区块链技术发展现状与展望

斯雪明
中国计算机学会区块链专委会 主任
复旦大学区块链联合技术创新中心主任

[1] 概述

[2] 区块链关键技术发展现状与现实挑战

[3] 区块链技术发展趋势与展望

[4] 对加快区块链技术发展的若干思考

［1］概　　述

概述

在区块链研发投入与政策支持方面，国内外发展情况各异

国外发展程度不同，欧盟投入力度大，美国产业政策推动较慢，亚太地区（日本、韩国等）表现活跃

FOREIGN

- 【欧盟】2018年2月成立欧洲区块链观察论坛
  - 在Horizon2020投入500万欧元作为研发基金
- 预计三年内（2018-2020）投资达3.4亿欧元

DOMESTIC

- 在区块链领域已颁布多份相关支持文件、政策
- 基础理论研究方面仍较薄弱，技术独立自主性不强
- 多数具备部署能力的基础平台是由国外机构提出、推广
- 依赖已有系统基础，缺乏完全拥有核心技术的能力

概述

区块链关键技术研究方面，国外技术强国领先国内发展

以美国为代表的科技强国，在区块链前沿领域的探索十分活跃

相较于科技强国，国内区块链关键技术突破尚不足，技术核心竞争力较弱

FOREIGN

- 网络与信息安全领域的国际顶级会议上，以美国为首的科技强国占据主导地位
- 【专利方面】截止至2019年7月，全球区块链专利申请数目达1.8万项
- 【科技论文方面】（Web of Science数据），近五年美国发表相关SCI论文730篇，英、国、澳、意、加、南非、印七国合计发表相关SCI论文1267篇

DOMESTIC

- 同期中国专利申请数目为全球总数的一半
- 同期中国发表相关SCI论文843篇（其中2018-2019年间发表607篇）
- 国内能充分发挥区块链优势的落地应用比较少

概述

在区块链技术融合方面，国外应用强调落地能力，国内区块链产业融合关注度较高，实际落地仍面临挑战

国外主流的技术强国对区块链的应用都有明确的落地方向，许多基于区块链的应用已经实现落地应用

FOREIGN

- 美四大银行已实现基于区块链技术的理财服务业务
- 韩国以金融为切入点探索区块链应用
- 以太坊基金会、Hyperledger社区等不断创新区块链技术，有力促进技术的迭代发展
- 英、加的央行在研究本国央行的法定数字货币，澳、新等国暂不考虑，而俄、瑞典、立陶宛等国计划推

DOMESTIC

- 区块链+的概念得到了社会的广泛关注，但实际应用的部署存在诸多困难
- 许多技术融合尚处在预研阶段，在许多应用场景尚难实现有效支撑
- 区块链技术常涉及多方共治，需有政府的支持政策

概述

在区块链人才培养方面，国内外主要集中在高等教育领域

由于技术门槛较高，区块链人才匮乏、课程设计等问题是国内外在人才培养方面共有的问题

FOREIGN

- 区块链技术培训的课程选择较少，在Coursera可搜课程数量仅为46个

DOMESTIC

- 目前在高等教育体系鲜有独立专业设置，具备培养区块链人才的高等教育机构有限
- 教师培养体系不完善，教师队伍规模小
- 技能培训不足，社会培训资源良莠不齐，急需补充专业培训教育力量

