CAICT 中国信通院

全球区块链标准现状与发展趋势

2018年7月

01 全球区块链标准生态

区块链在开源世界中蓬勃发展

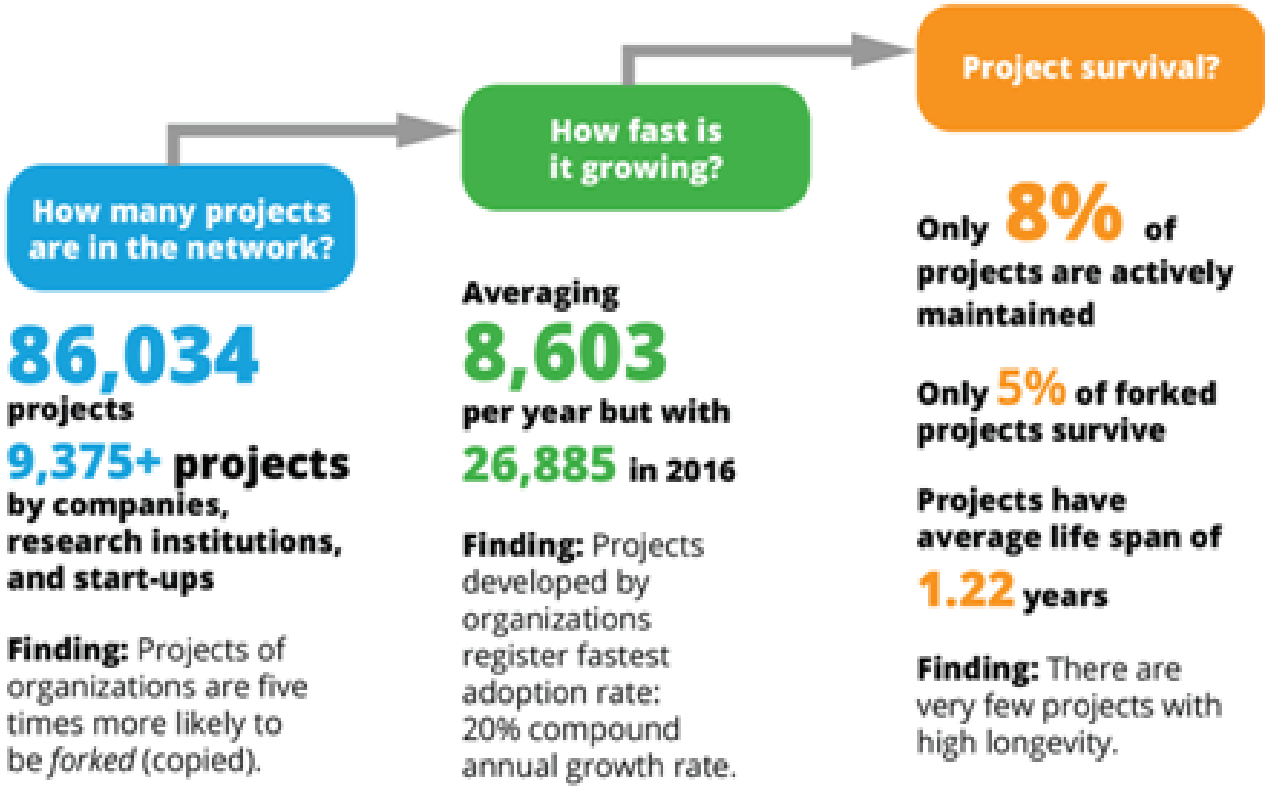
- 当前区块链技术的演进阶段，开发者的兴趣更多在于对开源区块链解决方案的开发。区块　链能通过开放源代码协作，更快速地实现严格的协议和标准化。
- 区块链开发最受欢迎的编程语言：C++排第一，Go排第二。

现有平台综述和框架映射

平台	准入机制	数据模型	共识算法	智能合约	开发语言	代币/激励
Bitcoin	公有链	基于交易	PoW	基于栈的脚本	C++	比特币
Ethereum	公有链	基于账户	PoW/PoS	Solidity/ Serpent	Go/C++	以太币
Ripple	公有链	基于账户	RPCA	-	C++	瑞波币
Hyperledger Sawtooth	公有链/ 联盟链	基于账户	PoET	Python	Go	-
Hyperledger Fabric	联盟链	基于账户	SBFT/PacificA	Go/Java	Go	-
CITA	联盟链	基于交易	Tendermint/ RAFT	Solidity/Java	Java	-
TrustSQL	联盟链	基于账户+交易的混合	BFT-Raft	JavaScript	Java	-
Factom	公有链/ 联盟链	基于账户	类Pos	-	C++	FCT

区块链生态竞争激烈

■ 区块链缺乏统一**标准**，不利于区块链技术的创新发展和项目应用落地。



Source: Deloitte analysis of GH Torrent data and GitHub API data, as of October 12, 2017.

■根据德勤从GitHub上爬取的数据，截止2017年10月，网络上总共有近9万个区块链项目；

■平均每年新增8600多个项目。但在2016年，就新增了27,000个区块链项目；

■如今，仅有8%的项目有人维护，5%被复制的项目存活下来。项目平均寿命仅为1.22年。

全球区块链标准化进展：缺乏统一标准

2017年5月，成立**分布式账本焦点组（FG DLT），**聚焦讨论区块链和分布式账本的相关应用、技术框架和监管治理。**中国信通院联合央行数字货币研究所**，代表产业界，提交了一个技术提案“可信区块链：一个分布式账本技术评估框架”，获得了现场各国代表的广泛好评。

万维网联盟（W3C）于2017年11月，成立**区块链社区组**，基于ISO20022标准，**制定区块链通信协议的格式规范**，主要涉及分布式存储、内容分发网络、公链、联盟链、侧链的消息格式。

国际标准化组织（ISO）成立**ISO TC 307工作组**，专门推进区块链和分布式账本的标准制定。目前分为基础定义、安全隐私和智能合约三个工作组，已有10个标准草案在研制。

