链在这中间能起到作用吗？

Moshe Vardi：我们要逐渐的摆脱这种集中化，来实现一种分布式的信任。到目前为止，人们依靠可信赖的第三方，来促进我们在生活当中所开展的交易，包括银行、产权公司等等。但是我们对于这种集中化机构的信任正在下降。

在这里一种解决的方式就是区块链。区块链是一个全局可信的分布式账本协议，它并不是百分之百的安全，仍然会有一些黑客会去攻击它，但是它的弹性和恢复力是非常强的。所以我们相信基于区块链的互联网是很有潜力的。

2. 蔡维德——学者眼中的区块链



蔡维德，现任国家特聘教授、北京航空航天大学国家“千人计划”特聘教授、清华大学长江讲座教授、美国亚利桑那州立大学终身荣誉教授、英国伦敦大学学院（UCL）区块链研究中心科学顾问、赛迪区块链研究院名誉院长等职务。

谢绍韞：您认为如何把握区块链行业的话语权？

蔡维德：我认为有创新思想才有话语权，30多年前，日本提出一个第五代电脑计划，当时许多美国人认为日本的第五代电脑项目将会大大推动日本在计算机研究上的发展，如果当时日本没有提出第

五代电脑这概念，说不定过去30年来在计算机领域都不会有日本的声音，只有当自己提出一个新概念新构想时，才可能在世界舞台上有一点话语权。可以说第五代电脑计划是当时的日本梦，日本比美国更早提出这个概念，让世界重新认识日本。

谢绍韞：之前看过您的文章曾提到数字社会是中国梦，这其中存在怎样的联系，而区块链在这其中又发挥了怎样的影响？

蔡维德：第一个问题，我们说数字社会是中国梦，因为这首先会提升中国民众的医、食、住、行、育、乐环境。医：中国老百姓可以有好的医疗卫生条件；食：中国老百姓可以吃到健康营养的食物；住：中国老百姓可以住上美观舒适的房屋；行：中国老百姓可以有好的出行工具——安全快捷的飞机、火车或汽车等等；育：中国老百姓可以得到好的教育、好的就业渠道和可靠的人力资源；乐：中国老百姓可以公开获取内容健康阳光、适合自己需求的娱乐，包括电影、电视、书籍、音频和视频等。

现在人民生活水平已经有了很大提高，但教育、医疗和出行仍然是中国社会的痛点，数字社会可以让中国老百姓享受更好的东西，使人民更加安居乐业。

第二个问题，因为人类开始使用区块链共享式账本等技术，所以今天看到的商业、政务等社会上各种流程和秩序将会产生重大变化，而且金融、法律、基础设施、政府等社会生活的各个方面也将会受到影响。

谢绍韞：既然区块链对于实现中国梦如此重要，您认为中国应该如何监管区块链技术，国外有没有相关案例借鉴？

蔡维德：我建议以科技监管区块链和应用。

英、美等发达国家在对区块链如何监管的问题上经历了一个探索的过程，其中的经验和教训可供我们借鉴。

2015年，因为看到新型区块链技术极具创新性，英国率先提出沙盒监管计划。而且英国央行还发现，如果英镑以数字货币出现，会是320年来世界货币历史上最大的一次突破，这会影响到全世界。2019年，美国也认同这一观点。

为了实现沙盒监管计划，英国央行从2015年开始密集研究区块链技术。英国央行让新科技公司在特许的环境下从事实验并且给予监管指导。

目前，世界已经有50多个国家和地区实践沙盒监管，累积了许多经验。可是大家却发现这个计划有很多缺点，例如流程设计粗糙，不是设计出来监管新科技的，而仅是让监管单位学习新科技。以美国为主的监管单位和科研机构纷纷发表文章指责这一制度不合理、不科学、成效低，认为英国央行如果想学习，应该自己花钱去学习。这些缺点在2018年就已经表现得非常明显，许多国家都更改了原来的沙盒监管计划。

对此，英国也认为原来的沙盒监管有很大的进步空间，进而推出下一代沙盒计划，即全球金融创

新网络GFIN（Global Financial Innovation Network），这一计划并不实行监管，也不再发许可证给参与单位，只重视监管科技创新和国际合作，一同建立平台和进行实验。

其他国家和地区，例如澳洲、欧洲、美国也提出了不同的取代方案。美国在2018年开始启动新型监管计划，是基于产业的监管，重视以科技来评估科技，以软件工程测试的方法来评估系统，这一计划已经用在美国医药供应链管理系统上。另外联合国民航组织也使用类似方法，建立了一个国际民航区块链产业沙盒（Industry Sandbox）。

英国的下一代沙盒计划和美国的新型监管计划都具有如下特色：

第一，深度融合产业；第二，公开化、科学化、系统化评估；第三，基于产业标准。先制定产业区块链标准，再根据这样的标准建立产业沙盒；第四，商业化。沙盒以服务为出发点，扶持产业，最后还可以在产业沙盒上盈利。

如果区块链系统和应用是“矛”，这些产业沙盒就是“盾”，美国就是要让“矛”和“盾”一起发展，互相扶持，互相监督。

其实，在产业沙盒方面，中国才是第一个开发产业沙盒的国家，在2017年就开始开发泰山沙盒。泰山沙盒可以测试软件，还可以自动评估软件品质，如果软件在社区，还可以评估参与人员和追踪社区活动。自动评估系统可以比较一个项目和世界类似项目，通过这样的比较，对于项目是不是具有创新性一目了然。

除了监管，中国还需要通过法律规制区块链。我建议，在区块链相关应用、产业方面开始立法工作。现在世界一些国家已经在做了，美国、英国等使用现有法律对区块链进行解释；而瑞士则是重新立法，已于2018年12月拟出新法律框架，并在2019年补充了内容。中国需要在区块链和其应用上立法，因为区块链是不断进化的技术，所以立法也要逐步进行，首先是能够针对区块链使用和技术等进行立法，例如以法律禁止使用逃避监管的区块链和伪链，在司法、立法、执法、金融、民生、政务等方面提出对区块链的基本需求。起码先有一个比较简单的法律框架，以后在细节上再慢慢细化。重点是需要使用科技来监管科技，不能只使用法律来监管科技。

谢绍韞：那么，现在的区块链技术是否能够满足监管等需求？

蔡维德：现在的区块链技术并不能满足金融和监管需求，以前，许多人提出区块链会改变世界甚至颠覆世界，但我一直在讲，区块链要先改变自身才可能去改变世界。实际上加拿大央行在2017年的实验报告中就讲到，现在的区块链系统还达不到金融系统监管规则的要求，如何能够使用？如果连在合规市场使用区块链都有困难，又何谈颠覆现在的金融界？

加拿大央行在2017年率先使用PFMI（金融市场基础设施原则）来评估区块链系统，后来欧洲央行和日本央行也跟进使用，而PMFI是全球多个国家央行支持的标准，包括中国人民银行、美联储、法国央行、欧洲央行、英国央行等。加拿大央行、欧洲央行、日本央行评估区块链系统后都认为，现在的

区块链系统不能达到PMFI的需求，其中包括区块链可靠性与安全性，而这两个特征一直都是区块链强项。这带来一个重要的信息：许多人一直认为区块链是可靠的和安全的，可是三个国家的央行却认为现在的区块链系统不可靠，不安全。

所以“因为我使用区块链，我就改变世界”的想法只是以前区块链热衷者美好的理想，事实上，区块链技术还有很长的一段路要走。而对于目前市场上的区块链，需要实际评估。而据以往案例，很多区块链的功能和性能与实际评估的结果差距非常远。

如超级账本，这个链在2015年12月发布，被中国许多机构采纳，而2017年居然爆出超级账本是伪链，是一个不安全的链。这件事虽然在中国区块链界有大量讨论，但中国还是有支持者。2019年美国摩根大通银行出文认为超级账本不是区块链。但是这时候中国已经成为超级账本的重灾区，伪链已经在金融和公检法应用上使用。

在了解情况后，中国公检法系统表示监管这些系统必须到位。

区块链自身要改变，而不是寄望于改变监管或者评估原则。现在许多区块链评估标准，都是给区块链系统量身制作的（例如共识机制的评试），而不是从金融系统和监管需求出发。

刚才谈的产业沙盒就没有这样的问题，前面提的美国医药供应链管理系统标准就是以产业观点制定的区块链标准，这点和国内标准大不相同。

建议中国建立区块链产业标准，或者使用现有标准例如PMFI。根据这些标准，可以开始更新区块链系统设计。例如交易可回滚性及可监管性是两个必须改的重要功能。现在的数字代币，例如比特币和以太坊，都是逃避监管的，刻意设计系统让监管很难完成。监管的时候，监管单位必须快速找到相关的账户并搜寻到相关交易信息，但是比特币账户的数据结构让搜寻变得耗时。所以，这些系统设计必须更改或是换掉。交易可回滚性是现代交易系统必须有的机制，如果区块链不能支持交易回滚，就代表监管不到位。

未来，可监管的区块链才是中国应该发展的方向。账户注册的时候监管，交易前监管，交易时也监管，交易后例如清算的时候还需监管，但同时也需要政府保护，这样才不会出现风险。另外，可监管的区块链设计应和以前的区块链设计不同，中国学者应该在区块链理论上做最前沿的研究，提高创新的能力，勇敢提出新区块链模型。