区块链自主创新能力有待加强

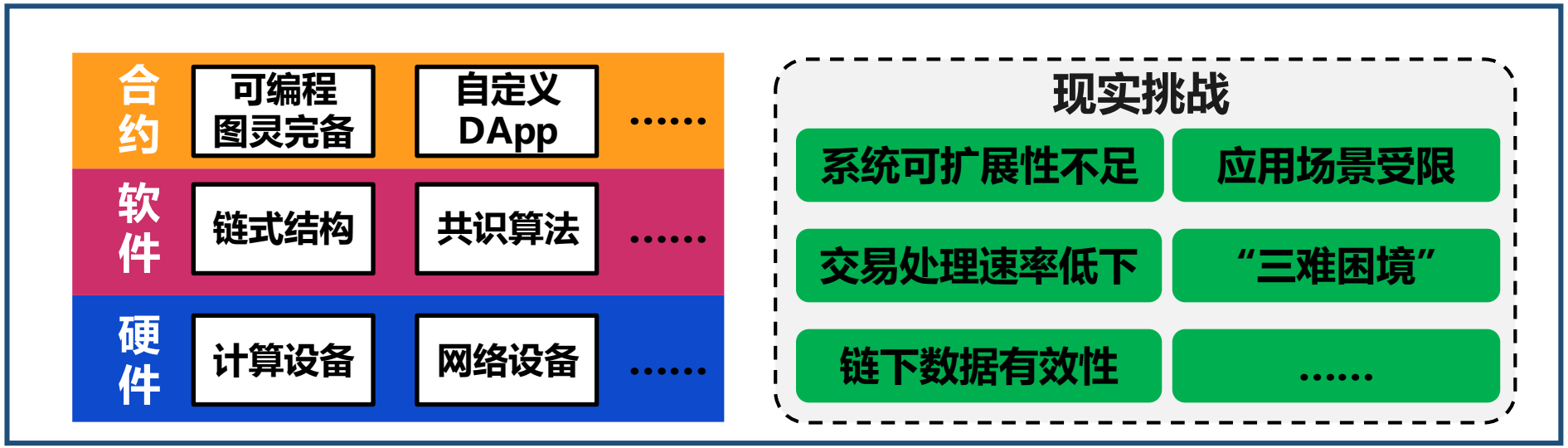
关键技术突破存在短板

区块链技术与其它前沿信息技术融合不够

高端人才、复合型人才严重不足

[2] 区块链关键技术发展现状与现实挑战

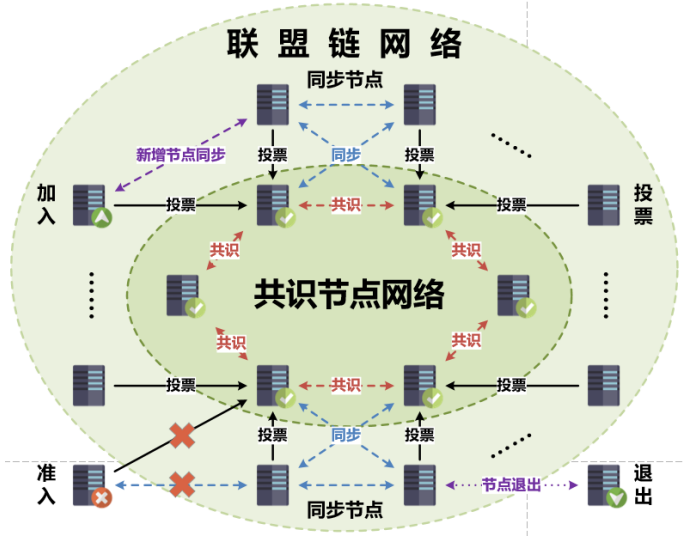
经典区块链体系架构


合约
可编程
图灵完备
自定义
DApp
……
软件
链式结构
共识算法
……
硬件
计算设备
网络设备
……
现实挑战
系统可扩展性不足
应用场景受限
交易处理速率低下
“三难困境”
链下数据有效性
……

区块链技术发展现状　　共识机制

共识机制是区块链系统能够稳定、可靠运行的核心关键技术。众多地理位置分散、信任关系薄弱的区块链节点通过共识机制维持一致性的可信数据副本，保证系统稳定运行。

现有共识机制分类



- ▶ 选举类共识（PBFT, Paxos, Raft ）
- ▶ 证明类共识（PoW, PoS ）
- ▶ 随机类共识（ Algorand, PoET ）
- ▶ 联盟类共识（DPoS）
- ▶ 混合类共识（PoW+PoS, DPoS+BFT）