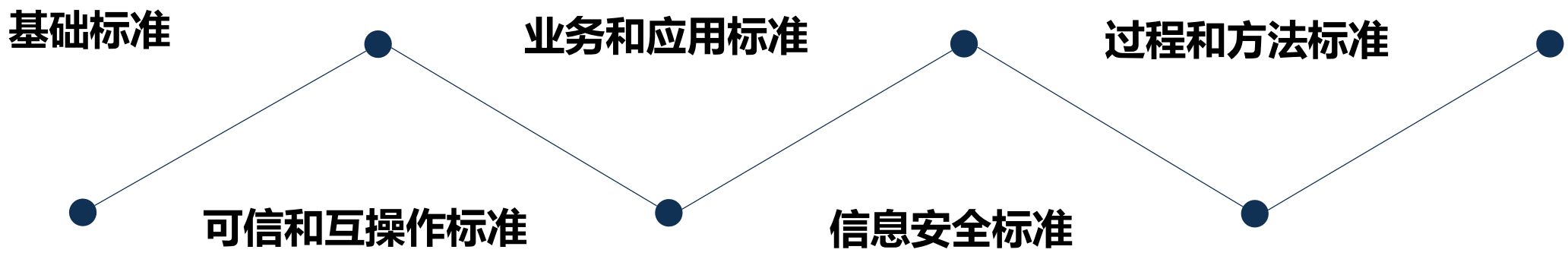
IEEE于2016年7月组建了一个**区块链工作组**，已成立P2418物联网区块链研究组和P825能源区块链研究组，推进区块链在农业、自动驾驶汽车和能源交易领域的标准制定 。

全球区块链标准化进展：各国竞相角逐

我国已开始着手建立区块链国家标准

在2018中国数博会上，工信部信软司信息服务业处李琰处长在致辞时透露，我国已开始着手建立区块链国家标准，计划从顶层设计推动区块链标准体系的建设，目前已提出全国区块链和分布式记账技术标准化技术委员会组建方案。

国家区块链标准的重要组成部分



行业联盟：启动可信区块链推进计划

2018年4月9日，由中国信通院牵头，百度、阿里、腾讯、京东金融、微软、Intel、SAP、中国电信、中国移动、中国联通、华为、中兴等**158家**企业联手，共同启动了“**可信区块链推进计划**”。**中国通信标准化协会理事长奚国华、工业和信息化部信息化与软件服务业司巡视员李颖、中国信息通信研究院院长刘多出席并致辞。**
中国科学院院士郑志明、中国工程院院士陈纯担任战略指导委员会主任委员。

《可信区块链》系列标准阶段性成果

行业专家共同参与标准的制定过程，形成最广泛的行业共识

中国信息通信研究院、
腾讯科技有限公司、
浙江蚂蚁小微金融服务集团有限公司、
百度在线网络技术有限公司、
北京奇虎科技有限公司、
联动优势科技有限公司、
上海保险交易所、
中国移动通信集团有限公司、
中国电信股份有限公司北京研究院、
中国联合网络通信有限公司、
上海证券交易所技术有限责任公司

SAP中国研究院、
华为技术有限公司、
中兴通讯股份有限公司、
杭州趣链科技有限公司、
布比（北京）网络技术有限公司、
北京泛融科技有限公司、
智链数据科技（南通）有限公司、
北京博晨技术有限公司、
北京太一云科技有限公司、
北京欧链科技有限公司、
北京泰尔英福网络科技有限责任公司

目前国内首个可信区块链标准已经编写完成，并更新迭代

《可信区块链第1部分：区块链技术参考框架》

《可信区块链第2部分：总体要求和评价指标》

《可信区块链第3部分：评测方法》

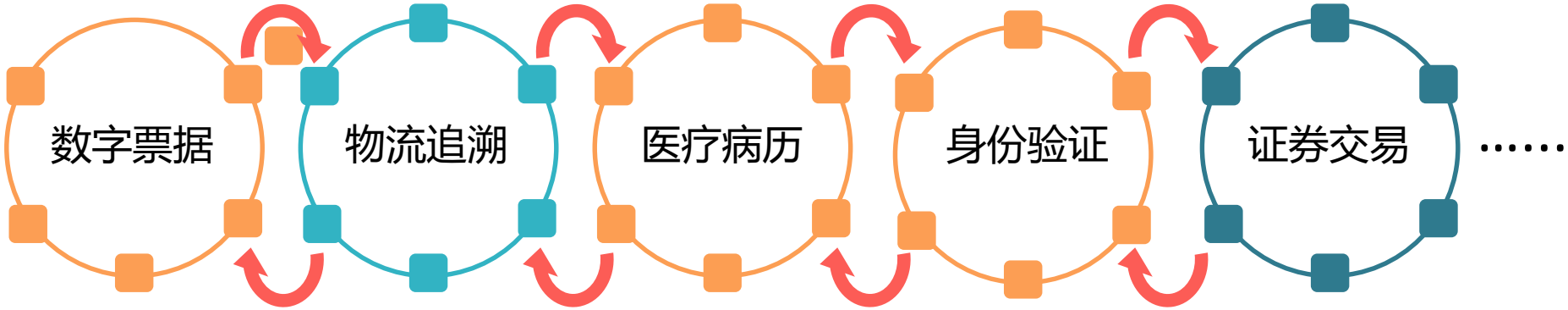
02 可信区块链标准

区块链越来越不像一条链

技术迭代

链上	解决性能低下的问题	链下
单链	解决扩展适配的问题	多链
孤链	加速价值流通增值	跨链
区块链	区块树、区块图的出现	分布式账本

跨链流通



跨链：价值要在不同区块链系统中流通、增值

不同区块链平台的对比

特性	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
机密性	无	无	无	基于哈希的内容地址	无	无
信息可获取性	区块镜像	区块镜像	账本镜像	图和文件镜像	区块镜像/分布式哈希表镜像	哈希图/可选择的事件历史镜像
完整性	多区块认证	多区块认证	最新的区块认证	基于哈希的内容签名	多区块认证	大概率共识
不可抵赖性	数字签名	数字签名	数字签名	数字签名	数字签名	数字签名
来源验证	交易输入/输出	以太坊状态机与交易功能	数字签名账本和转移指令	数字签名与版本控制	交易输入和输出、虚拟链参考	哈希图/可选择的事件历史镜像
签名	公钥	公钥与合约地址	公钥	公钥	公钥或者公共信息	不支持；或许分层
选择性披露	无	无	无	无	选择性访问加密存储	不支持；或许分层