3.王嘉平——技术大拿眼中的区块链



王嘉平博士，创新工场执行董事，师从全球知名人工智能科学家沈向洋博士(前微软全球执行副总裁，清华大学教授)。

谢绍韞：您认为区块链技术核心关注是什么？

王嘉平：区块链技术核心关注的是一个计算系统的自动化监管和治理。这个关注点并不是计算机系统一开始就有的。单机软件时代，整个计算系统都在用户掌控之中，此关注点则毫无意义。在互联网初期的通讯和内容分发时代，虽然计算过程已经有一部分交给了他人掌管的服务器，但是我们对计算结果和行为有确信的判断能力，或者计算结果即使背离了我们的预期，通常也无关痛痒，所以这个关注点在当时也不是什么大事。而我们现在处于社交、搜索和推荐服务时代，计算系统深刻影响着我们对世界的认知、行为的决策，甚至生存的保障。此时，这个关注点意义重大。当下两大局面决定了对一个大规模面向公众服务的计算系统的监管和治理是一个关乎国计民生的大事。

1. 用户对计算服务系统给出的结果无法有效判断其正确性和合理性，无力甄别获取到的信息是否经过了别有用心的筛选和排序。

2. 计算服务系统可以直接触及和覆盖比例很高的社会人群，并且承载了人们的社交关系、经济资产、物理身份、信誉征信等关键社会性元素。

谢绍韞：能否举个例子来看看区块链技术实现了怎样的前所未有的能力？

王嘉平：我们用一个小案例：以太坊是另一个全球性的公开区块链网络，并支持智能合约使其在区块链网络中执行逻辑可编程，部署各种第三方应用。2018年7月，以太坊网络上出现了一个游戏应用——Fomo3D，玩家众多，一时间严重阻塞了以太坊网络。这是一个典型的奖池游戏，玩家陆续以递增的价格向主办方买钥匙，所有购买资金计入一个公共的奖金池。如果一段时间内始终无人买钥匙，则游戏停止，最后一个钥匙买家赢得沉淀资金的一半，另一半资金则向之前的玩家均价回购所有的钥匙。

首轮结束时，游戏玩家瓜分了价值180万美元的以太币。最有意思的不是这个游戏本身，而是游戏执行的方式。游戏主办方完全匿名，没有任何背景可查。游戏是在一个完全没有信任背书和监管的情况下开始并执行的。一切都如期发生，之前约定的规则都被严格执行了。

且不论游戏本身是否合法合规，这样的活动要公正地开展通常需要严格的监管和治理才能保证。奖池资金需要被托管，主办方需要被监管。以现今的互联网云计算架构来实施这个项目，如果没有监管措施，最后的结果要么是游戏停止，主办方把服务器一关，卷款跑路；要么是暗中篡改上述规则，中饱私囊。现在这种以服务器/客户端为基础的互联网服务的黑箱计算模式，是阻碍互联网服务可信公正的根本症结。

谢绍韞：谈谈您对现阶段区块链技术的看法？

王嘉平：现在初级阶段的区块链技术已经在特定场景中实现监管和治理的技术化，使大家公认的规则能够可信地执行，没有人可以篡改，甚至最初制定规则、实际运营业务的人也无法在大家不认同的情况下篡改规则。前提是这些规则及其涉及到的状态，能够精准完备地被形式化、数字化，能够完全落实到计算机中的数据结构和程序代码。这是计算机技术的核心突破，而其中涉及的非对称加密技术、安全哈希、P2P网络通讯等都是实现区块链系统的技术手段，而非其技术本质。

科技进步，本质上是要提升生产力，提高效率，降低成本。而区块链技术的出现也一样，只不过效率提升的并不是计算本身，而是关乎计算背后映射的实际意义。区块链技术使得我们可以以更高的效率、更低的成本对大规模计算服务系统进行全自动的监管和治理，从而保障其背后映射的实际意义和价值不被恶意操纵和利用，同时也使制度化的监管和治理实施得更广，穿透得更深，定位得更精准。

谢绍韞：区块链发展到现阶段，你认为会面临哪些挑战？

王嘉平：区块链技术要实现更大规模的实际应用，在技术层面最大的挑战是性能和规模的提升。区块链系统本身是分布式系统的一种，和其他分布式系统一样，性能提升最大的障碍来自“分布式”这三个字。网络传输所带来的延迟和带宽限制是提升性能的第一绊脚石。为了脱离特定的物理计算设备，区块链在性能上付出了更多额外的代价。在不同的节点上间歇完成计算步骤，需要每个节点都准备好计算所需要的上下文和输入数据。在一个计算步骤完成之后，需要每一个节点都获取到最新的输出数据，并更新上下文。期间涉及到大量冗余的信息传递和存储以及相应的计算。无论设计如何优化，这些冗余的通讯、存储和计算是不可能彻底避免的。

一个区块链系统的性能瓶颈主要体现在两个方面，一个是吞吐量，另一个是状态容量。一个开放公链系统看起来有很多节点，其内存和计算能力总和是非常可观的，但是由于区块链系统要求每个节点都全量同步和构造整个网络的状态，导致每个节点实际上都在做完全重复的交易计算和状态表示。这是约束区块链系统性能的根本原因，使得全网的实际处理能力和容量等效于一台单机电脑。

吞吐量瓶颈。实际工作中的区块链节点，无时无刻不在接受全网的已确认区块以及未确认交易，

并构造成链，不断维护账簿的最新状态，然后抓紧机会尝试在链尾追加新的区块。无论采用哪种共识算法，都会历经以下几个步骤：

1. 根据账簿的最新状态，在未确认交易集合中选出若干验证合法的交易，然后构造一个新的区块；
2. 新的区块参与出块的竞争或者候选，在这个阶段，很可能会因为账簿状态更新（其他节点成功出块）而中断，回到第一步；
3. 获得出块的权力之后，向全网广播新块，更新账簿状态，回到第一步。

无论哪种共识算法，都有一个不可调和的性能矛盾，本质上由区块数据的广播延迟导致。这个矛盾使得如果每次出块比较大（可以包含更多的交易），就必须有比较长的出块间隔，以保障该区块在下次出块之前在全网被充分传播。如果传播不充分，在最终一致性共识系统中，将表现为较高的分叉率（出了无效的块），而在即时一致性共识系统中则表现为较高的失败率（区块在投票周期内拿不到2/3的同意票签名）。所以任何区块链系统都需要预先设定两个参数——块大小和出块间隔，使得在当时的网络环境中每次出块大都可以保证在下一个块出现之前完成充分的广播。这从本质上决定了一个区块链的吞吐量，其实和具体的共识算法没有太大关系，只要共识机制本身不拖后腿就行。

状态容量瓶颈。为了完成接力计算过程，每个节点都需要维持计算所需要的上下文，其中包括每个账户的状态（例如余额），以及待确认的所有交易。由于广播接力必须在新块被验证之后完成，为了保证接力过程以最快速度完成而不产生额外的广播延迟，这些信息需要常驻内存。在单链系统中，没有任何办法可以降低这个压力，无论采用什么共识算法都无法解决。这个瓶颈直接限制了全网用户量的上限，尤其在链上有很多应用的情况下。

谢绍韞：在区块链方面中国有哪些自主创新的技术突破？

王嘉平：这几年新启动的区块链系统性能提高了不少，主要得益于现在的互联网带宽的提高。这些新系统可以采用更大的块，或者更短的出块时间，轻松获得至少几十倍的性能提升。当然，这对状态容量瓶颈的改善也没什么帮助。另外，提高参与节点的要求，甚至把节点全部部署在数据中心里面，这样很容易把性能提升上去，但是完全违背了区块链本身分散执行的初衷。

从根本上提升性能的办法，是从区块链系统性能受限的根本原因入手，即现在的区块链系统无限冗余，有多少个节点参与，就有多少倍冗余。基于P2P网络的开放区块链系统，有一定程度的冗余是必要的，有助于提高系统的安全性。但是当全网有几千甚至上万节点的时候，这成千上万倍的冗余将使边际效应急速递减，着实不必要。那么是不是可以将区块链网络的全网工作量切分开来，不同部分的节点负责网络的不同部分？

这种分而治之的想法，在之前的并行计算系统中早已广泛采用，例如大数据处理中的Spark架构和MapReduce架构。同样，区块链系统也可以应用这样的思路，将全网工作量切分成多个分组，将账

簿（与内存相关）、广播的范围（与通讯相关）、交易处理（与CPU相关）、交易归档（与硬盘存储相关）这四个方面的工作量全部切分开来。然后对应地将全网节点分成不同的组，每组承担一个分组。但是如何有效安全地实现这种切分，一直是区块链系统技术中的一个难题。在区块链系统中，应用这种分而治之的思路，不仅面临切分分布式系统通常都有的挑战，例如涉及有效的数据工作流以及要牺牲一些编程的灵活性，还面临区块链系统特有的挑战，例如缺乏中心调度，以及可能削弱共识的安全性。

这个技术方向终于在2019年取得突破性进展，是由毕业于中科院计算所的两名博士完成的，发表于该年的计算机网络系统顶级会议NSDI (Networked Systems Design and Implementation)上。这篇名为“Monoxide: Scale Out Blockchain with Asynchronized Consensus Zones”的论文，以非常简洁的方式实现账户模型区块链系统的全面切分，并支持灵活的智能合约。在不引入任何中心化调度和协调的情况下，将全网切分成多个完全独立的异步并行子区块链系统，分摊全网的工作量，从本质上解决了区块链系统在性能上的两个瓶颈。论文提出了“最终原子性理论”，使得区块链系统在切分之后仍旧可以非常高效地完成业务逻辑在不同切分中的接力执行，使得整体性能实现线性提升。同时，论文还提出了“诸葛连弩挖矿”，保障了网络切分之后的安全性没有明显下降。在论文的真实互联网环境验证试验中，即使在非常保守的参数设定下，系统吞吐量高达1.16万TPS，状态容量高达16 TB。

