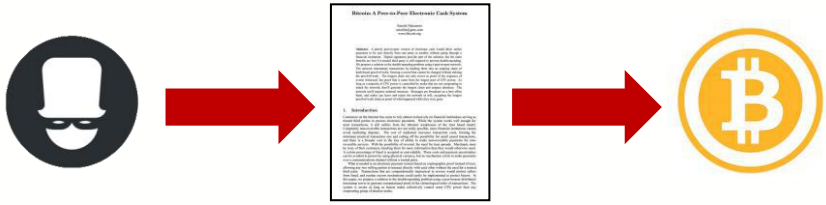
可信区块链标准解读

中国信息通信研究院 卿苏德

区块链的出现和特点

区块链的诞生

2008年11月1日，一个自称中本聪(Satoshi Nakamoto)的人在一个隐秘的密码学讨论邮件组上贴出了一篇研究报告，报告阐述了他对电子货币的新构想，比特币就此问世，区块链也随之诞生。



Satoshi Nakamoto　Bitcoin P2P e-cash paper　Bitcoin

结合了现有技术

区块链

- 对等网络
- 密码学
- 共识算法

与传统数据库相比

SELECT ✓　INSERT ✓

~~UPDATE~~　~~DELETE~~

区块链的出现和特点

典型区块链的特点

1、集体维护

依靠工作量证明、投票等算法来选出一个用户记录本时段的交易数据，而不由中心机构来担任记录和管理的角色，所以区块链的安全性依赖于对算法的信任而非对中心机构的信任。

2、不可篡改

区块链中所有用户都有整个系统中数据的完整备份，包括每个区块按照加密算法连接起来构成的“链”，一旦更改其中的任何数据，都会使其与其它区块无法成“链”。

3、开放性

在公有区块链中，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公开，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。