不同区块链平台的性能对比

特性	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
一致性	区块确认（60分钟）	区块确认（15*15~15*30，约5分钟左右）	单块确认（小于1分钟）	P2P镜像（主要受网络读写速率影响，对于128kb以下文件秒级响应）	区块确认（60分钟）	大概率共识；拜占庭共识
系统复杂性	中	高	中	中	中高	低（非完整系统）
容错性	以最长的链为准	以最长的链为准	最新被投票的区块总是获得共识	内容地址哈希。抗网络波动	以最长的链为准	强拜占庭容错
可测量性	区块大小（平均每秒7笔交易）	区块大小（平均每秒15笔交易）	每秒万笔交易	每秒万笔交易	区块大小（平均每秒7笔交易）	每秒万笔交易（仅受带宽影响）

可信区块链标准：因为透明，所以可信

区块链的
需求侧

- ✓围绕最终用户视角
- ✓构建统一话语体系
- ✓行业的最高水准
- ✓可实现、可验证
- ✓与技术架构中立

区块链技术
供给侧

不同区块链厂商由于解决方案不一样，技术架构、通信协议和实现方法都不一致，在将解决方案大规模部署至生产环境之前，系统的性能、可扩展性、安全性、稳定性和可维护性等都需要严格的测试验证

制定区块链标准：确定基本概念和明晰范围

确定区块链在金融领域的定义和范围

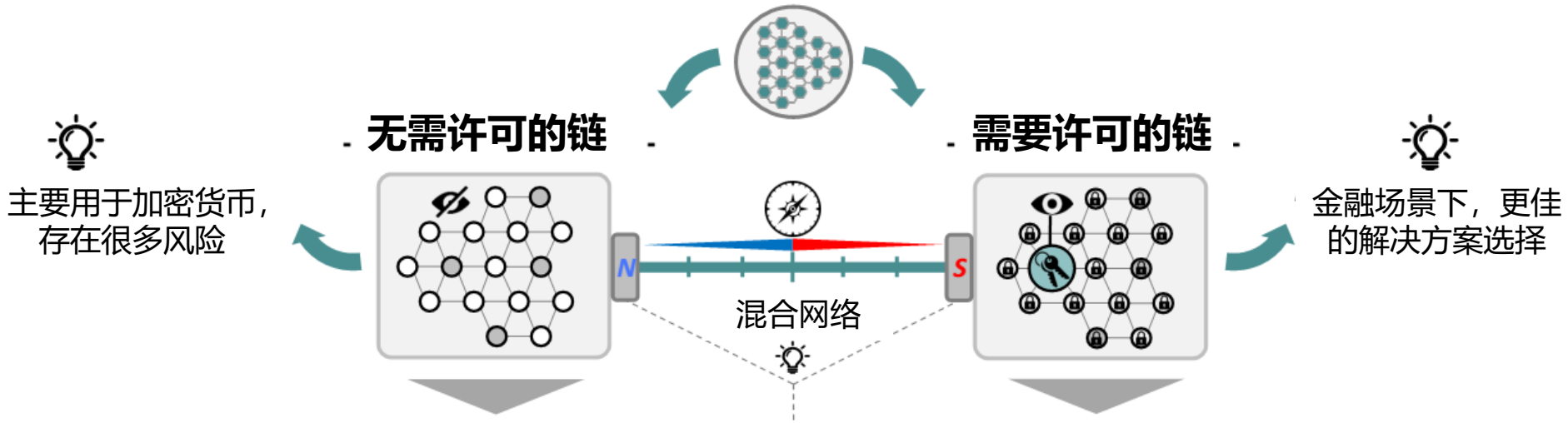
链上	性能	链下	Bitcoin→Lightning Network Ethereum→Raiden Network
单链	适配	多链	Plasma: root blockchain and sub-blockchain RSCoin: higher-level block and lower-level block
孤链	融合	跨链	COSMOS、Polkadot
区块链	演化	分布式账本	L0：区块树 IOTA：区块图 R3 Corda：无链之链

确定“金融区块链“的基本概念和范围

- 不同行业：银行业、证券业和保险业
- 同一行业：行业支付清算、跨行支付清算和跨境支付清算
- 同一业务：大额支付系统和小额支付系统
- 同一操作：实时全额支付系统和批量小额支付系统