4.王岳华——知名投资人眼中的区块链



王岳华，著名投资人，德丰杰龙脉基金（现为德鼎创新基金，德丰杰龙脉为全球著名风险投资公司德丰杰在中国境内的唯一下属基金）合伙人。

谢绍韞：您认为区块链行业存在哪些机遇与挑战？

王岳华：我从事风险投资已有十余年，在早期科技类的风险投资，特别是集成电路，医疗健康以及互联网行业都曾有过很多成功的投资案例，而在区块链这个赛道，我们也还是本着传统风险投资的视角与投资逻辑做行业研究，市场调研以及风险投资。我将简短阐述我们对区块链产业的看法以及对未来市场的趋势判断。

区块链技术正在成为多个行业的业务重点，包括生活消费、生产制造、金融服务、医疗保健、生命科学和公共部门等。短期内，区块链的价值主要是通过提高后端效率来降低成本，尤其是在金融领域。从中期来看，区块链的价值将在于扩大数字经济等领域的潜力。区块链安全、数据保存和网络功能可以独特地绕过传统的网络安全壁垒，实现数字连接世界所需的信息共享，特别是在物联网方面。长期来看，区块链的价值将受自身的几个基本特性，信任、不可篡改性、透明度和分布化的影响，从而产生新的业务模型和交易类型。影响将不仅仅体现在经济上，还将体现在文化和政治上。

当然，挑战也是并存的。比如如何提高吞吐量和性能，提高标准和互操作，降低复杂性和成本。在监管层面，如何满足法律合规支持，在产业领域如何接入实业的生态进一步落实通证体系，在商业规模方面如何真正的达成行业合作生态合作，这都是需要努力的方向。

所以在投资的机会上，我们还是会侧重在服务协议与基础设施，例如对区块链网络在性能和使用友好度提升的服务协议以及生态基础设施服务，如何在5G协议层上布一个区块链协议。在应用方面，例如场景支付、数字身份ID、信用认证、市场营销、电子商务、通讯、社交媒体、游戏、企业级应用、通证数字化，微保险以及公共事务（例如2020年的新冠病毒的公共卫生事件）等，在应用层面市场发展的机会巨大。在数字资产服务方面，例如数字资产管理系统，数字资产交易服务商，数字资产风险管理平台，数字资产对冲和托管服务等等。在监管服务层面，证券型代币投行，社区经济体，这些都是我们特别关注的领域。

谢绍韞：从投资人的角度，您是如何看待并研究区块链的？

王岳华：区块链产业是一个大的实验室。区块链产业从2008的比特币开始，一路蓬勃发展，自成一个生态，涵盖政府监管，法律，投资，投行，交易所，市值管理，企业服务解决方案，媒体社群等商业闭环，其中，在新创公司（新创区块链技术）发展方面更是快速迭代。所谓的区块链1.0，2.0，3.0，技术上的分片，侧链，跨链，应用上讲的DeFi，乃至互联网巨头发起的生态经济（如Libra）试图引领新的商业业态，这些都是“实验”。从历史上，我们也同样发现在一个新的思想，新的主义，新的产业萌芽阶段，必然伴随着一大推的实验，成功的项目在市场里留下来了，失败的只能淹没在历史的浪潮里。所以为了进一步领先行业，洞察趋势，引领市场，实验是一个必须的存在。我也不断在整个行业的发展中学习，研究，参考全球的区块链发展态势，也定了几个课题。

第一个课题是类Libra生态的研究。脸书作为一个拥有月活20多亿的社交类经济体，发起这个项目的意图以及背后所隐含的商业机会是值得思考与学习，所谓的类Libra生态，也就是在我们思考学习后，

加上本地的应用场景以及商业业态，再改造成适用于自身生态资源的项目。第二个课题是Telegram，作为全球另一个大的生态体系，并且加密的即时社交软件服务商，在2018年初开始布局公有链开放，如果我们把社群经济视为一个独立的经济体，那么Telegram可以发展的生态经济也当然值得我们关注研究。虽然美国SEC屡次认定Telegram不合规，但就如同以上所言，这是实验，寻求合规，寻求共识的最大公约数就是现实中会遇到的情况。第三个课题是监管，监管的重要性其实不言可喻，从维护国家金融秩序的维度，或从健全数字经济发展的维度，适当适度的监管都是必须的，唯有制订好游戏规则，并且在法律的保障之下，这个产业才能有序健康的发展。而监管的创新，更是代表了一个经济体在这一次革命性的经济范式出现后，能引领国计民生到哪一步，也唯有合规，才能将区块链应用引导到主流市场。第四个课题是应用，众所周知，基于区块链技术的通证经济模型，如果有广泛的社群参与，那就更加能发挥在C端的经济价值。所有的互联网巨头公司，无一不是靠流量起家，有流量的项目都有一套适合其社群的通证经济模型，无论是权益分享或是营销激励，通证在场景支付，游戏，电商，社交，IM，健康领域，微保险，金融服务，数字身份等等应用场景，都有极大的发挥空间，这里说的是通证能创造出更大的商业价值，引入更多更大的商业机会。第五个是ST，也就是所谓的证券型代币。顾名思义，这一类的通证具有证券的性质，这里的证券指的是在国家法律下赋予的证券性质。这个课题的研究其实很有趣，如何在现有的合规体系下，整一套能满足新的数字经济属性（特别是份额化以及流动性），又能够适当的阉割区块链精神（即改变所谓生产消费的关系），在理想的通证经济体系里面，没有所谓投资者，消费者一说，这两者是不可分割。但这现世的体系里，投资人与被投资项目之间的权利义务还是泾渭分明的。作为一个过度，ST的研究充满趣味。并且ST中的S属性，即大家认定的证券属性，并不是那么的唯一。例如，我们把这个S属性定义成一个商业项目的收入权益呢，也就是收入的部分比例是这个S的权益，那么从传统的财务观点就很好理解了，因为这个权益其实就是占掉部分的毛利率。第六个是基础设施协议。我们都知道科技改变未来，嫁接在5G上的区块链协议能够带来什么新的业态？另一个不只是时间戳记的分布式账本方案又能带来什么新的应用场景？基于技术上可行的分布式商业模式是否会出另现一个互联网巨头而去颠覆脸书？或是百度？这让人很兴奋。

以一个投资人的立场，我们寻找能够改变世界的梦想家，白话就是我们关注投资那些可以找到痛点，打破常规，从中重组生态链，并从其中创造而获取商业价值的项目。从以上课题里面，我看到满满的机会。

谢绍韞：您是否觉得区块链是重要的投资风口？

王岳华：作为一个常规、典型的风险投资机构，我们看重的是科技创造价值，科技改变未来。因为这个信仰，我们不需要追逐风口，这从我们2014就开始关注区块链行业项目可以得到佐证。

然而区块链作为一个协议或软件系统，如何从应用层面带来商业价值，就的确是我们专业投资机构（Smart Money）要调研的课题。这也可以从几个角度来探索。首先区块链的三大网络特性：第一，

分布式存储，数据和文件存储在不同的节点上，保证数据无法被篡改和删除。第二，分布式网络，每一合格的服务器都可成为网络中的服务节点。第三，可信数据，在运用公钥与私钥机制下，数据变得更为安全可控可管理。通过这些特性，我们认为新的商业形态、业态可以被重构。这三个特性往下深挖，我们可以轻易的理解，在存储，分布式数据，以及数据本身，就可以思考出很多的商业机会。例如大的互联网巨头彼此之间的数据是不共享的，例如数据的价值并没有回归反馈到数据提供者，再例如分布式可信技术应用在C端上的各个应用（保险，消费，内容创作，健康医疗）降低因为信任的内部以及外部摩擦成本。

区块链架构是分布式的价值网络，中心化的信息网络叠加上分布式的价值网络，商业一定会被完全、彻底重构。所以互联网仅仅是重构了商业的一部分，加上区块链可以重构的更加彻底。重构商业当中区块链带来的就是重构金融，为数字化的经济提供一整套新的金融服务体系，其中包括点对点实时的支付和清算，新的帐户体系等服务。基于区块链协议的未來商业应用当中，并不只有分布式，它应该是中心化和分布式相结合相辅相成。并且基于区块链协议的商业模式，数据是公开的、共享的，这降低了进入门槛。因此，我们鼓励创业者真真切切的了解区块链在经济上的意涵，从经济价值结合社会价值，从而找出行业痛点，行业机会乃至于创业机会。这个产业是一个真正未来的新兴战略产业。

四、专家视点

1.马小峰：区块链将带来消费者数据保护“革命”

区块链技术将首先深度嵌入消费领域的信息保护，尤其是用户与消费者的隐私保护，与信息红利相关联的交易会越来越正规。未来的世界将是一个信息化的数字世界，互联网企业过去通过泄露用户数据而获利的情况将不允许再发生。可以想象，区块链将是信息加密保护与授权的钥匙，利用信息获取收益与分得利益的情况会越来越正规化。当下在消费领域引发的许多问题归根到底都是用户身份确认和确权问题，而在引入区块链技术后，商家的数据难以篡改，在信用方面的消费会得到改变。在区块链上产生的任何交易都可以真实地记录下来，任何企业抵赖不了，这将有大量数据而目前变现困难企业的巨大利好。疫情期间，“云”办公已成为一种趋势，而这也产生了云端商业机密被盗取的风险。利用区块链技术对文档和关键信息给予保护会成为“云”办公的一大技术趋势，这种保护将为法院提供可追溯的存证。如今，区块链在线招投标的一系列流程中已经取得了初步应用，未来还会越来越多。（马小峰：同济大学区块链研究院院长）