面临挑战

- ➢ 性能需求与分散性需求的矛盾
- ➢ 数据公开与隐私保护的矛盾
- ➢ 数据不可篡改与监管需求的矛盾

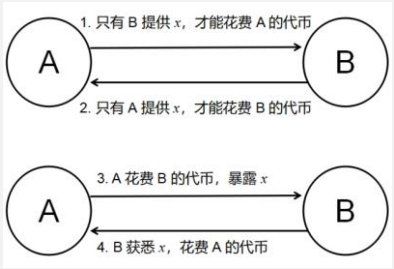
区块链技术发展现状

互操作性

区块链的发展与完善打破了同一场景下不同参与方之间的价值孤岛，但是现有区块链系统的不同设计使得价值在不同行业、不同场景下仍然难以流通，区块链互操作成为实现最终价值流通的必要途径。

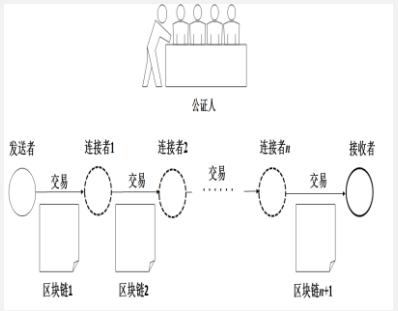
当前研究成果

原子交换技术



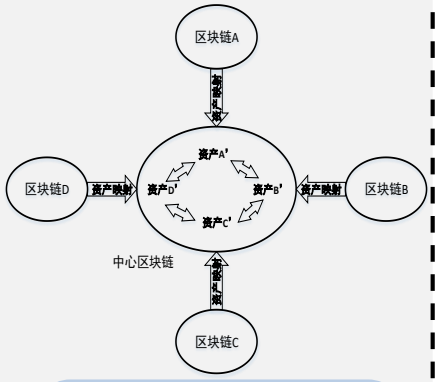
仅能用于代币交换，应用可扩展性有限

公证人技术



需要特定的公证人群体，带来安全隐患

分布式私钥控制技术



仅能用于代币交换，应用可拓展性有限

侧链技术

一对一侧链技术

一对一设计，应用可扩展性差

星型侧链技术

一对一设计，应用可扩展性差

区块链技术发展现状

安全性

任何违背区块链安全定义的行为均可归结为从算法安全层面、协议安全层面、实现安全层面、使用安全层面和系统安全层面进行的破坏、更改和泄露。

安全层次	技术现状
系统安全	严格的用户、员工培训
使用安全	密钥管理，权限管理
实现安全	智能合约形式化验证 底层代码自动化审计
协议安全	安全的网络通信协议 可靠的共识激励机制
协议安全	自主可控、抗量子攻击的 密码学算法

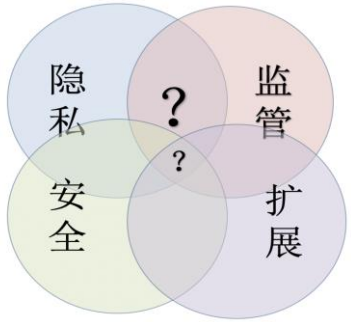
隐私定义

身份隐私：用户身份信息和区块链地址之间的关联关系，身份隐私需要保证攻击者无法将区块链上的地址对应到用户的真实身份

交易隐私：区块链中存储的交易记录和交易记录背后的知识，交易隐私需要保证用户在交易过程中的敏感数据不能够被攻击者窃取

现实挑战

- 区块链监管与隐私之间的权衡
- 隐私方案对应架构的部署难度及鲁棒性
- 隐私保护方案对性能本身的影响



技术现状：区块链上的隐私保护

交易混淆

混币方案操作简单、适用性广，在区块链数字货币中应用广泛，有很多改进方案，主要包括基于中心节点和去中心化的混币方法两种，如中心化混币服务有Bitlaunder等，去中心化混币方法有Coinjoin等机制

网络防御

通过网络防御的手段，来增加攻击者搜集数据的难度，例如限制网络接入的方式，对联盟链节点进行授权控制；节点之间的黑名单机制阻止恶意节点继续搜集敏感信息；混淆网络层数据，让攻击者无法获取真实IP，从而无法从网络层面分析用户的行为和地理位置。