制定区块链标准：锚定测试对象（许可链）

非许可链在物理访问控制、网络安全保障、服务性能要求、系统可靠运行等方面不能满足《信息系统安全等级保护基本要求》、《金融行业等保标准》的要求

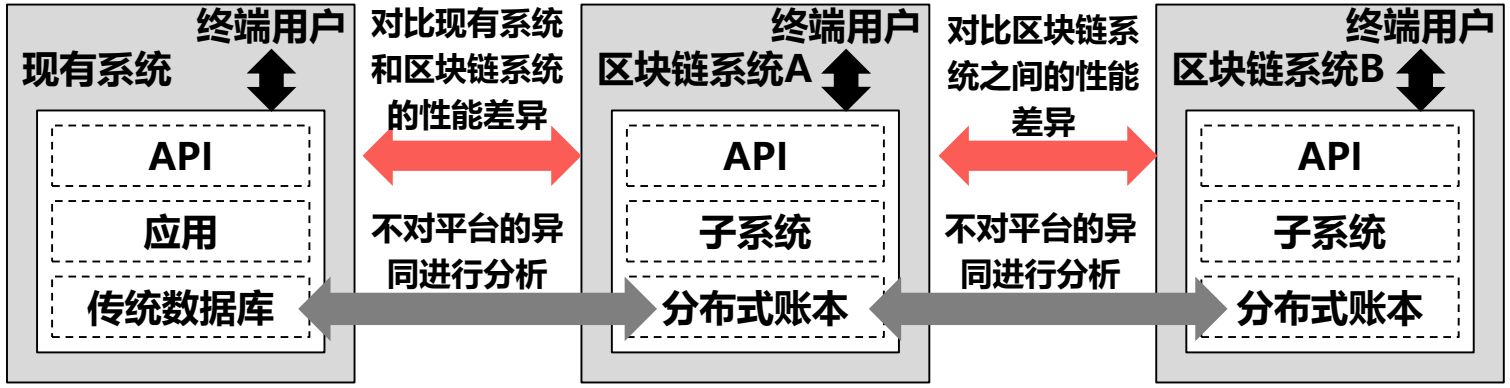


• 用户匿名	• 用户验证
• 网络接入不受限	• 网络接入需要管控
• 账本写入的见证者列表是不确定的	• 账本写入的见证者列表是确定的
• 没有系统管理员	• 有系统管理员，可配置和管控系统

制定区块链标准：明晰测试范围（系统级的评测指标）

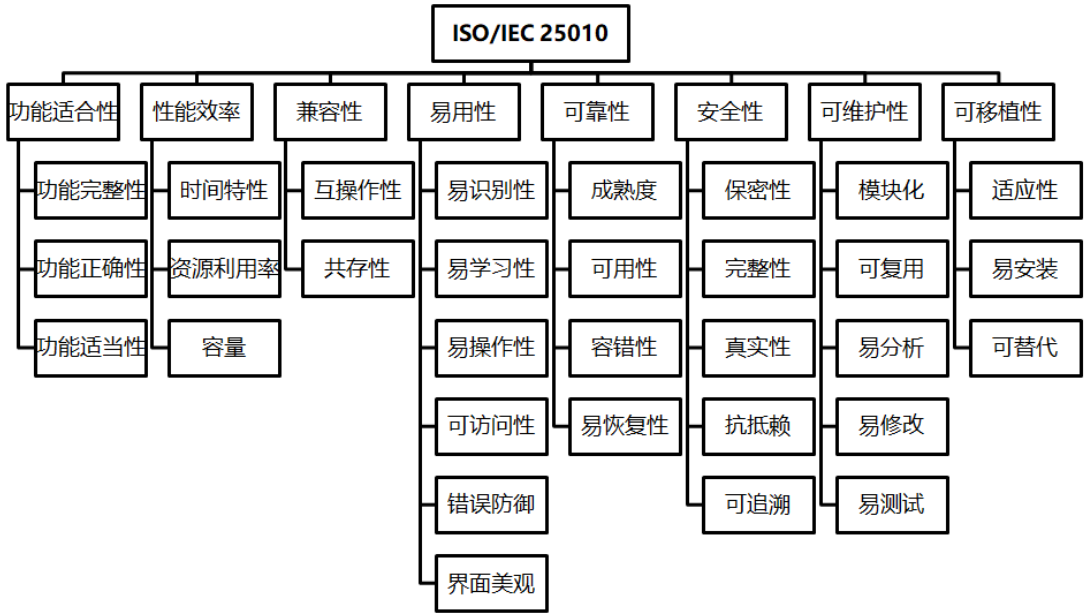
范　围

对标日本经济产业省（METI）发布的《基于区块链的系统评估方法》报告，从系统角度去对比，而不是关注平台异同



指　标

参照ISO/IEC 25010模型，从8个维度（功能测试、性能测试、兼容性测试、易用性测试、可靠性测试、安全性测试、可维护性测试、可移植性测试）对系统评测指标进行设计。



可信区块链标准：因为透明，所以可信

针对19个标准指标，涵盖了功能、技术、安全、合规等评测

数据可溯性	交易确认时间	智能合约	私钥管理安全性
基本功能检测	密码技术	性能测试	应用运行稳定性
分级分类授权认证	平台稳定性	数据私密	存储拓展
业务隔离	组件支持	节点管理扩展性	可运维性
数据审计	数据移植	共识算法在安全、性能方面有效性	

共95个评测点，让区块链用户全方面了解一个区块链产品等情况

评测指标 – 功能视图


核心技术
共识算法在安全、性能方面的有效性
数据可溯性
交易确认时间
智能合约
私钥管理的安全性
基本功能检测
密码技术
性能测试
应用
应用运行的稳定性
分级分类授权认证
平台稳定性
数据私密
存储拓展
业务隔离
组件支持
运维
节点管理的扩展性
可运维性（故障恢复能力）
数据审计
数据移植

构建区块链评测体系

《区块链业务场景模块的评测方法》

- 数字票据
- 跨境支付
- 积分交易
- 信用证
- 证券交易
- 资产证券化

《区块链共性基础部分的评测方法》

- 数据处理基本功能
- 节点管理功能
- 身份认证功能
- 查询历史数据功能
- 共识机制有效性
- 数据私密性
- 核心技术自主可控
- 数据可审计性
- 故障恢复能力
- 最小硬件要求
- 密码技术合规性
- 吞吐率要求
- 应用层稳定性
- 妥善私钥管理措施