2.于佳宁：“区块链+”未来发展需要完善的数字金融体系支撑

于佳宁认为区块链跟产业的结合发展，需要一个具体的过程，相对来说纯数字化的领域更容易去跟区块链做结合，而数字化程度稍微低一些领域，往往是要先实现数字化的转型，再去搞区块链+。区块链的四个基本发展方向，一要加快让区块链取得产业优势，增加所谓的技术创新；二是扩展区块链在各领域的应用，实际上是加快应用落地；三是保证区块链的安全；四是提高运用管理区块链技术的能力，加强制度建设和管理。这次在疫情期间区块链发挥了很大作用，主要是在促进数据共享等方面。

过去传统大企业的资金在采购商品的时候并不是直接付钱，而是会有一个账期，有一个押款，白条的一个机制，这种方式下实际上是会造成中小企业资金链的短缺。在疫情的影响下，资金短缺的这种问题会更加明显，并且企业之间商业信用可能会受损。产业链条上的某一个企业倒闭之后，会使得整个行业上资金链受重大影响。区块链如果能把所有的债权债务关系全部打通，全部上链，全部连接起来，就可以很好的实现有效的互认，实际上债务就可以在链上流转的情况下为企业之间的信用做保障，这也是区块链很好的应用。

区块链可以进一步打通创新链、应用链和价值链。创新链是新的基础设施，应用链是实际的场景应用，价值链是新的价值交换方式。区块链的逻辑是技术实现交易，交易创造公平，公平带来效率，效率达成协作。从这个角度来说，实际上区块链是一种三位一体式的创新，它是以产业应用为最终目标和价值导向，以数字金融为一个核心的动力支撑，从而实现三位一体式的创新。（于佳宁：火币大学校长）

3.谢绍蕴：“代码智能化”是区块链的重要发展方向

区块链智能合约、代码的智能化是非常重要的。如果说智能合约缺乏全局观，代码不能处理更高级语义，那么当区块链网络接收带有“攻击”的指令的时候，系统本身是无法判断出来的，它只知道指令的合格与否，却无法理解这条指令与下一指令的联系，也不明白它会对系统整体造成什么影响，所以区块链网络自己永远不知道“什么是攻击”，以太坊DOA攻击就是一个非常典型的例子。所以，代码智能化的区块链平台对于自己的整体状态认知，是清晰的，这是一个非常大的优势。我认为代码智能化是区块链行业非常重要的发展方向，这个也是我们公司在AI+区块链方向的探索与研究。（谢绍蕴：苏州黑云信息科技有限公司CEO）

五、项目展示

1.江苏银行：区块链可信存证的应用与落地

一、江苏银行区块链的发展

自2016年起，江苏银行就开始研究区块链的技术应用，是国内较早开始研究区块链的银行之一。自平台上线至今，已成功落地“票据贴现”“物联网动产质押”“OA无纸化审批”等多个业务场景，在供应链金融、互联网金融服务等方面都取得了不错的成绩，并荣获“人民银行银行业科技发展奖全国二等奖”、2019年中国物流与供应链产业“双链奖”。

随着应用的不断深入，开拓新业务场景对技术的要求逐步提高。为了支撑场景建设，实现科技赋能，江苏银行对区块链平台“苏银链”进行了全方位的升级，解决区块链固有的共性问题，打造了“苏银链2.0”。“苏银链2.0”对底层区块链技术进行了定制化改造，增加了智能合约代码安全监测，执行容器的安全加固（容器突破、命名空间、日志和审核、守护进程特权等），所有节点间通讯采用国密算法，在存储安全上，采用原子级的事务操作。同时，增加了通用接口平台，其解耦了业务系统与“苏银链2.0”平台，屏蔽了叠加业务系统对系统框架的影响，隔离了区块链与上层应用的差异，实现无差别对接。

随着场景的不断丰富，节点的不断增加以及链上数据容量的不断提升，一个便捷的运维平台变得至关重要，“苏银链管控平台”应运而生。该平台支持快速建立区块链的运行环境，提供基于区块链的搜索查询、交易提交、数据分析等一系列服务，同时也具备节点预警功能，让区块链的运维工作变得更加简单便捷。

通过“苏银链管控平台”可实现对机构、用户、通道和节点的全生命周期管理，对链上数据的直观展现，助力探索共享经济的新模式，打造数字经济产业生态，从而更好服务于各类应用场景。



二．大流量与新技术的结合

江苏银行的网贷业务蓬勃发展，与京东、唯品、支付宝等各大互联网平台均有合作，作为我行主要流量渠道的江苏银行直销银行平台也有享借、享花等贷款品牌。为提升品牌创新能力，降低贷中、贷后风险，将贷款业务场景与区块链技术相结合，打造电子合同可信存证平台。江苏银行以其直销银行做为创新技术的试验田，实现了网贷业务电子合同链上签约，在链上流转的电子合同数据进行全节点共享，确保了存证信息不可篡改，保证安全性。同时，平台还将用户在签约合同过程中的所有交互信息过程以链式结构保存在区块上，可以最大限度还原合同签约的过程。

三．基于区块链的可信存证

1. 链上验签，加盖签章

用户在江苏银行直销银行端下载CFCA证书后，通过证书签名生成合同模板，同时将用户信息上链，执行智能合约驱动用户证书的签名验证，生成防伪标识、生成电子机构印章，最终合成带客户签章且具备法律效应电子合同。全流程依靠智能合约自动执行，签章数据全节点共享，确保合同文本不可篡改，在保证信息安全的前提下提升了业务办理效能。



（电子合同签约样例）



2. 链上合同存证

通过智能合约将加盖了客户签章的合同存储在江苏银行的区块链节点上，同时也会在提供存证服务的系统上建立节点进行共识。同时对需要加盖电子印章的双方或多方的电子文件均进行哈希运算获取哈希值，加盖时间戳并提取文件摘要信息及签章用户的真实身份信息，将这些信息嵌入到区块链中，链上的各个节点都将同步这些信息，并将这些信息写入结构化数据库中，加强追溯能力，并且链上

数据防篡改，签名数据防抵赖，实现了电子合同的可信存证。

3. 链上流程驱动

智能合约实现用户引流、用户创建、贷款合同创建与签署、合同变更、放款、还款、逾期、催收、合同关闭等全流程一站式操作与上链存证、业务流转的非中心化处理平台。智能合约是区块链平台的基础，借助智能合约，可以在区块链中设置交易规则，可以使用它们自动执行验证步骤，以此来驱动合同条款的自动执行。

业务上链后，提升防篡改能力。普通存证只有加盖电子签名的电子合同不能够被篡改，其它环节产生的数据均容易篡改；降低数据丢失风险。区块链以其共识机制，保证链上全节点均保持一份完整的副本，数据的完整性得以保障；可信程度高。链上数据可追溯，智能合约公开，确保合同信息在司法举证和审计时具备可信效力；智能化程度高。使用智能合约来实现关键的流程化调度逻辑，提升自动化处理能力。

后期我们将会继续探索更多场景，“一枝独秀不是春”，当下虽然不少企业都有自己的联盟链，但只有互相联通，才能更好发挥区块链的价值。期待能在不久的将来，与更多同业的合作，打破信息孤岛，更好地提供进行金融服务，实现让科技与业务的融合发展，以金融科技赋能美好生活。

2.黑云科技：区块链与人工智能的完美结合

产品介绍：

黑云团队通过人工智能与区块链的积累，成功开发了基于区块链底层框架，独有的人工智能算法应用层相结合的四大不同应用场景的实用平台：

（1）全网内容确权追踪平台

所解决的问题：原创版权大量抄袭。数字权益缺乏源头创意保护，数字产权利益分配不均，大量盗版，抄袭现象无法得到有效解决。使得大量有原创价值的信息作者，不愿意在互联网上分享自己的信息。

优势特点：

- 基于区块链框架的数据及算法上链（版权存证）

原创数字内容实时上链，不可篡改，具有唯一标识。且所有AI分析算法通过区块链共识记录。不可篡改，实时可追踪。

- 原创度计算库

根据独有人工智能语义分析算法，可对明文/密文进行被抄袭（相似度）百分比分析，并给出各抄袭部分的原始出处路径。

- 侵权流向取证

实时追踪原创内容，被抄袭引用部分的流向，点击阅读或其他收益，并反馈于原作者。

（2）目标人物分类标签搜索平台

所解决的问题：信息查找繁琐且精确度低。信息大爆炸的今天，用户在网上搜索相关敬遵信息时会遇到大量噪音信息，需要耗用户大量时间去逐个阅读筛选，并不能在较短的时间内找到自己想要的精准内容。且大量用户隐私被侵犯出售，用户毫无隐私安全可言。

优势特点：

- 区块链算法共识框架

整个AI算法都纳入基于区块链的系统计算框架被执行，保证算法的可追溯，公开透明可信。

- 区块链底层框架，保证用户隐私不被侵犯

用户个人隐私及浏览记录不被恶意盗取及出售，无虚假广告。

- 结合统计算法，基于规则的模式

建立自然语言的句法分析模块和信息抽取模块；使用基于深度学习，建立实体识别算法，以及文档分类算法

- 通过聚类分析，对关键信息分类

构建针对人名等实体的精准索引库和关联实体数据。



（3）分布式算力激励平台

所解决的问题：大量硬件资源浪费。全球高达30%商用和企业数据中心的服务器很处于“昏睡”状态。不产生价值的同时还在耗费大量电力和维护成本。而另一边，各类互联网服务平台，需要花巨额成本去购买服务器和计算硬件，导致越来越多的商家通过售卖获取到的用户信息来抵消付出硬件成本，形成用户隐私被泄露的恶性循环。