区块链被认为是推进互联网由不可信到可信，由信息传递到价值传递的重要基石。

不可信 → 可信

信息传递 → 价值传递

区块链

区块链现阶段的应用场景

基于区块链的特点，现阶段其应用场景条件可能在于：

- 缺乏有中心（中介）的良好解决方案
- 传递的数据具有较高的价值（如资产类）
- 缺乏信任或者弱信任

根据世界经济论坛调查报告预测，到2025年，全球GDP中有10%的相关信息将用区块链技术保存。

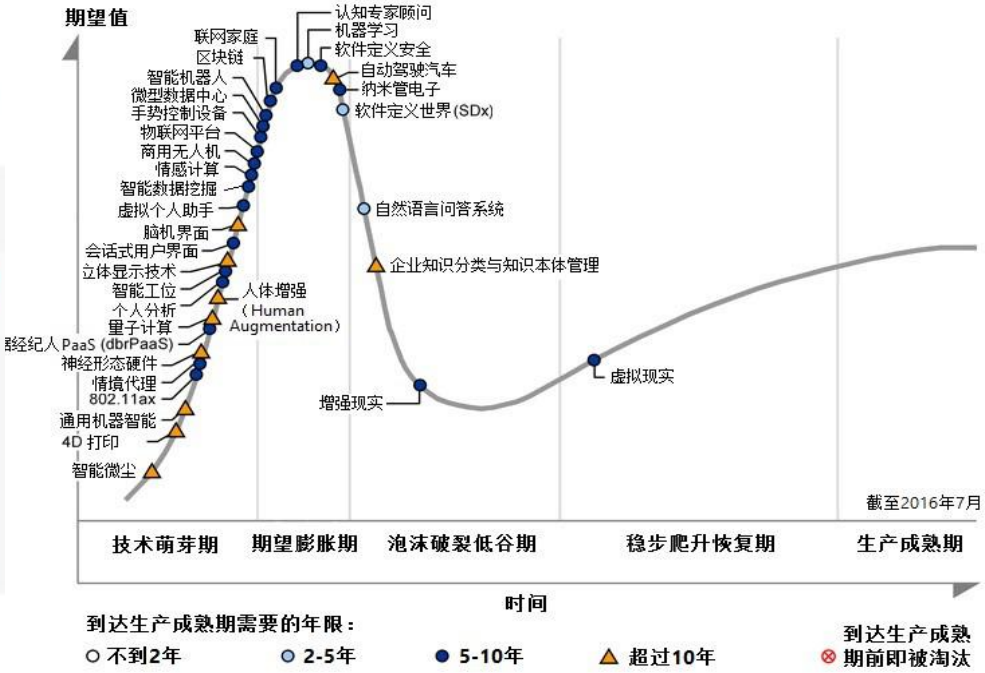
区块链受到公众广泛关注

区块链还处开发初期，技术成熟仍需时日。

百度指数显示，从2015年起，国内用户对区块链的关注逐渐增多。

据美国高德纳(Gartner)公司发布报告显示，区块链已经达到了舆论炒作的巅峰。

（数据来源：百度指数）



（Gartner曲线）

从金融的角度看区块链发展

24+国家正在投资区块链技术

过去三年，产生了2500+区块链相关专利

90+公司加入到区块链联盟

80%的银行将在2017年前启动区块链项目

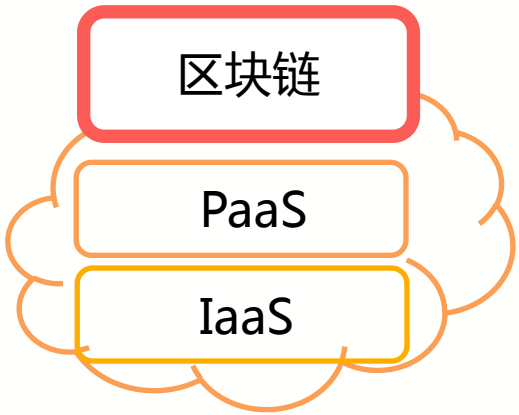
过去三年，区块链的风险投资超过14亿美元

90+的中央银行加入了区块链的讨论

（数据来源：世界经济论坛2016报告）

BaaS有望成为公共信任基础设施

区块链与云的结合有两种模式



区块链在云上

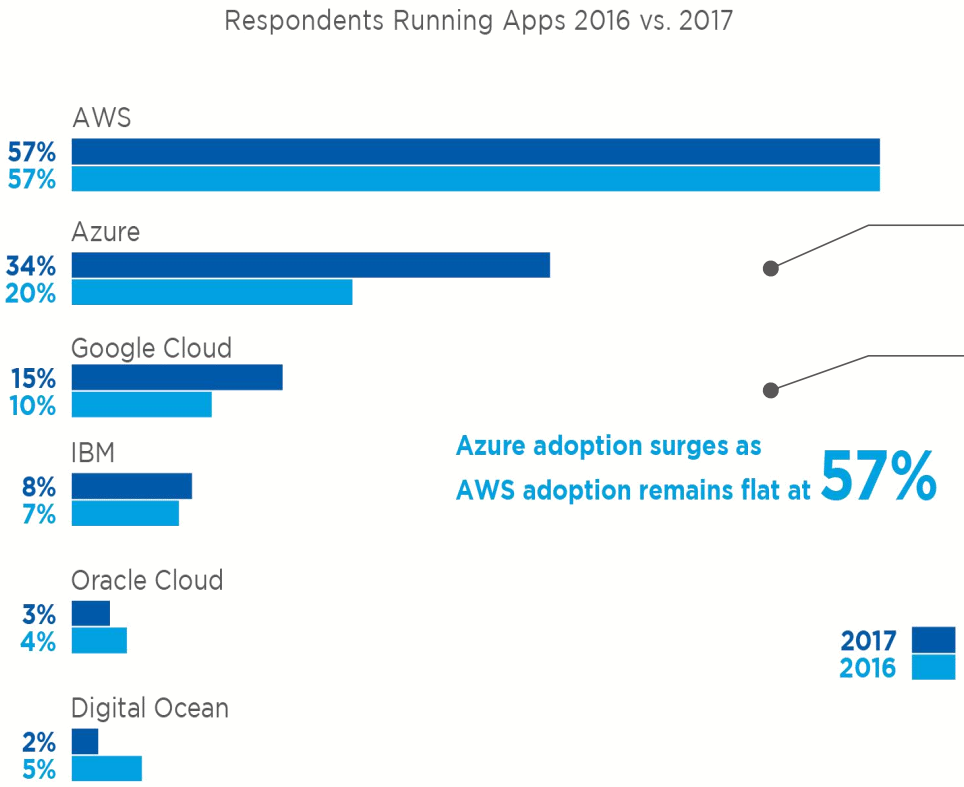
区块链在云里

- 区块链与云计算的结合，将有效降低企业应用区块链的部署成本，降低创新创业的初始门槛，是构建公共信任基础设施、激发数字经济的关键组件。

BaaS（Blockchain-as-a-Service）

- 截止2017年5月，国外IT巨头，例如微软、IBM、谷歌、亚马逊、SAP都明确提供区块链即服务功能

从云的角度看区块链发展



Source: RightScale 2017 State of the Cloud Report

亚马逊 amazon.cn

2016年5月，亚马逊选择与数字货币集团（DCG）进行合作，为企业提供区块链实验环境。

Microsoft