《区块链的定义、总体要求和评估范畴》

- 定义
- 总体要求
- 评估准则和范畴

针对业务进行分类

(准）实时业务

跨境支付	数字票据	股票交易	……

2017年3月9日，招商银行依靠自身研发及境内外联通的双重优势，打造了基于区块链技术的跨境直联支付系统，在国内区块链金融应用领域具有重大意义。

特点：秒级支付、私有链、无单点故障和高扩展性

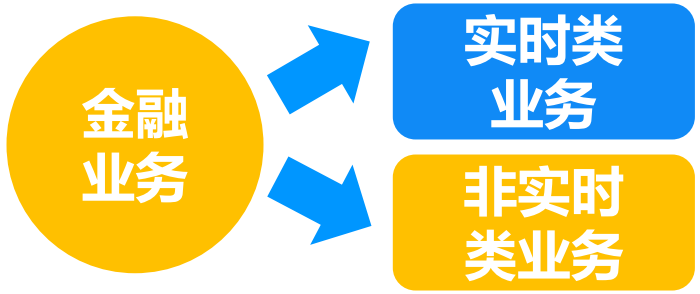
非实时业务

互助保险	电子存证	股权众筹	……

2016年8月16日，大规模商用电子存证区块链联盟“法链”宣告成立。“法链”是由Onchain、微软（中国）以及法大大等多个机构参与建立和运营的证据记录和保存系统。

特点：去中心化、联盟链、防篡改、数据零丢失

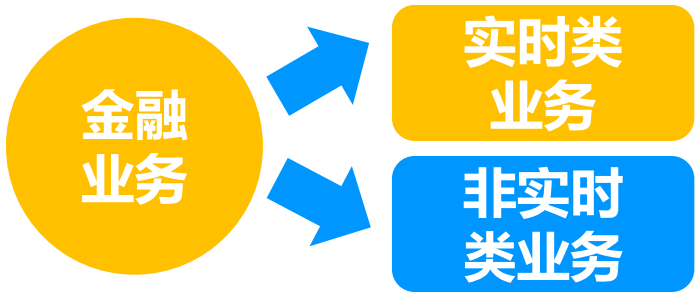
不同的业务有不同的测试标准：实时业务更注重性能测试



通过区块链保证参与交易多方之间金额平衡。
同时引入监管方，增强KYC和AML的能力

测试重点	能力指标	指标描述
性能评测	交易确认时间	从交易发起到接受者的余额可消费的时间
	单方交易TPS	一对一交易的平均TPS和峰值TPS
	多方交易TPS	多对多交易的平均TPS和峰值TPS
	交易失败率	正常交易因超时、被作恶节点篡改形成的交易失败率
功能评测	反洗钱能力	引入监管方，是否具备反洗钱账户冻结和账户恢复后解冻的能力
	故障恢复能力	测试系统是否可从故障中恢复，抵御DDos攻击，不受作恶节点的影响
	隐私保护能力	具有交易匿名化和保密资产内容的能力
	权限管理能力	具有注册、用户管理、鉴权和授权的权限管理能力

不同的业务有不同的测试标准：非实时业务更注重功能评测



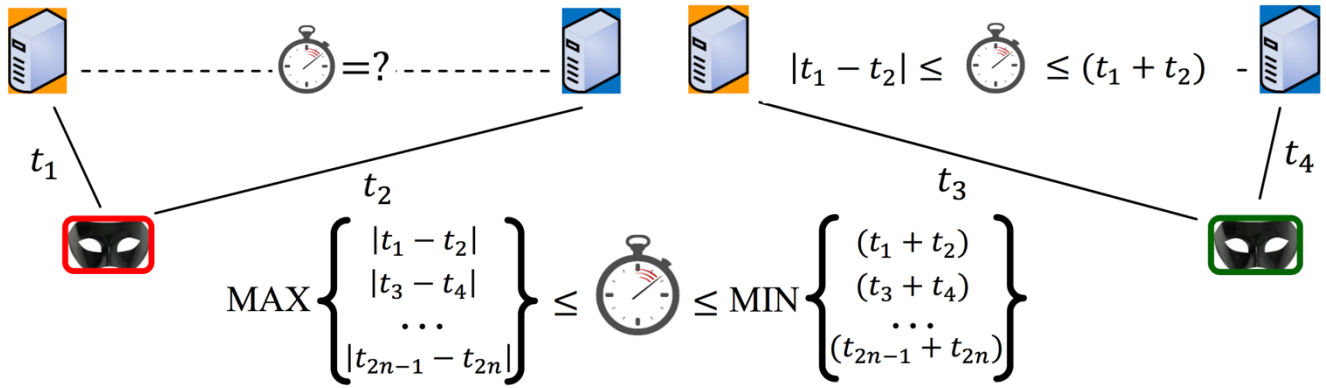
通过区块链的防篡改、不可删除、防抵赖的特性提高机构间信息共享的特性

测试重点	能力指标	指标描述
性能评测	存证确认时间	从事件发生到电子证据在链上固化所需的时间
	故障恢复时间	超过理论节点数的故障发生时，系统恢复正常的相隔时间
	防篡改节点比例	作恶节点实现篡改的节点数占全网节点的比例
功能评测	追溯能力	区块链上可以完整追溯信息修改的流水和相关机构的能力
	防篡改能力	具有在作恶节点存在时，保护数字资产和存证不被篡改的能力
	隐私保护能力	能够按照参与节点的类型划定信息共享范围的能力
	信息查询能力*	具有灵活的信息查询能力按照时间、状态等统计的能力