优势特点：

- 通过区块链建立起可信的协同计算过程

建立整个基于区块的协同计算框架，公平公正的建立共享资源平台。

- 将工作流程，拆分为不同功能类型的计算工作节点

每种功能的工作节点具有不同的算力和存储要求，加入平台工作节点，可以根据自身的硬件条件来选择作为其相应类型的功能节点。

- 充分并行各运算流程

从分析处理到存储检索，分类记入账本，并设有相应贡献度模型，通过区块链记账模式公平可信的记录贡献值。例如所需计算资源可具体地体现为CPU、存储系统、带宽等不同维度性能，从而设计相对应的贡献度计算公式。

（4）全球公链可视化分析平台

所解决的问题：全球公链质量参差不齐，大量伪造虚假数据，各公链间数据孤岛，无法真实有效的统计公链的发展情况及活跃度。虚拟货币的产生，给不法分子提供了洗钱等不法行为的机会，通过对可疑账户的追踪，为监管部门提供可视化服务。

优势特点：

- 区块链算法共识框架

整个AI分析算法都纳入基于区块链的系统计算框架被执行，保证算法的可追溯，公开透明可信。

- 通过AI算法区分真实及虚假链上行为

实时追踪账户及交易动态，警示可以资金流向

3.南京翼太原:签书区块链电子证书服务平台

南京翼太原信息科技在3月上线了测试版一站式通用区块链电子证书平台：签书区块链电子证书服务平台（www.certifybook.com）。

签书区块链电子证书服务平台是一个一站式的证书服务平台，证书颁发机构可以在签书进行电子证书的设计，颁发，撤销等证书相关操作；被授予证书的个人或团体可以在签书获取证书，分享证书给需要验证的第三方；证书核验方可以在签书进行电子证书的查询，核验。

签书实现了证书的完全电子化，将“最多跑一步”提升为“一步不用跑”，同时区块链技术将实现证书的保真与多方确认，降低证书行业的信任成本。同时签书还可以支持定制化，发证机构可以根据自己的业务需求定制电子证书服务。

签书区块链平台技术架构：

签书底层采用自主研发设计的，国产可控的区块链底层平台，具有高可用性，高定制化，低成本的优势，可以根据不同发证机构的不同需求做具体的定制化操作。签书提供区块链浏览器服务，证书相关方可以在区块链浏览器上查询证书上链的具体细节，比如时间，链上哈希，区块，节点等信息。

同时，签书区块链电子证书服务平台还融合了阈值签名（Threshold Signature）和零知识证明



(Zero—Knowledge Proof)等先进技术,以实现证书在区块链上的多方“盖章”确认,同时保护相关方的隐私。

后面随着区块链的不断普及和跨链技术的完善,签书区块链电子证书平台可以作为集成服务方,与求职,招聘,比赛,会员等业务进行集成,与其他的区块链网络进行交互,提供证书相关服务,通过零知识证明等技术,实现安全保密的资格认证和数据共享。

产学研合作项目:基于区块链技术的用户用电数据管理架构研究

南京翼太源信息科技有限公司与南京工程学院能源研究院共同开展了一项合作课题:基于区块链技术的用户用电数据管理架构研究。

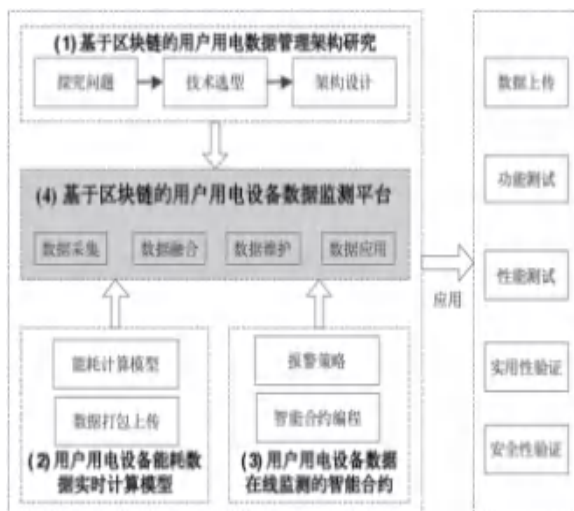
此课题是产学研前瞻性课题,旨在探讨和研究区块链技术在电力数据监控管理方面的应用,研究内容包括:

(1) 基于区块链技术的用户用电数据管理架构研究

分析现有用户用电数据管理系统存在的问题,探究引入区块链技术来管理用户用电数据的可行性;进行技术选型;根据用户用电数据管理的需求,设计基于区块链技术的用户用电数据管理架构。

(2) 用户用电设备能耗数据实时计算模型

设计能耗数据实时计算模型;研究区块链的数据结构与上传机制,将统一后的用户用电数据打包形成特定的数据区块,最终上传至区块链。



(3) 用户用电设备数据在线监测的智能合约研究

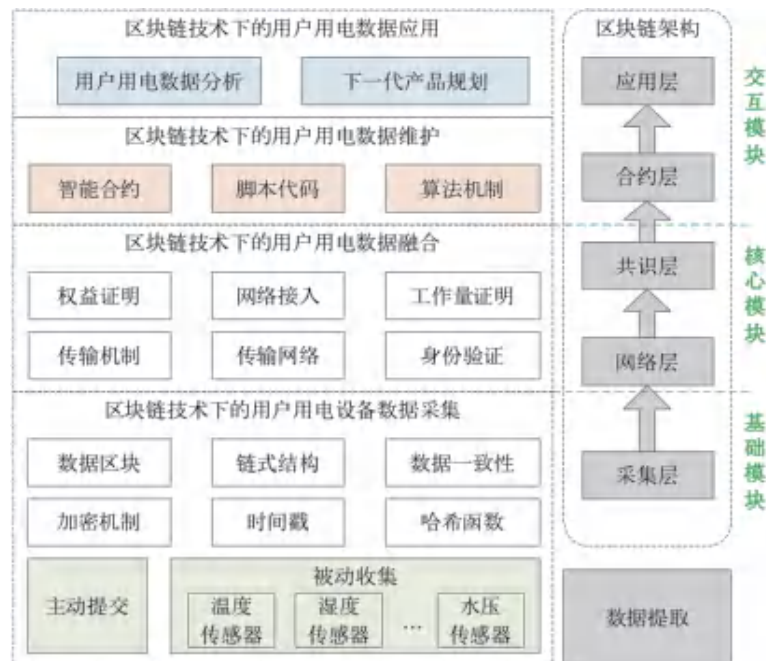
根据各设备中部件的运行数据临界值,设计不同的报警策略;将报警策略编程内嵌至区块链合约层,以满足对能耗数据计算和监控需求。

(4) 基于区块链的用户用电设备数据监测平台研发与应用

设计并研发基于区块链的用户用电设备数据监测平台,并将真实的信息数据上链,完成对平台功能和性能的测试。

项目将形成基于区块链的用户用电设备数据监测平台一套,同时专利若干。后续此项目的研究将有助于区块链在能源电力方面的落地应用。并将依托南京工程学院在电力,电网方面的深厚积累,拓展更多区块链+电力方面的场景。

基于区块链技术的用户用电数据管理架构研究（研究内容1）的研究方案如下图所示



南京翼太源信息科技有限公司是一家区块链咨询和开发公司，技术部门拥有多位从事区块链领域开发和技术研究的资深专家。公司有多年公链底层和应用开发经验，同时从2017年开始就开展区块链咨询和解决方案的业务，在联盟链的设计开发有丰富的经验。

六、技术交流

1.三类常见跨链方案以及 Cypherium 跨链机制

跨链主要是指原本存储在特定区块链上的资产可以转换成为另一条链上的资产，从而实现价值的流通。也可以将其理解为不同资产持有人之间的一种兑换行为，这个过程实际并不改变每条区块链上的价值总额。和目前交易平台提供的币币交易一样，不同类型的数字货币之间可以进行兑换，只是交易平台的币币交易是通过中心化的数据库上进行，并没有发生在区块链上。

目前跨链主要有以下三种相对成熟的方案：

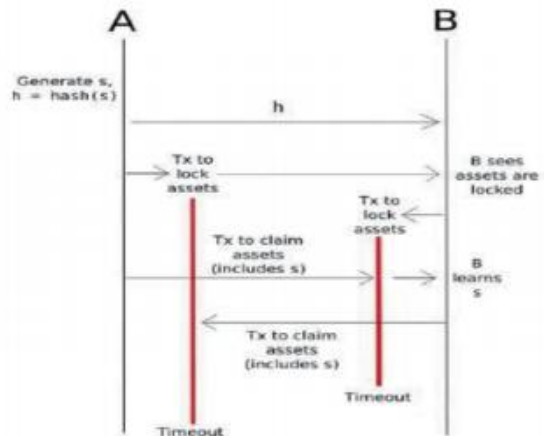
公证人机制（Notary schemes）

哈希锁定（Hash-locking）

侧链 / 中继（Sidechains/relays）

公证人机制

中心化或多重签名的见证人模式，见证人是链 A 的合法用户，负责监听链 B 的事件和状态，进而操作链 A。本质特点是完全不用关注所跨链的结构和共识特性等。假设 A 和 B 是不能进行互相信任的，那就引入 A 和 B 都能够共同信任的第三方充当公证人作为中介。这样的话，A 和 B 就间接可以互相信任。它本身不是一个账本，不寻求任何的共识。相反它提供了一个顶层加密托管系统称之为“连接者”，在这个中介机构的帮助下，不同的记账系统可以通过第三