数据加密

加密是隐私保护的常用方案，可确保只有持有秘钥的用户能够阅读数据。为不失区块链本身的可靠性基础，目前区块链中采用加密技术保证节点可以在加密数据上完成交易验证任务，同时尽量减少加密机制对验证效率的影响

区块链技术发展现状　　可监管性

技术现状：研究区块链地址的反匿名

国外研究成果

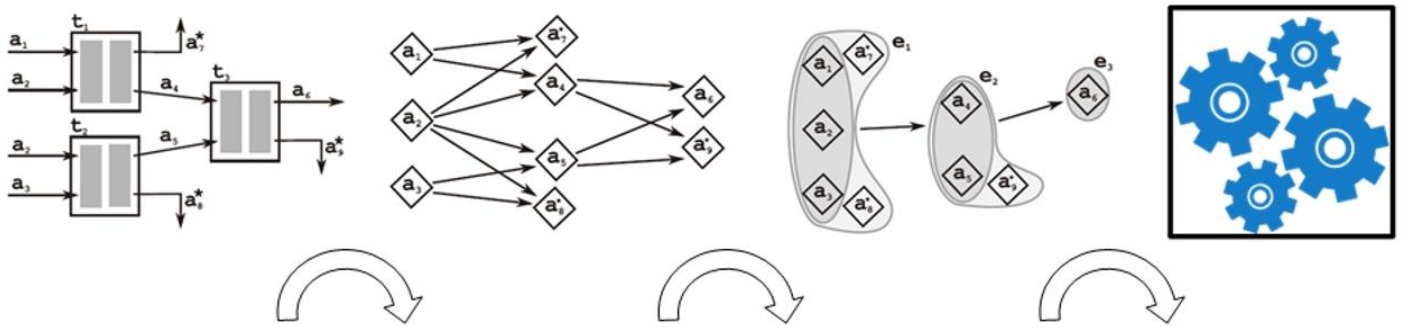
通过监听比特币交易传播信息，推测始发交易节点的IP地址

利用地址聚类技术，结合公开信息，实现Zcash中违法犯罪行为的监管

国内研究成果

基于启发式聚类规则，将可能属于同一用户的所有比特币地址进行聚类

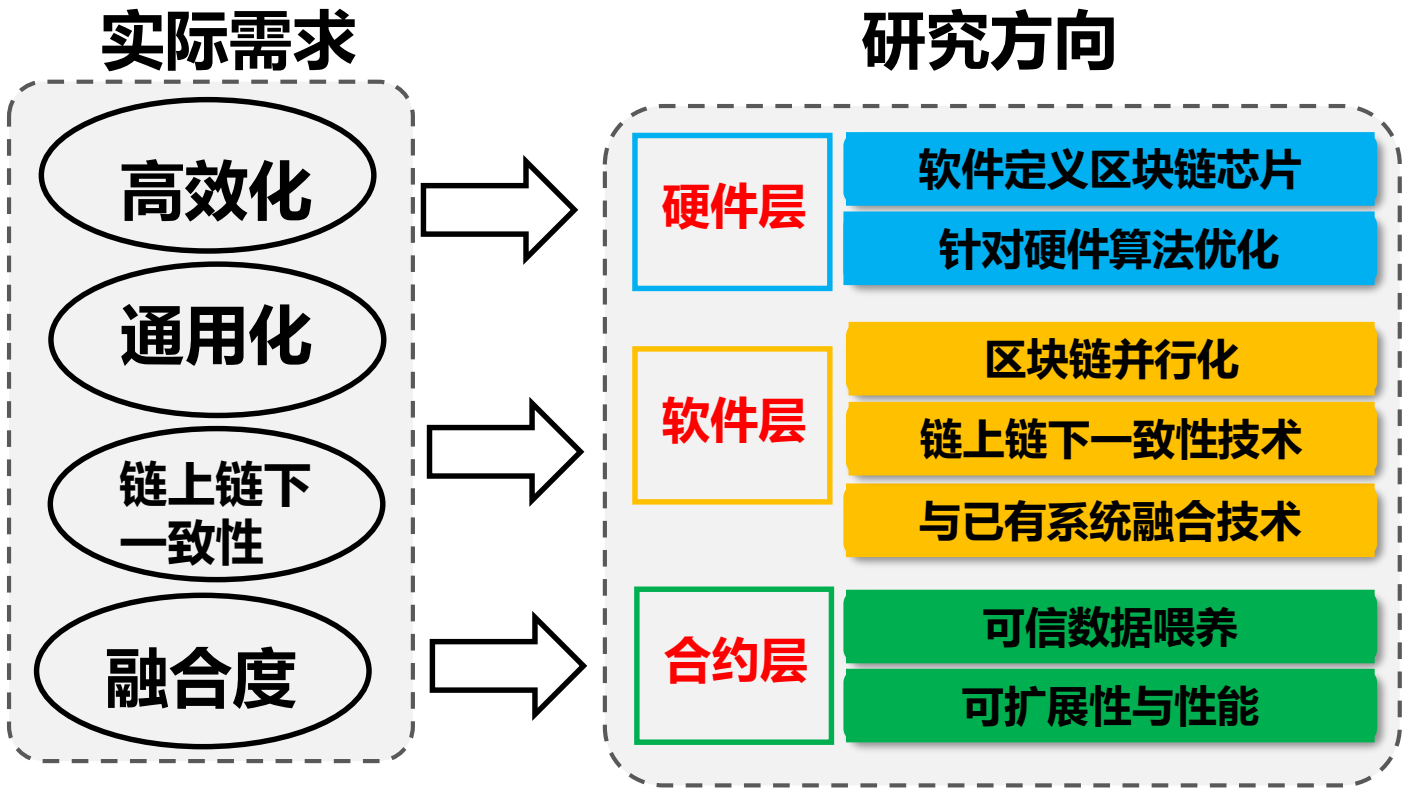
提出了一种轻量级比特币交易溯源机制，可用于区块链监管的场景中