性能指标的一些设计思考（1）

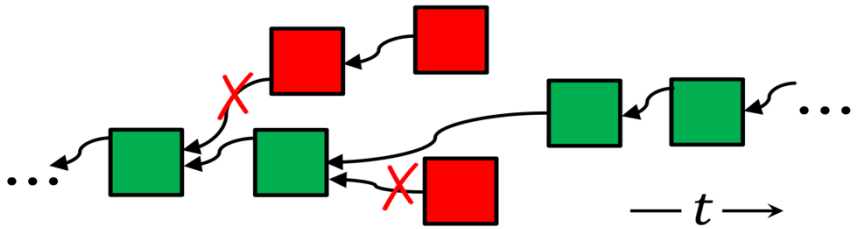
延　迟

P2P系统中都是虚拟链接，实际路由可能每次都不一样。



共识率

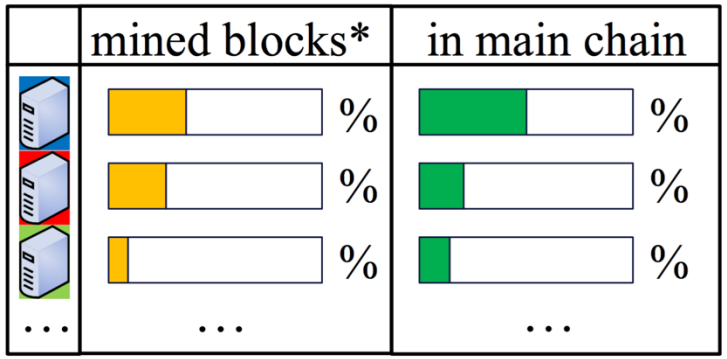
系统中设定一些节点，故意篡改释放假数据，看是否成功。



$$\frac{\sum \blacksquare}{\sum(\blacksquare+\blacksquare)}$$

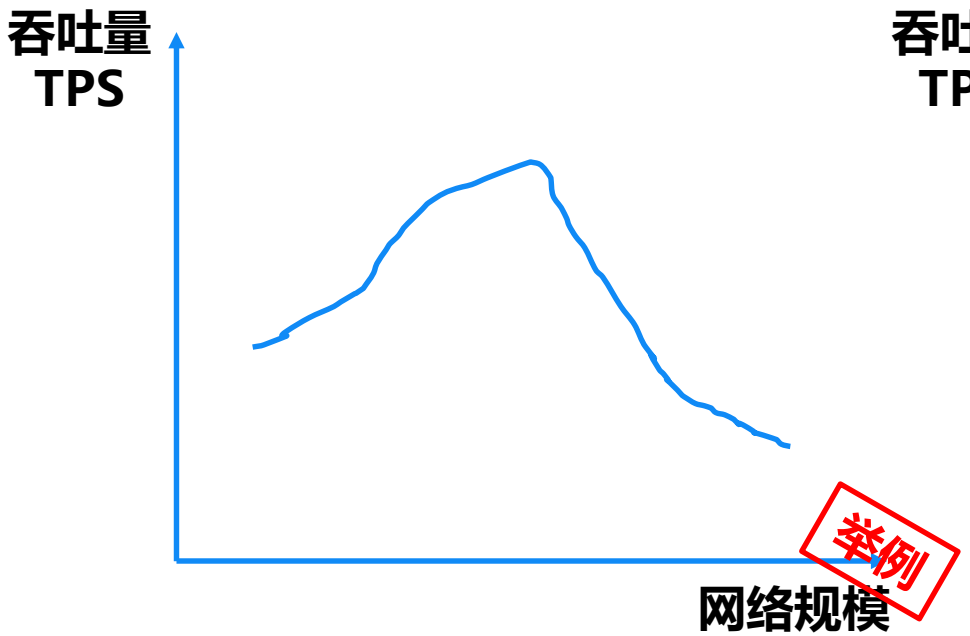
吞吐率