方“连接器”或“验证器”互相自由地传输货币。记账系统无需信任“连接器”，因为该协议采用密码算法用连接器为这两个记账系统创建资金托管，当所有参与方对交易达成共识时，便可相互交易。该协议移除了交易参与者所需的信任，连接器不会丢失或窃取资金，这意味着，这种交易无需得到法律合同的保护和过多的审核，大大降低了门槛。同时，只有参与其中的记账系统才可以跟踪交易，交易的详情可隐藏起来，“验证器”是通过加密算法来运行，因此不会直接看到交易的详情。理论上，该协议可以兼容任何在线记账系统，而银行现有的记账系统只需小小的改变就能使用该协议。从而使银行之间可以无需中央对手方或代理银行就可直接交易。主要代表方案有：Interledger 协议、0x协议

哈希锁定

哈希锁定起源于闪电网络的 HTLC（Hashed TimeLock Contract），如今也使用较为广泛。它实现的过程如下：

例如使用 Hash-locking 来实现 20ETH 和 1BTC 的原子交换过程：

1. A 生成随机数 s ，并计算 $h = \text{hash}(s)$ ，将 h 发送给 B；
 2. A 生成 HTLC，超过时间设置为：2 小时，如果 2 小时内 B 猜出随机数 s ，则取走 1BTC，否则 A 取回 1BTC；这里 A 用 h 锁住 BTC 合约，同时 B 也有相同的 h 。这样 A 和 B 都有相同的锁 h ，但 A 有钥匙 s ；
 3. B 在以太坊里部署智能合约，如果有谁能在 1 小时内提供一个随机数 s ，让其 hash 值等于 h 则可以取走智能合约中 20ETH；
 4. A 调用 B 部署的智能合约提供正确的 s ，取走 20ETH；
 5. B 得知 s ，还有 1 小时时间，B 可以从容兑现 A 的 HTLC 的 1BTC。
- 一旦超时，交易失败，符合原子性。

注意：这里引入时间的参数主要是为了，一旦时间超时，当前用户可以收回自己的币。不然自己的币可能被恶意无限制锁定。

侧链 / 中继

侧链系统可以读取主链的事件和状态，即支持 SPV (Simple Payment Verificaiton)，能够验证块上 Header、merkle tree 的信息。本质特点是必须关注所跨链的结构和共识特性等。一般来说，主链不知道侧链的存在，而侧链必须要知道主链的存在；双链也不知道中继的存在，而中继必须要知道两条链。

侧链是以锚定某种原链上的代币为基础的区块链，如法币对黄金的锚定一样。该技术最初是为了解决主链扩展性问题而想出来的扩容技术，每个区块链可以通过协议来实现强制执行的共识。一个区块链系统性能能够理解其它区块链的共识系统，能够实现在获得其它区块链系统提供的锁定交易证明之后，自动释放比特币。

例如 BTC-Relay 以太坊当作比特币的侧链，与比特币通过以太坊的智能合约连接起来，依赖于 SPV 证明可以使用户在以太坊上验证比特币交易。

中继更为灵活，“中间人”仅仅充当数据收集者的角色，目标链收到发送链数据后由接收链自行验证，完成交易确认的工作。自行验证的方式依据系统结构不同而不同，主要代表有Cosmos、Polkadot，目前似乎技术方面遇到了障碍，一直未能取得实质性的进展和应用。

各方案的对比

	哈希锁定	公证人	侧链/中继
互操作性	只有交叉依赖	所有	所有(需要所有链上都有中继,否则值支持单项)
信任模型	链不会失败或者 51%攻击	多数公证人诚实	链不会失败或者 51%攻击
适用跨链交换	支持	支持	支持
适用跨链资产转移	不支持	支持(需要共同的长期公证人信任)	支持
适用跨链预言机 (Oracles)	不直接支持	支持	支持
适用跨链资产抵押	大多数支持但有难度	支持(需要长期公证人信任)	支持
实现难度	容易	中等	难
实际应用层度	主要在闪电网络得到应用	瑞波和世界 200 多个多银行使用	基本没有实际应用,还在发展中

Cypherium 采用的跨链方案

通过比较以上方案并考虑到Cypherium链自身的特点，决定采用公证人机制，也不另搞一套其他协议，准备直接采用Interledger协议，因为InterLedger协议虽然是由Ripple公司发起并主导，但是它是一个开放式协议，任何公司或个人都可以参与共同开发并免费使用，它不和任何区块链进行挂接，它的初衷是建立一个全球统一支付标准。它像是一个专用于连接的组件，专注于连接各类账本的支付标准、统一协议。其支持通信对象不仅包括了区块链，还包括了各类账本（通常为各个银行内部账本系统），各类账本通过去信任的第三方“连接器”来互相连接。InterLedger 协议是哈希锁定的实现模式。在这个系统中，两个不同记账系统可以通过第三方“连接器”或“验证”机器来互相自由地传输货币。记账系统无需去信任“连接器”，因为该协议采用密码算法为这两个记账系统和连接器创建资金托管，当所有参与方对资金量达成共识时，便可相互交易，跨账本的资金流动马上原子性发生。并且只有参与交易记账系统才可以跟踪交易，交易详情可隐藏起来，“验证器”是通过加密算法来运行，因此不会直接看到交易详情。这种方式特别适应于现有的银行系统，银行不喜欢用别人机器来验证他们交易，简单来说就是不喜欢公开处理方式或半公开处理方式，因为这两种方式都可能会给外人窥视他们内部数据机会。

2.Wanchain 4.0 通用跨链框架 T-Bridge

Wanchain的宗旨是要解决棘手的区块链互操作性（通常也称为跨链）问题。当前，越来越多的公链和联盟链问世，实现链与链之间的互跨便成了当务之急。然而，有相当数量的区块链是属于异构链，因此，跨链的问题变得十分复杂。因为，如果两条链属于异构链，那就意味着这两条链的技术架构如共识机制、智能合约语言等是大不相同的。

随着区块链在全球范围内获得人们的认可以及众多企业和机构开始采用区块链技术，人们就会日益产生这样的需求，要把越来越多的资产搬到链上，但前提是这些现实世界的各类资产要符合各地各部门的监管要求。在这样的大背景和趋势下，Wanchain 4.0和T-Bridge框架恰恰满足了这一现实需求。这是全球首个也是目前为止唯一一个解决公链与联盟链之间的互操作性问题的框架协议。

Wanchain 4.0的核心是T-Bridge框架，它是通用跨链框架，是包含模块化组件和一系列协议的参考体系架构。这些模块化组件和协议与当前跨链集成公链的Wanchain Storeman跨链机制相兼容。T-Bridge框架将原链、目标链和路由链组件链接在一起，并且定义了一系列的标准组件协议用于跨链交易（CCT）。本文将从技术上讨论T-Bridge框架。

T-Bridge 框架的内涵

T-Bridge框架是一个标准化的通用框架，它让区块链之间的资产交换和数据交换成为可能。

标准化。T-Bridge框架是根据形式化方法的规范所进行的标准化制定。采用逻辑一致的语言来正式描述框架规范。该语言允许在不同计算机环境和区块链网络中实施。

通用性。T-Bridge框架能够适用于任何具备智能合约能力的区块链，而不必拘泥于链的底层技术，如共识机制、智能合约语言等。这也意味着T-Bridge框架允许公链与公链间、联盟链与联盟链间、公链与联盟链间的相互链接。

资产和数据。T-Bridge框架不仅允许资产在不同链间的自由流转（如当前Wanchain已经实现的比特币、以太坊、EOS以及以太坊和EOS上的生态代币间的跨链交易），而且还允许数据在不同链间的共享。这样就能创建复杂的具备跨链能力的去中心化应用，即一条链上的交易可以由另一条链上的事件触发产生。

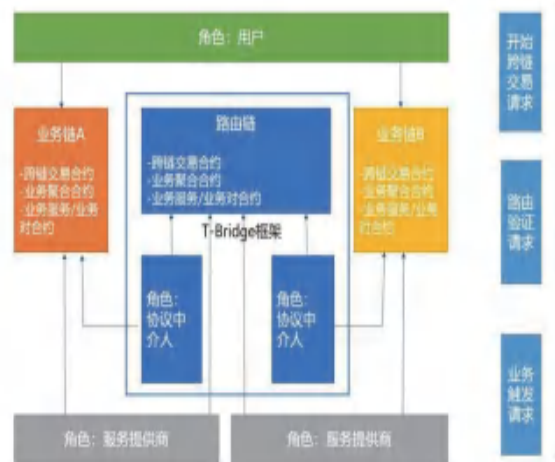
T-Bridge 框架的工作原理

以下是 T-Bridge 框架工作原理的简化描述：

T-Bridge框架允许不同链上的用户和服务提供商分别与各自链上的智能合约交互从而参与跨链交易。扮演中间角色的路由链（Route Chain）则进行与跨链交易有关信息的注册和同步。协议中介人（Protocol Mediator）则监视不同链的状态，他们能够根据原链上发生的事件而在目标链上进行交易（协议中介人的角色与当前跨链节点 Storeman Node 相似）。