图：区块链地址的反匿名

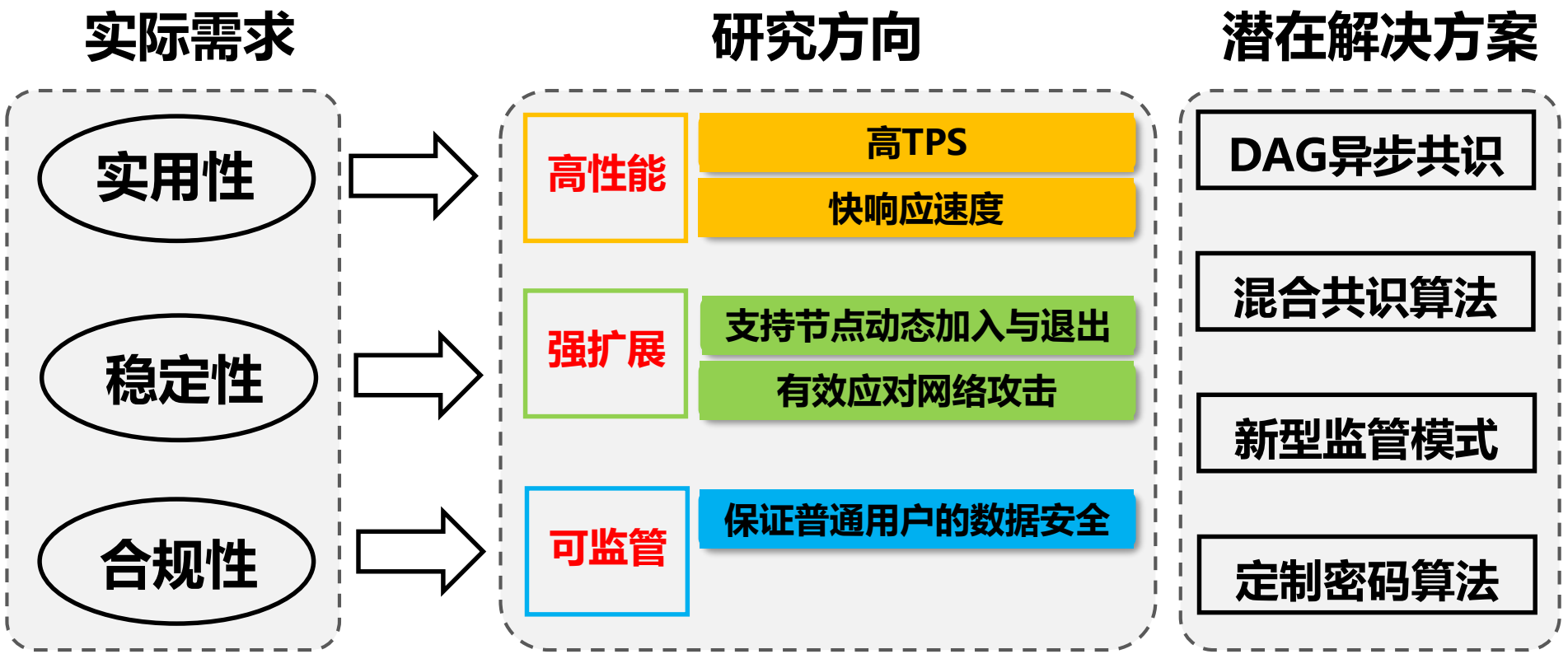
[3] 区块链技术发展趋势与展望

国内外对区块链系统架构的探索仍处于起步阶段



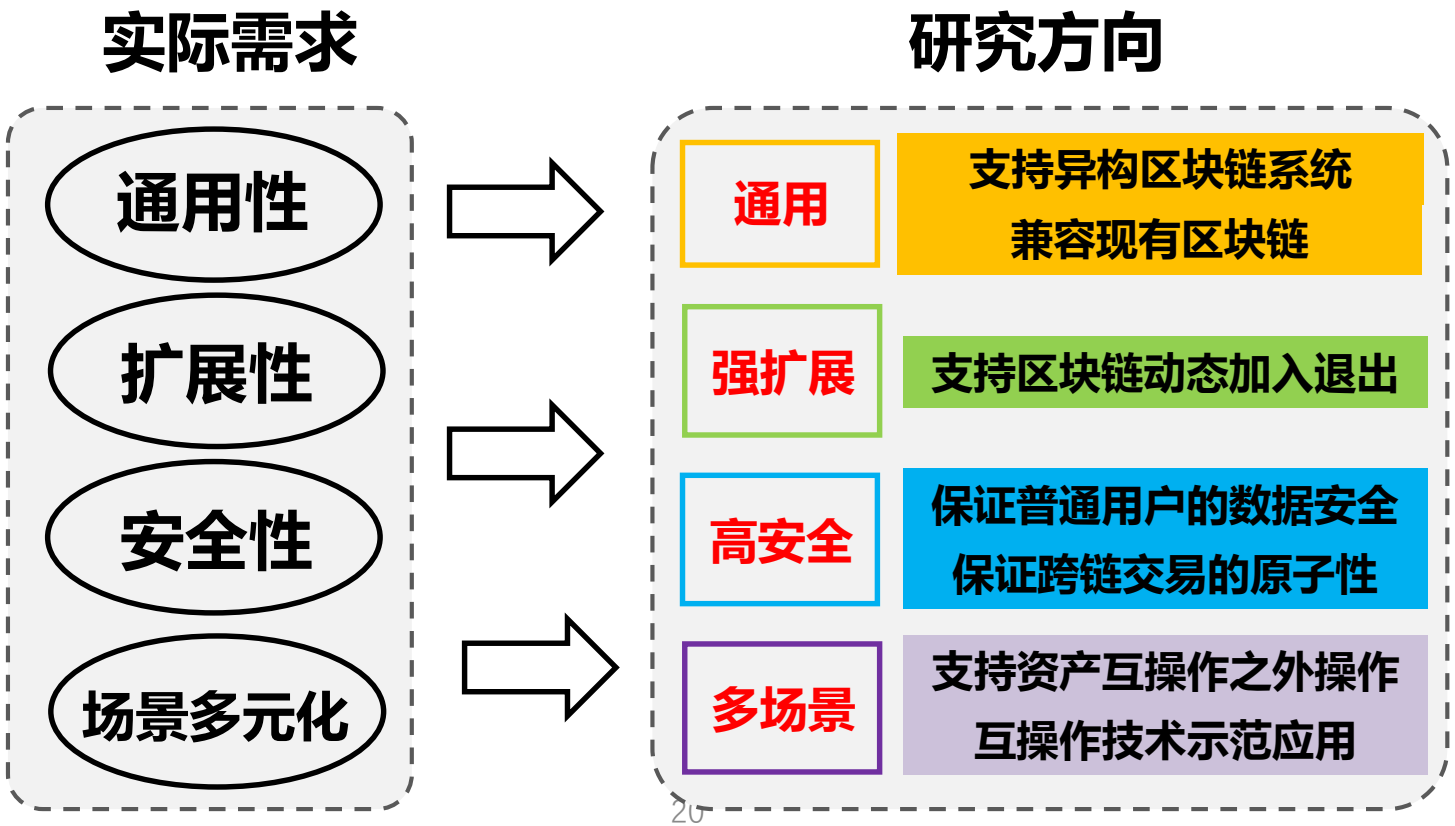
共识机制

现有的共识机制在性能、扩展性、安全性方面均存在一定缺陷，难以满足实际场景的需求。未来区块链共识算法的研究方向将主要侧重于共识机制的性能提升、安全性提升和新型区块链架构下的共识机制创新。



互操作性

目前进行的区块链互操作技术研究在安全性、通用性、扩展性等方面存在不足，且场景单一。未来区块链互操作的研究方向将侧重于系统架构的通用性、扩展性，系统的安全性以及场景的多元化。



安全性

目前技术演进阶段	下一步研究方向