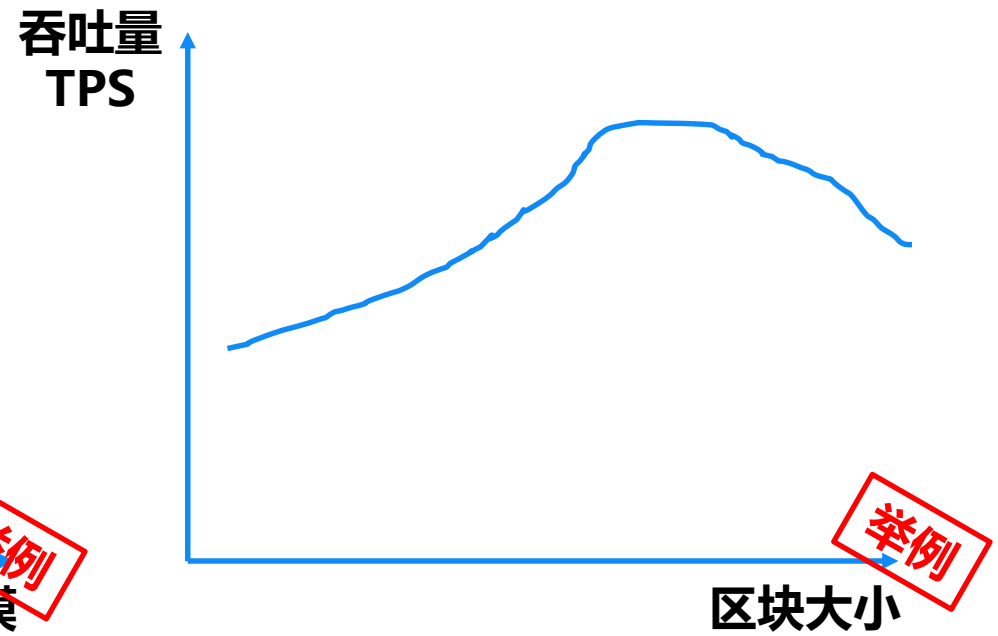
检查矿工的效率，即整个系统每秒的有效交易数。



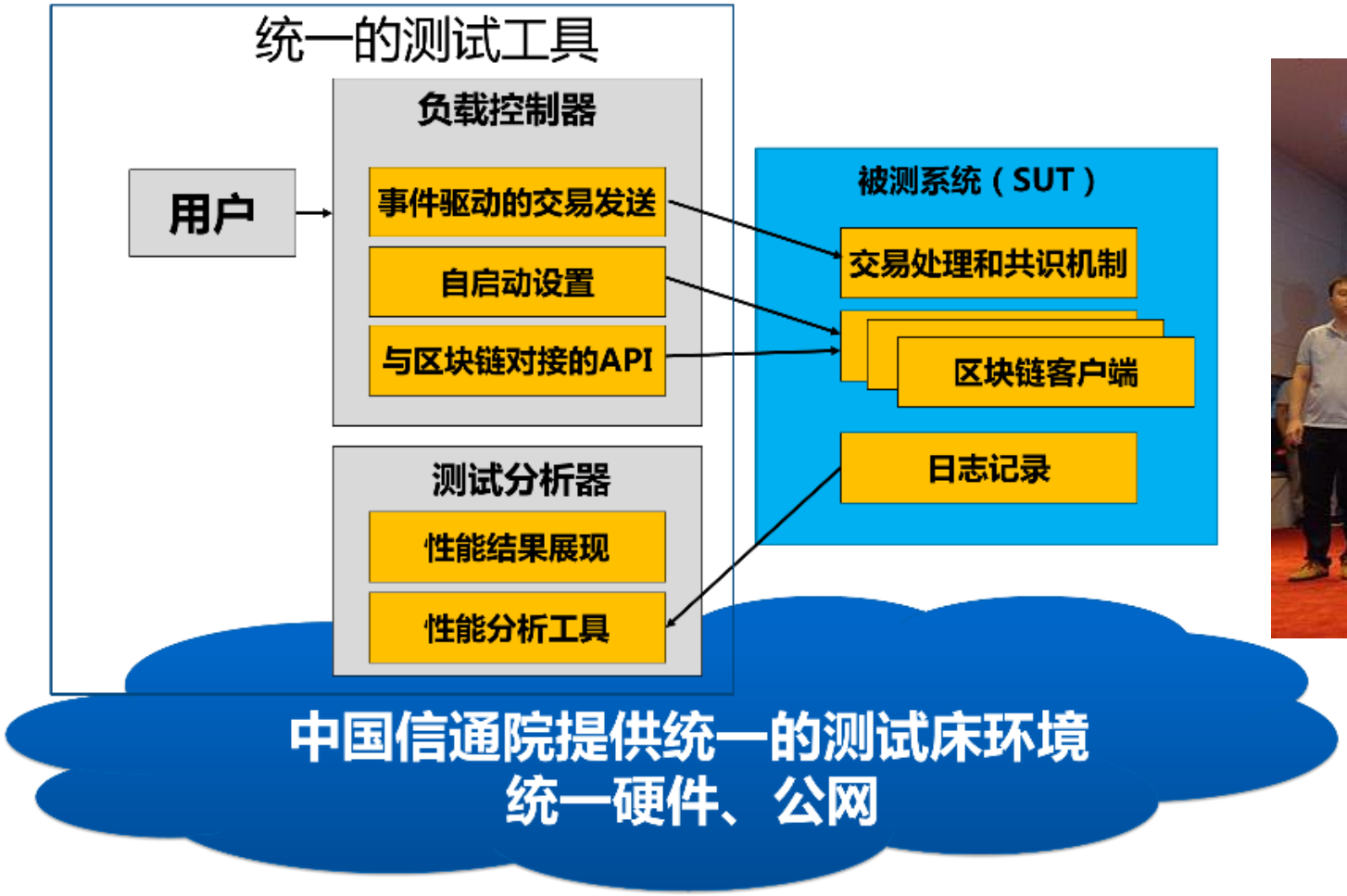
性能指标的一些设计思考（2）

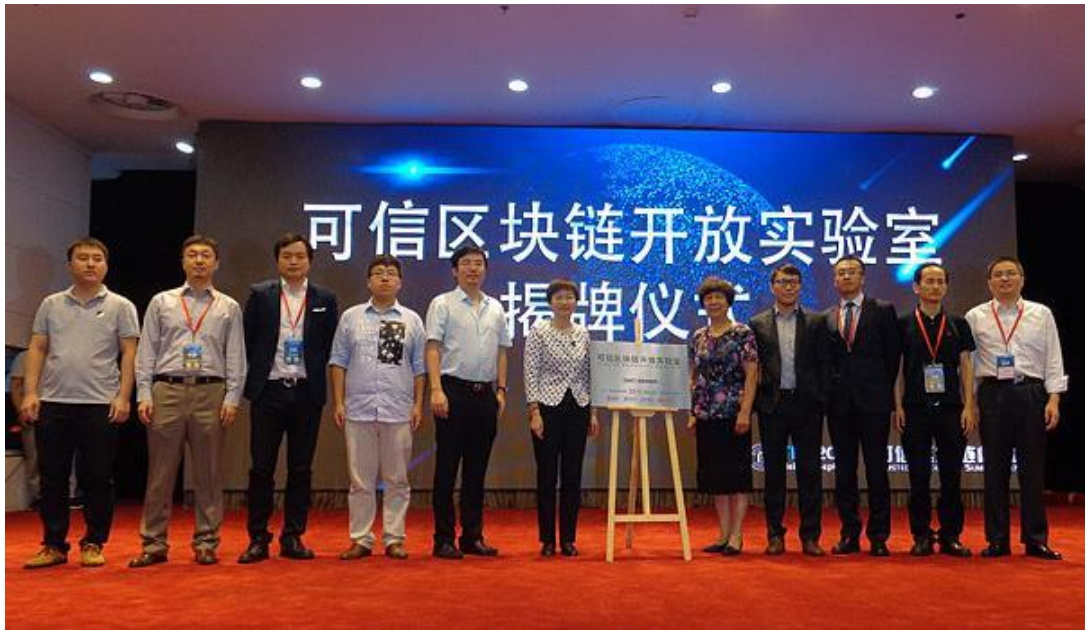
- 目前性能评测中，常见的是脱离网络规模和区块大小谈每秒交易数（TPS）
  - 实际中，网络规模越大，需要达成共识的节点越多，达成共识的进度越慢，吞吐量（TPS）就越低
  - 区块越大，可扩展性越大，吞吐量可能发生抖动，大概率是变低。





