浙江大学软件学院区块链研究中心

浙江大学软件学院区块链研究中心课题组是浙江大学区块链方向主要的科研团队，早在2016就开始相关研究工作，是国内最早从事区块链领域教学、科研和产业化工作的团队之一。团队在陈纯院士领衔下，已经成为全国区块链研究、人才培养、技术创新的高地。

中共中央政治局于2019年10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调：“区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。”陈纯院士就以上问题作了讲解，并谈了意见与建议。

课题组在联盟区块链核心技术与区块链监管等领域国内外领先，承担国家区块链技术战略规划重大问题研究报告及多项省部级区块链发展规划编写任务，通过突破共识算法、安全隐私等关键瓶颈，为国产自主可控联盟区块链平台提供支撑（在中国银联等各大型机构的技术测评中均名列第一），技术成果服务于中央网信办、中国人民银行、住建部、市监局、四大国有银行等政府及企事业单位，并与杭州趣链科技、华为、阿里等顶级企业开展合作，提供人才与智力支持。

研究中心负责人蔡亮教授（博士生导师）是浙江大学软件学院副院长、浙江大学区块链研究中心常务副主任、浙江省区块链技术研究院常务副院长，同时兼任中国计算机学会区块链专业委员会副主任、全国区块链和分布式记账技术标准化技术委员会副秘书长。蔡亮教授担任了2019年10月24日中央政治局学习区块链材料的编写组专家，也是全国网信系统学习贯彻党的十九届四中全会精神宣讲团的特邀专家。先后参与了IEEE、中央网信办、工信部、中国人民银行、国家卫健委等多家权威机构的信息化标准制定，是我国区块链领域著名专家。

课题组致力于研究区块链前沿理论与关键技术、应用落地方案及产业规划，特别是与物联网、人工智能等前沿技术融合创新，并通过产学研合作推动科研成果快速落地。

研究中心专注于区块链前沿技术探索及区块链应用落地实践，主要研究方向包括联盟区块链关键技术与应用研发、区块链监管技术、智能合约开发和维护、区块链与新兴技术融合研究、区块链安全等。

方向一：区块链关键技术与应用

研究国产、自主、可控的区块链底层关键技术平台，并以此为基础面向政务、金融、军工、能源、医疗等领域研发新型分布式商业应用系统，为未来数字化社会和下一代价值互联网提供可信技术支撑。重点研究鲁棒性高效共识、节点与数据的动态恢复、高性能智能合约执行引擎、链上链下隐私安全保护、智能合约安全验证等区块链关键技术，以及基于区块链的数据基础服务平台、政务数据共享平台、信用评价体系、危化品监管等典型应用。

方向二：区块链监管技术

研究区块链智能管理与自治机制、以链治链技术体系、内容监管检测技术、跨链监管技术等。重点研究区块链网络信息监管体系、政务信息数据互联以及区块链网络传播内容影响。针对区块链主要应用领域，重点识别、关注、分析具有内容分发、即时通信等传播属性的区块链服务，甄选其中具代表性的作为重点监管的对象。

方向三：智能合约开发和维护

智能合约是一种在区块链上运行的应用或程序。智能合约具有中心化、去信任、可编程、不可篡改等特性，因此其开发和维护成为一大难题。该方向主要利用人工智能（深度学习、知识图谱等）、数据科学、程序分析、智能化软件工程等技术分析智能合约代码及其相关软件制品，构建各类智能化软件系统和工具，帮助开发人员提高生成效率。主要研究内容包括：（1）智能合约相关的缺陷和漏洞检测和修复；（2）智能合约代码搜索和 API 推荐；（3）利用众包知识的智能合约演化分析；(4)智能合约监管技术；（5）智能合约文档自动生成。

方向四：区块链与新兴技术融合研究

研究区块链与人工智能、大数据等相互赋能，扩展区块链计算能力，实现区块链自学习动态演化，形成具有智能感知能力和自主自治能力的更安全、高效、节能的区块链理论体系。研究区块链与物联网、5G、边缘计算的有机融合，有效促进领域聚焦、能力聚集，突破现有理论瓶颈，创新新型计算范式与协作模式。面向智能制造、工业互联网等产业融合应用，开展高性能、低成本、低功耗、集成化、轻量化、微型化的智能终端、