分层安全：针对不同安全层面，分别提出解决方案	总体安全：综合考虑区块链系统总体架构，并结合外界安全形势，提出成体系的解决方案
被动防御：安全问题出现后，采取弥补措施	主动防御：区块链系统依据环境变化，自适应选择安全策略

隐私保护

	目前技术演进阶段	下一步研究方向
公有链	公有链目前主要通过混淆、加密等方式保证匿名性，但是性能仍然是较大问题	需要对交易数据、地址、身份等敏感信息进行保护，同时又能让记账节点验证交易的合法性
联盟链	对于联盟链而言，可通过CA方式审计并限制节点的接入，确保联盟内节点的可信	联盟链在构建隐私保护方案的同时，需考虑可监管性/授权追踪等因素，适应监管要求

区块链技术发展趋势与展望　　可监管性

	目前技术演进阶段	下一步演进方向
公有链	对公有链的监测刚刚处于起步阶段，研究方向不全面，检测技术也不成熟	加强对公有链监测技术的研究，实现对公有链交易、数据、内容的全面监测
联盟链	当前的联盟链架构中并未设计专门的监管节点，无法满足监管方的监管需求	研究监管友好的联盟链基础架构，在保护隐私的前提下实现对联盟链的监管需求

- 对区块链的监管成为了当前区块链领域亟待解决的问题，也成为了当前区块链项目落地的最大挑战。
- 需要加强对区块链监管技术的研究，只有这样才能够保证区块链行业的健康和可持续发展。

[4] 对加快区块链技术发展的若干思考

➢ 对区块链技术本质的思考

- **公有链---信任的机器**
- **联盟链---？？？**

一、大力发展自主创新区块链基础理论与技术

二、坚持应用驱动、问题导向

三、积极探索区块链体系结构创新

四、深入开展应用技术创新研究

五、加强区块链技术与其它技术的融合

六、加大区块链技术人才培养力度

谢 谢