2016年8月，微软区块链服务（BaaS）正式向Azure云平台用户开放。

Google

2016年9月，Google云服务宣布将为银行提供区块链测试服务。

IBM

2016年10月，IBM推出了Bluemix云平台上的区块链服务（BaaS）。

ORACLE

2016年9月，甲骨文提交申请了区块链专利，提出“流程区块链”的概念，增加跨行业数据交换的安全性。

除此之外， 2016年10月，通用电气（GE）和爱立信合作，在GE Predix云上提供基于区块链的“数字指纹”存证服务；2017年5月，SAP发布了Leonardo生态系统，提供区块链云服务，希望整合物联网、机器学习等前沿科技

区块链发展正进入混沌时期

区块链概念不统一，标准规范缺失，应用场景不明确。

基本概念 → **交付形态 部署方式 …**

- 用户是否真的希望“去中心化”？
- 用户是否真的希望“不能篡改”？
- 用户是否真的希望“公开透明”？

产品形态 → **貌合神离，貌离神合**

- 交易过程中使用签名技术就是区块链？
- 数据分布式存储就是区块链？
- 信息交换采用P2P技术就是区块链？

国际标准化组织的最新进展

人们意识到区块链缺乏统一标准，不利于区块链技术的创新发展

2015年9月，由区块链创业公司R3牵头，巴克莱银行、西班牙毕尔巴鄂比斯开银行（BBVA）、澳洲联邦银行、等九家银行共同宣布成立区块链联盟R3CEV ，开始投入分布式账本的技术研发及应用探索。

万维网联盟（W3C）于去年6月在麻省理工学院（MIT）媒体实验室举行“区块链与网络研讨会” ，参与者们讨论了区块链行业标准的相关事宜，希望能推动区块链领域的标准化。

去年4月，国际标准化组织（ISO）收到了澳大利亚标准机构Standards Australia的提案，要求其为区块链技术设定全球标准。目前，澳大利亚国家标准局根据国际标准组织ISO分配的任务发布了国际区块链标准开发路线图。

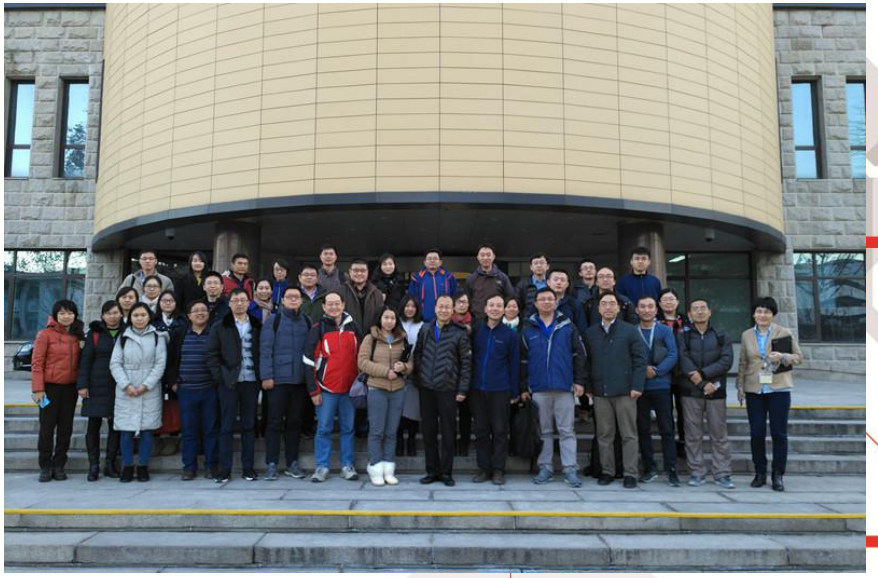
IEEE旗下The Institute消息，IEEE于2016年7月组建了一个特殊的区块链团体，为有志于从事区块链技术研发的人士提供继续教育课程，并且促进该技术的标准制定。