海量异构信息可信采集、异构终端高效可信协同计算、面向工业控制等重点领域的新型网络体系架构等理论研究。

方向五： 区块链安全

浙江大学网安中心区块链团队在区块链技术理论与应用研究方面起步较早、已积累了大量的研究成果。在共识协议方面，针对常见基于工作量证明（PoW）的共识算法弊端（如挖矿导致的能源消耗等），提出不可区分的零知识证明与工作量证明协议，相关成果发表于密码学旗舰会议 ASIACRYPT 2016；提出基于可信硬件的联盟链共识协议，研究成果发表于计算机系统领域顶级期刊 IEEE Transaction on Computers 上。在区块链安全方面，开发针对以太坊的区块链数字货币盗取攻击捕获系统，捕获了来自世界各地的 100 个攻击者，相关成果发表在 RAID 2019；在现有系统适应性改造方面，提出了一种支持群体管理和去中心化协同决策的区块链项目管理系统，该系统是第一个可证明安全的区块链分布式决策系统，相关工作发表在安全顶会 NDSS 2019，该系统目前被包括 Cardano（世界排名前 10 的区块链平台）、Horizon、Ethereum Classic 在内的多家大型区块链平台所使用。

实验室拟招生方向与研究项目：

一、区块链关键技术与应用

二、区块链监管技术

三、智能合约开发和维护

四、区块链与新兴技术融合研究

五、区块链安全

附：软件学院招生意向表

导师姓名	杨小虎、蔡亮、尹可挺、李启雷、梁秀波、王强、朱小军	邮箱	yinkt@zju.edu.cn
联系电话	0571-87953244	招生人数	35
提供实习起薪（元）		是否有宁波合作或发展意向	是
项目介绍	包括四个方向： 1. 区块链关键技术与应用 2. 区块链监管技术 3. 智能合约开发和维护 4. 区块链与新兴技术融合研究		
实习岗位情况	1. 区块链算法工程师：区块链底层协议及算法的研发与优化； 2. 区块链安全工程师：区块链平台底层系统安全框架设计与研发，智能合约形式化验证及安全评测系统设计与研发； 3. 区块链应用开发工程师：基于区块链平台的应用研发； 4. 区块链测试开发工程师：区块链平台及应用安全、性能、稳定性测试与调优； 5. 区块链产品经理：在熟悉区块链技术体系基础上，结合业务场景，完成区块链产品的需求整理、原型设计等工作。		
对学生的要求	1. 掌握扎实的数据结构和算法基础； 2. 对底层区块链技术有浓厚的兴趣，有志于长期从事区块链技术研发工作； 3. 熟悉至少一种编程语言（C/C++,Java, GO 等）； 4. 具有较好的文献检索阅读能力； 5. 逻辑能力强、思维活跃，接受新事物能力强，有较强的学习和自我驱动能力； 加分项： 有论文、专利等知识产权发表经历或相关项目经验		

导师姓名	任奎、周亚金、张秉晟、吴磊、刘健	邮箱	liujian2411@zju.edu.cn
联系电话	13439771175	招生人数	20
提供实习起薪 （元）		是否有宁波合作或发展意向	是
项目介绍	方向为区块链安全： ● 高效的共识协议与分片技术。 ● 基于区块链的联邦学习。 ● 区块链智能合约安全平台。 ● 区块链系统性能优化关键技术研究。		
实习岗位情况	1. 区块链安全工程师：区块链的安全加固与漏洞检测 2. 区块链应用开发工程师：基于区块链的应用开发 3. 区块链测试开发工程师：区块链平台及应用安全、性能、稳定性测试与调试。		
对学生的要求	1. 熟悉至少一种编程语言（C/C++， Java， Go）； 2. 了解网络编程，熟悉 socket 的使用； 3. 了解并行并发编程； 4. 了解机器学习与人工智能的相关知识； 5. 对知识图谱、Elastic Search 有一定基础的同学优先； 6. 对系统优化方法有一定基础和经验的同学优先。		