核心概念和角色的定义：

层	描述	组件
应用层	为角色提供具有跨链能力的应用服务或业务服务	T-Bridge浏览器 协议中介人门户 钱包客户端 业务服务
SDK层	具备跨链能力的SDK，部署便捷	T-Bridge SDK 离线SDK 在线SDK
合约层	跨链交易合约和业务合约	跨链交易合约 业务合约
协议中介人服务层	在链间侦听和执行交易	协议中介人服务
链代理层	用于不同区块链间的通信	链代理服务
区块链层	不同区块链网络	区块链节点



路由链：路由链是 T-Bridge 框架内业务链之间进行跨链交易的连接枢纽。

业务链：业务链参与跨链交易提供相关的服务或资源。

协议中介人：协议中介人在路由链和业务链间提供跨链交易机制。协议中介人侦听来自原链的信息并执行相应的跨链交易请求。

服务提供商：服务提供商提供跨链交易中涉及的服务或资源。

用户：用户通过发起交易进行跨链资源或服务的交换。

跨链交易合约：跨链交易合约为 T-Bridge 框架提供各类基础功能，如跨链注册机制、受支持

的信任模型、基本跨链交易信息等。

业务合约：业务合约提供必要的其他服务，是对核心跨链交易合约的补充。

T-Bridge 框架的技术栈介绍

万维链研发团队为说明用途，提供了如下可参考的技术栈：

核上图是对技术栈的抽象描述，图中并未明确具体的技术和实施细节。实施细节会因项目的不同而不同。万维链团队当前正在开发T-Bridge 的概念原型（PoC），该概念原型将Wanchain作为路由链和业务链，并将HyperLedger 的Besu作为另一条待连接的业务链。链代理（Chain Agents）的链上查询数据通过MongoDB进行存储，链服务（Chain Services）是对链代理的补充和增强，用于与区块链进行通信，从而允许协议中介人查询区块链信息并发送区块交易。（朱正明：北京大学数学学院本科和硕士，万维链研发总监）

七、江苏动态

1.江苏省委书记娄勤俭：大力发展区块链等前沿产业和新业态新模式 培育新增长点

据新华日报消息，3月13日，江苏省委书记娄勤俭发表署名文章《疫情防控不松劲 推动发展再加力》，文章表示，这次疫情对整个产业结构、组织方式带来了深刻变化，我们要主动适应，加快转型，大力发展人工智能、区块链、云计算、大数据、边缘计算等前沿产业和新业态新模式，谋划储备加快推进“新基建”项目，大力培育新增长点。

2.区块链技术为江苏优质农产品写“日志”

据新华网22日报道，近日，南京六合小麦种植户夏兆宏正通过农业区块链小程序上传了自家农田的照片和管理步骤，10分钟后，他便收到江苏艾津农业科技服务有限公司研究院副院长李志杰发来的意见。眼下，利用区块链技术对农产品进行记录溯源、综合管理已在江苏开展探索运行，从而为生产者、消费者、监管者带来利好，已成为区块链技术落地的又一有效场景。

3.江苏区块链技术为抗疫防疫提供支撑

南京金宁汇科技有限公司充分运用区块链技术，第一时间投入到防疫抗疫援助工作中，基于区块链技术的构建可信环境、不易篡改、可追溯等特性，搭建了应急物资协同平台与慈善基金管理平台，依托两个平台，高效、精准地开展为湖北地区筹集、捐助物资的工作。

利用区块链网络创新技术建设的应急物资协同平台，建立了物资供应商和受助医院的点到点渠道，加快流转速度，减少物资二次分配，提高物资到位效率，切实保证一线人员物资供给。

慈善基金管理平台利用区块链技术实现捐款及物资的全程可信追溯，为每笔捐款生成唯一且包含由捐赠信息生成的哈希值的捐赠证书上链保存，作为该笔捐款后续全程追踪的唯一标识，让捐赠者的捐助行为永远记录在区块链网络中。平台强化了对捐款的监督，捐款转化成医疗物资及调拨、发放等全过程上链，提高了募捐行为的公信力，让群众参与募捐更为安心和放心。

4.江苏省级农产品质量追溯平台已实现省、市、县追溯系统数据互联

为了给消费者“看得见的信任”，江苏省级农产品质量追溯平台已实现省、市、县追溯系统数据互联。这一平台将逐渐实现全省农产品质量追溯信息“一张网”管理。江苏省农业科学院农产品质量安全与营养研究所的系统研发负责人卞立平说，“基于区块链的去中心化、共识信任机制，可为农产品的产供销打造全新的安全信任体系，能够有效保障农产品的品质和安全。”这套农产品质量安全溯源系统，和适用于农业生产加工型企业的品质安全管控智能系统相结合，能够完整采集到农产品从生产、运输到消费者餐桌的全过程信息，解决数据造假的核心痛点，并帮助企业提高生产管理水平，实现信息化转型。

5.江苏省推“文化业态创新十条” 支持区块链技术在文化领域的创新应用

据新华日报报道，3月5日，江苏省委宣传部、省科技厅、省财政厅、省文旅厅、省广播电视局联合发布《关于应对新冠肺炎疫情影响推动文化业态创新的政策措施》。该政策措施分为促进文化科技融合、优化文化供给结构、加强载体平台建设、完善服务保障体系4部分共10条。此次十条政策措施颇具针对性，如“支持共性关键技术攻关”，明确提出支持5G、人工智能、大数据、云计算、物联网、区块链等共性关键技术在文化领域的创新应用，省重点研发计划、省重大科技成果转化专项等省级科技计划将对文化科技创新项目给予倾斜支持。

八、国内讯息

1. “人民链”搭建信用体系，缓解中小微企业融资难

据人民网3月25日消息，近日，人民网舆情数据中心/人民在线开放“人民链”信用体系，旨在为中小微企业融资提供风控、增信、供应链金融等“一站式”服务。“人民链”信用体系通过整合平台服务，打通金融服务绿色通道，向企业提供精准、高效、低成本的金融服务。

据悉，“人民链”信用体系由人民云企、人民企信、人民金服等平台构成。在实际场景中，中小微企业接入人民云企平台，可以实现查询舆情数据、经营、工商、司法、行业、宏观政策等信息，从而及时发现企业自身、产业链上下游和行业潜在风险；人民企信为中小微企业和金融机构搭建线上撮合平台，企业自主授权共享自身数据，打破银企信息不对称现状，借助全行业数据，建立金融机构和企业的信任关系；在人民金服平台，核心企业接入该平台后，其链属的上下游企业可凭借与核心企业的真实贸易凭据，在人民金服平台上直接发起融资需求，金融机构在该平台受理需求，并实现金融贷款发放。

2. 杭州将为加快区块链、5G商用等产业布局创造有利条件

杭州城市大脑建设将有法制支撑。日前，浙江日报记者从杭州有关部门了解到，制定有关城市大脑赋能城市治理的地方性法规，已列入今年杭州市人大常委会重点立法项目。杭州将疫情防控视为倒逼提升城市治理能力的重大契机，持续深化城市大脑应用，强化数字赋能城市治理，为打造“全国数字治理第一城”注入强大动能。

杭州干部群众和企业界人士表示，要把总书记对浙江提出的新目标新定位转化为工作干劲，坚定不移推进城市治理体系和治理能力现代化，继续探索创新，进一步挖掘城市发展潜力，加快建设智慧城市，为全国创造更多可推广的经验。

高标准、高起点建设政务数据共享体系，加快打造“移动办事之城”。杭州深化“最多跑一次”改革，建设全市统一、多级互联的政务数据共享体系，建成办事材料共享库等六大数据库，已实现全市68个单位的数据汇聚。依托把数据送到“大厅”“网上”“掌上”“链上”优势，杭州以群众为中心促进行政服务大厅的“去中心化”。接下来，杭州将尝试引入社会资本拓展部署

综合自助机，聚焦“异地通办”服务长三角一体化，打造服务长三角的“移动办事之城”。

中枢系统+部门（区、县、市）平台+数字驾驶舱+应用场景，杭州已基本构建城市大脑核心架构，建成148个数字驾驶舱和48个应用场景。在此基础上，杭州将持续推进数字与治理融合创新，以深化城市大脑应用为突破口，不断拓展健康码、“亲清在线”等应用场景，将应急治理效能固化为常态治理机制。

通过部门协同，再造政企服务流程，杭州“亲清在线”平台打破以往“企业申报、政府审批、层层拨付”的流程，实现了一键兑付，加快兑现100亿元防疫补助。加速统筹各行业各领域数字化建设应用，杭州城市大脑建设定下时间表：到2020年底，城管、医疗、房管、安监、市场监管等领域系统建成投用；到2022年，实现城管等领域应用全市全覆盖，亚运、旅游、环保、消防等领域系统建设全面完成并投入使用。杭州市数据资源管理局副局长吕钢锋说，充分运用新技术，整合各部门、区（县、市）、社会的数据，杭州将通过城市大脑实现业务协同、数据协同、政企协同，满足便民直达、惠企直达等各种场景需求。

争取在新型基础设施建设上先行一步、走在前列。杭州将为加快大数据、区块链、5G商用等产业布局创造有利条件，依托城市大脑打造若干个新基建产业群，积极培育新的经济增长点，形成新的竞争优势，以“新基建”为契机全面提升经济运行和城市治理数字化水平。

3.工信部谢少锋：区块链等技术在疫情防控和复工复产中发挥了重要作用

据财联社3月25日消息，工业和信息化部信息技术发展司司长谢少锋表示，这次应对新冠肺炎疫情以及复工复产工作中，我们之所以取得令世人瞩目的成效，其中一个重要的原因就是我们采用了科学的方法，成功地应用了新技术，其中互联网、大数据、人工智能、区块链等新一代信息技术，在此次疫情防控和复工复产中发挥了重要的作用。