统一的软硬件环境：可信区块链开放实验室的建立





《可信区块链》系列标准阶段性成果

行业专家共同参与标准的制定过程，形成最广泛的行业共识

中国信息通信研究院、
腾讯科技有限公司、
浙江蚂蚁小微金融服务集团有限公司、
百度在线网络技术有限公司、
北京奇虎科技有限公司、
联动优势科技有限公司、
上海保险交易所、
中国移动通信集团有限公司、
中国电信股份有限公司北京研究院、
中国联合网络通信有限公司、
上海证券交易所技术有限责任公司

SAP中国研究院、
华为技术有限公司、
中兴通讯股份有限公司、
杭州趣链科技有限公司、
布比（北京）网络技术有限公司、
北京泛融科技有限公司、
智链数据科技（南通）有限公司、
北京博晨技术有限公司、
北京太一云科技有限公司、
北京欧链科技有限公司、
北京泰尔英福网络科技有限责任公司

目前国内首个可信区块链标准已经编写完成，并更新迭代

《可信区块链第1部分：区块链技术参考框架》

《可信区块链第2部分：总体要求和评价指标》

《可信区块链第3部分：评测方法》

行业标准：国内首个可信区块链标准与评测

《可信区块链第1部分：区块链技术参考框架》
《可信区块链第2部分：总体要求和评价指标》
《可信区块链第3部分：评测方法》

（企业）信息披露 → **（测试机构）测试验证** → **（专家）公证评审** → **（联盟）大会颁证**

严格按照《可信区块链》系列标准进行测试

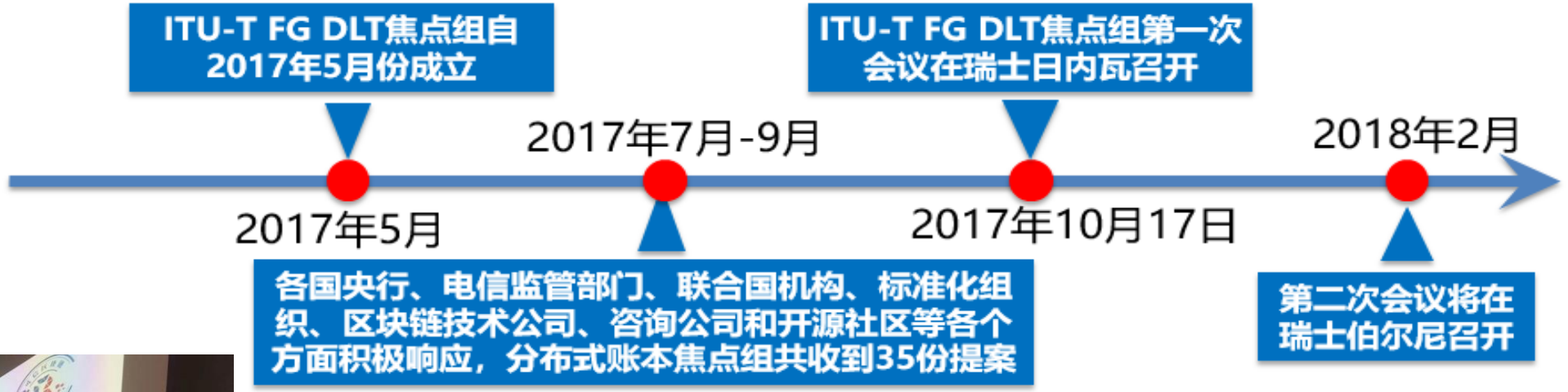
全国4个城市，9家企业开展实地测试

邀请行业专家、科研机构和参与厂商组成评审团队

中国支付清算协会
Payment & Clearing Association of China

- 承担编制中国支付清算协会的金融区块链行业标准：《面向支付清算应用的可信区块链》系列标准

国际标准：可信区块链走向国际舞台



由中国信息通信研究院和人民银行数字货币研究所，代表我国产业界联合在ITU-T分布式账本焦点组提交了“**可信区块链：一个分布式账本技术评估框架**”的技术提案，得到各方的热烈响应。

中国信通院的魏凯主任当选该组副主席

ITU-T分布式账本焦点组 | 组织架构

定义和总体组	定义和引入分布式账本生态系统的核心要件，例如名词、定义、分类和标准，阐述分布式账本概念，分析标准和生态系统之间的差距	美国安泰保险 Mr. Abbie Barbir	D1.1 术语和定义 D1.2 总概、概念和生态体系 D1.3 标准化全景图
应用与服务组	定义和描述基于分布式账本技术的商业案例，阐述分布式账本带来商业模式改变和技术竞争优势，强调出标准化给商业案例带来的益处	俄罗斯央行科技总监 Mr. Maxim Grigoriev	D2.1 水平维度的应用和服务（数据使用控制、身份认证和安全等） D2.2 垂直领域的应用和服务（电信、金融科技、供应链、能源等）
技术架构组	研究分布式账本的技术框架，包括跨链、互操作性等，提供现有系统与技术框架之间的映射，并探索分布式账本的评估评测方法	中国信通院云大所主任 魏凯	D3.1 技术架构框架 D3.2 现有平台综述和框架映射 D3.3 平台评测指标和评估方法
政策架构组	研究分布式账本相关的政策和监管措施，例如审计、隐私和兼容等，探索分布式账本相关的法律制约，并提供对应维度映射和评估方法	俄罗斯金融科技协会 Mr. Maxim Grigoriev	D4.1 基于分布式账本技术应用的政策、监管措施的维度和局限 D4.2 现有分布式账本应用与政策和监管措施的映射和评估方法

标准化路线图

可信区块链的中国力量

2018年2月6日和5月27日，ITU-T FG DLT第二次会议和第三次会议分别在瑞士伯尔尼和日内瓦召开。中国信息通信研究院云计算与大数据研究所主任、FG DLT副主席魏凯带领中国代表团（华为、腾讯、智链、博晨等公司）参会。会上，华为的胡瑞丰、中兴的王东分别当选WG3组长和副组长。中国信息通信研究院卿苏德当选为评测准则项目的牵头人，并提交相应的标准提案。

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

谢谢！