4.支付宝：依靠支付宝区块链等技术 消费券可实现“公平可追溯”等特点

据证券日报3月26日消息，据不完全统计，3月份以来已有超过10个省市推出了消费券等鼓励性政策。而各家支付机构正在积极配合，为其提供技术支持和应用渠道。支付宝方面表示，依靠支付宝的实名认证、区块链、风控等技术，消费券可实现“一城一策、按需定制”、“灵活可调整”、“公平可追溯”等特点。

5.央行持续推进法定数字货币研发

中国人民银行2020年全国货币金银和安全保卫工作电视电话会议近日在京召开。会议就2020年重点工作作出部署，提出要坚定不移推进法定数字货币研发，系统推进现金发行和回笼体系改革，加快推进钞票处理业务、发行库守卫和发行基金押运转型。

据介绍，新冠肺炎疫情发生以来，货币金银和安全保卫系统强化现金供应和流通管理，全力保障现金供应和使用安全。下一步，货金、保卫工作要切实提高服务实体经济、服务高质量发展的能力，尤其是准确研判现金供应总量的能力、多层次满足现金需求结构性差异的能力和数字经济条件下现金服务的适应能力，持续推动业务转型。

会议透露，今年将组织实施普通纪念币市场化发行，打造便利整洁安全和谐的现金流通环境，完善齐抓共管的反假货币工作机制，促进货币史研究与非标金银清查工作，加强对钱币市场的引导和管理。此外，还将稳步推进大额现金管理试点，全面提升内部管理水平。

九、国际简讯

1.国际证券委员会称全球稳定币计划可能受证券法监管

据CoinDesk消息，一份新的报告显示，国际证券委员会（IOSCO）认为，全球稳定币计划可能会受到证券法的监管。据悉，IOSCO研究了由公司治理委员会管理的假想稳定币，该稳定币由一篮子全球储备货币支持，并以自己的私有区块链为基础。它只能发行给买卖稳定币的“授权参与者”，并且可以在用户的数字钱包之间传递。该报告没有提及任何具体的稳定币名称（尽管该示例看起来很像Facebook领导的Libra项目）。从其假设分析来看，IOSCO发现该计划可能属于证券监管机构的职权范围。

2.意大利两所高中开始使用区块链发行文凭

两所意大利高中将开始使用以太坊的区块链公共技术发行不可篡改且易于共享的数字文凭。据报道，该措施旨在使整个发行和可追溯过程透明化，但最重要的是，要解决该国长期存在的问

题：假文凭。

打击伪造文凭的发放

罗马高中学院院长Maria Chiara Sidori关于这项倡议说：“该项目可以通过允许大学和公司验证任何候选人声称的资格的真实性的真实性，来消除与其他机构的信息不对称。”

这种技术还将使教育机构能够公证有关学生及其所修课程的所有信息，从而为他们提供个性化的跟进服务，而不必担心注册表会被更改。Sidori认为，该建议将有助于加强涉及教师和学生之间不断反馈的现有教学方法，因为这将使流程实时标准化。

受冠状病毒大流行影响学校的区块链解决方案

这一消息是在冠状病毒爆发引起的全球紧急情况之际发布的。意大利已成为大流行的新中心，截至发稿时，死亡人数超过1,000。正如先前报道的那样，基于区块链的教育技术提供商Odem宣布为受冠状病毒感染的意大利学校和大学推出了一个平台。

3. 罗马尼亚参与欧洲区块链技术研发项目

据罗马尼亚非政府组织“Spherik加速器”宣布，其将与另外4个欧洲伙伴联合启动“欧洲B节点”项目（B-Hub for Europe），该项目将基于欧洲市场已有潜力，推动区块链领域创新。该计划于2020年1月启动，为期2年，总预算近190万欧元。

该项目的5个合作伙伴分别为意大利、德国、法国、立陶宛、罗马尼亚。意大利罗马的Innova公司担任项目协调员，它们将共同助力欧洲区块链技术市场的发展。

“欧洲B节点”项目是由欧盟“欧洲初创”（Startup Europe）框架下的“欧盟地平线ICT33”所提出的46个动议中的6个中标项目之一。该项目的主要目标是：致力于为欧洲的区块链创建有利的监管框架；教育目标受众并提高其对区块链技术潜力及其可能应用的认识；有助于增加对技术的兴趣，并为使用区块链的项目创造新的机会来获取公共采购以及其他特定资源；增强区块链初创企业与私营部门之间的互动，增强其潜力并促进协作；监控区块链初创企业生态系统的增长并发掘人才和技术成果。

“欧洲B节点”项目将涵盖150多家创业公司，涉及2500余人，其中50家初创公司将获得指导，加快对目标市场的影响，300余人将参与提高技术知名度的研讨会，项目将选择最多25家初创公司参加5个生态系统的欧洲之旅，将有60个公共及私人组织、40个初创公司角逐区块链最佳实践案例。

4.美国商品期货交易委员会对新冠病毒相关的加密货币欺诈发出了警告

据Cointelegraph 3月23日消息，美国商品期货交易委员会(CFTC)警告公众警惕利用人们对新冠病毒的普遍担忧来进行的加密货币诈骗。CFTC在3月19日发布的一份声明中强调，欺诈者通常利用新冠病毒的传播等重大新闻事件，为他们的骗局增加可信度或操纵情绪。根据声明，该机构已收到数百起涉及在线数字资产或与外汇相关的欺诈性计划的欺诈投诉，这些承诺将在日益严重的冠状病毒问题中带来快速而巨大的回报。CFTC进一步指出，冠状病毒诈骗者不仅会在欺骗人们时将钱投入到假投资计划中，欺诈者还要求为兑现和纳税支付不必要的费用。

5.分布科技将为加拿大开发者区块链基金会提供 WaaS 解决方案

Onchain分布科技宣布将为加拿大开发者区块链基金会（CDBF）提供定制化数字资产解决方案，提供定制化数字资产钱包解决方案（WaaS）包括资金流入、归集到管理分发。CDBF表示将采用Onchain WaaS作为其唯一的数字资产管理系统，并表示双方后续将会在资产增值服务开展更多合作。分布科技称其Onchain WaaS采用了自主研发Trustless安全服务架构、全步骤电子签名以及FIPS 140-2 level4“最高加密标准”的三重安全防御机制。CDBF是2016年成立的加拿大本土基金会，由一群热爱区块链开发技术的人员组成，核心成员来自加拿大多个知名高校和企业，总部位于加拿大首府渥太华。据Block123.com显示，Onchain（分布科技）是一家中国的区块链底层技术公司，公司成立于2016年，提供区块链技术、金融科技创新与行业解决方案，获得来自复星、红杉（中国）机构投资，连续4年获得KPMG评选的中国金融科技50强。

十、术语解析

什么是区块链？

从科技层面来看，区块链涉及数学、密码学、互联网和计算机编程等很多科学技术问题。从应用视角来看，简单来说，区块链是一个分布式的共享账本和数据库，具有去中心化、不可篡改、全程留痕、可以追溯、集体维护、公开透明等特点。这些特点保证了区块链的“诚实”与“透明”，为区块链创造信任奠定基础。而区块链丰富的应用场景，基本上都基于区块链能够解决信息不对称

问题，实现多个主体之间的协作信任与一致行动。

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链（Blockchain），是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

比特币白皮书英文原版其实并未出现blockchain一词，而是使用的chain of blocks。最早的比特币白皮书中文翻译版中，将chain of blocks翻译成了区块链。这是“区块链”这一中文词最早的出现时间。

公有链

公有链（Public Block Chains）是指：世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。公有区块链是最早的区块链，也是应用最广泛的区块链，各大bitcoins系列的虚拟数字货币均基于公有区块链，世界上有且仅有一条该币种对应的区块链。

联盟链

联盟链（Consortium Block Chains）：由某个群体内部指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定（预选节点参与共识过程），其他接入节点可以参与交易，但不过问记账过程（本质上还是托管记账，只是变成分布式记账，预选节点的多少，如何决定每个块的记账者成为该区块链的主要风险点），其他任何人可以通过该区块链开放的API进行限定查询。

私有链

私有链（Private Block Chains）：仅仅使用区块链的总账技术进行记账，可以是一个公司，也可以是个人，独享该区块链的写入权限，本链与其他的分布式存储方案没有太大区别。传统金融都是想实验尝试私有区块链，而公链的应用例如bitcoin已经工业化，私链的应用产品还在摸索当中。

去中心化

区块链技术不依赖额外的第三方管理机构或硬件设施，没有中心管制，除了自成一体的区块链本身，通过分布式核算和存储，各个节点实现了信息自我验证、传递和管理。去中心化是区块链最突出最本质的特征。

开放性

区块链技术基础是开源的，除了交易各方的私有信息被加密外，区块链的数据对所有人开放，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。

独立性

基于协商一致的规范和协议(类似比特币采用的哈希算法等各种数学算法)，整个区块链系统不依赖其他第三方，所有节点能够在系统内自动安全地验证、交换数据，不需要任何人为的干预。

安全性

只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据，这使区块链本身变得相对安全，避免了主观人为的数据变更。

匿名性

除非有法律规范要求，单从技术上来讲，各区块节点的身份信息不需要公开或验证，信息传递可以匿名进行。

架构特征

一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。



江苏省互联网协会



江苏可信区块链

搭建政府、企业、网民沟通的桥梁
提供政府决策
促进行业发展
服务企业需要
普及网民知识