区块链标准引导产业健康发展

数据中心联盟成立工作组，推进区块链标准化预研。

- 2016年12月1日，**数据中心联盟**可信区块链工作组正式宣布成立。工作组由30多家单位组成，包括**中国信息通信研究院、中科院计算所、中国联通、中国电信、腾讯、华为、中兴通讯、金证股份、浪潮、世纪互联、飞天诚信、曙光信息、IBM、思科、太一云、火币网、比特大陆、布比、优刻得、中联润通、万国数据、深信服**等单位。

（工作组第一次会议现场）



（与会代表合影）

可信区块链标准研究的基本原则

明确标准起草的意向，探讨切实可行的标准化思路。

- 贴近用户需求
  - 以用户视角为中心
  - 自下而上
- 建立面向用户的统一“语境”
  - 方便用户横向比较
  - 引导产业发展方向
- 黑盒模式
  - 与技术和协议中立
  - 与实现和架构中立
  - 与具体应用中立
- 可实现
  - 代表业界最高水平和趋势
  - 标准与产业共同成长
- 可审查、可验证

行业专家共同参与可信区块链起草

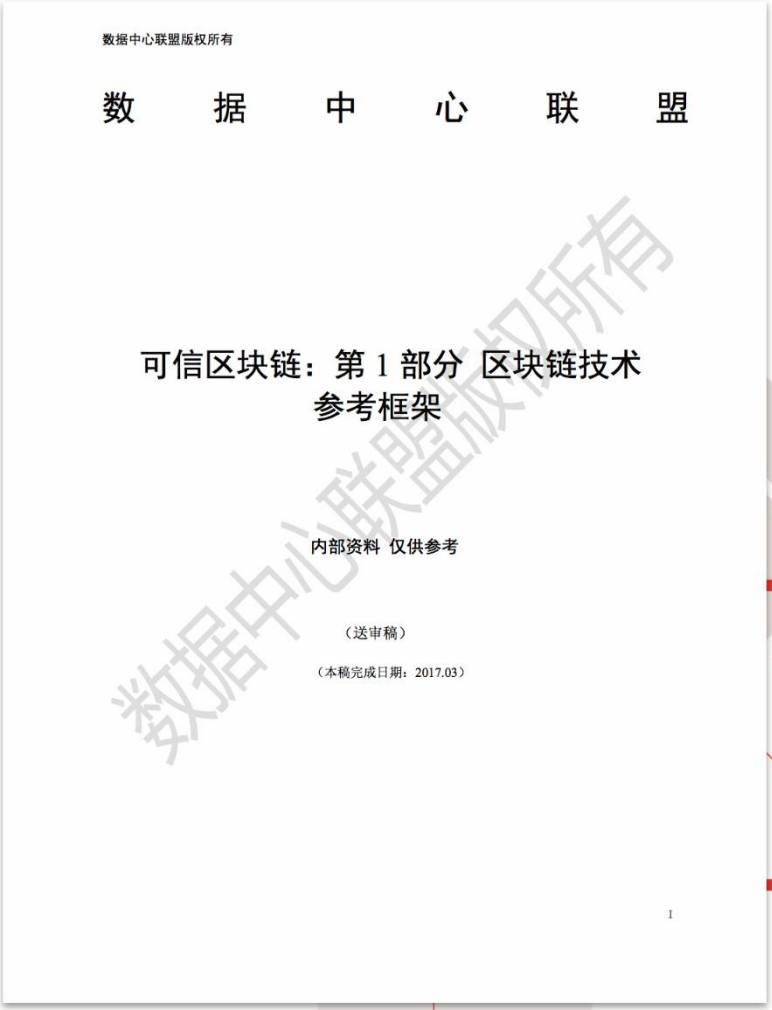
《可信区块链》系列标准已取得阶段性成果。

“可信区块链”系列标准：

- 第1部分:区块链技术参考框架
- 第2部分:总体要求和评价指标
- 第3部分:评测方法
- ……

目前，国内首个可信区块链标准已经编写完成！

《可信区块链第1部分：区块链技术参考框架》已进入报批阶段。
《可信区块链第2部分：总体要求和评价指标》已进入报批阶段。
《可信区块链第3部分：评测方法》也已基本完成。



行业专家共同参与可信区块链起草

《可信区块链第1部分：区块链技术参考框架》标准起草单位:

中国信息通信研究院、
腾讯科技有限公司、
北京太一云科技有限公司、
联动优势科技有限公司、
中国电信股份有限公司北京研究院、
布比(北京)网络技术有限公司、
北京比特大陆科技有限公司、
华为技术有限公司、
北京火币天下网络技术有限公司、
深圳市金证科技股份有限公司、
北京中联润通信息技术有限公司、
中国联合网络通信有限公司、
西安未来国际信息股份有限公司、
北京泰尔英福网络科技有限责任公司、
阿里巴巴(中国)网络技术有限公司、
深信服科技股份有限公司、
北京洋浦伟业科技发展有限公司、
国际商业机器(中国)有限公司。

目　　次

第2部分：总体要求和评价指标

用户的信任是区块链市场发展的基础。
可信区块链旨在培养用户对区块链技术的信心。

可信区块链的总体要求，也即可信区块链的“可信”主要指：

1、区块链厂商基本信息和业务信息真实、有效；

2、区块链产品符合区块链的技术特征；

3、区块链产品满足厂商承诺或用户期望的指标。

第2部分：总体要求和评价指标

《可信区块链第2部分：总体要求和评价指标》已进入报批阶段。

第3部分：评测方法

针对14个评价指标，涵盖了功能、技术、安全、合规等评测

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	妥善的私钥管理措施	

让区块链用户全方面了解一个区块链产品等情况

可信区块链工作组未来展望

1、标准制定和输出。

数据中心联盟

中国信息通信研究院

可信区块链

国际标准 —— 国际电联：SG16

中国通信标准化协会 China Communications Standards Association

行业标准 —— CCSA：TC1

2、标准的试点评估。 区块链开放实验室、区块链测试平台建设。

3、区块链行业纵向和横向交流。 项目落地；区块链与物联网、云计算等结合。

金融区块链以许可链为主

根据我国国标《信息系统安全等级保护基本要求》，公有链的技术架构在物理访问控制、网络安全保障、服务性能要求、系统可靠运行等方面并不能适应国家的相关规定。

名称	解释	优点
公有链	任何人都可以参与，容易部署应用程序，全球范围可以访问，不依赖于单个公司或辖区。	1、保护用户，免受开发者的影响。2、完全开放，可以开展全球性的交易。
私有链	可用于单独的个人或实体，对政府、公司内部的审计和测试有用。	1、规则可以很容易改变；2、参与验证的节点是可公开的；3、交易成本更低；4、节点可以更好的连接；5、隐私可以更好受到保护。
联盟链	对产业或国家的特定清算、结算用途有用，容易进行控制权限设定，有较高的可扩展性。	1、网络优化更好；2、能适应多种形态的交易类型；3、可扩展性更强；4、可以进行必要的隐私保护。

许可链包括联盟链和私有链，是指需要许可才能进行网络接入的区块链组织形式，这也是目前区块链应用于金融领域主要的组织形式。

金融业务的分类

（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

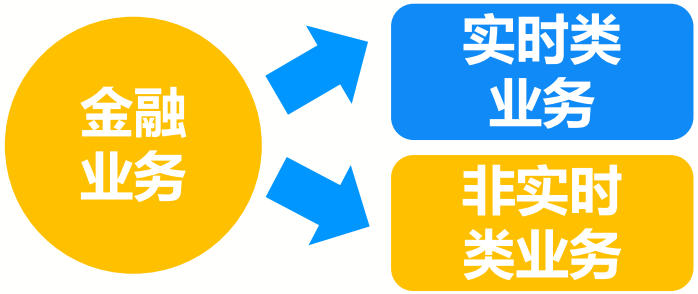
非实时业务

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

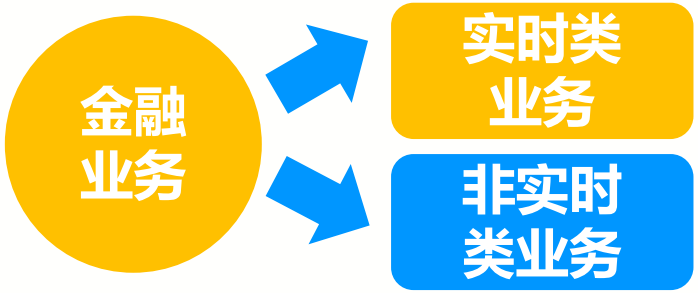
实时业务，主要注重性能评测



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	候选厂商
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	
	故障恢复时间	超过理论节点数的故障发生时，系统恢复正常的时间	
	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	
	资产交易能力	具有资产的发行、转让、兑付的能力	
	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	

非实时业务，主要注重功能评测



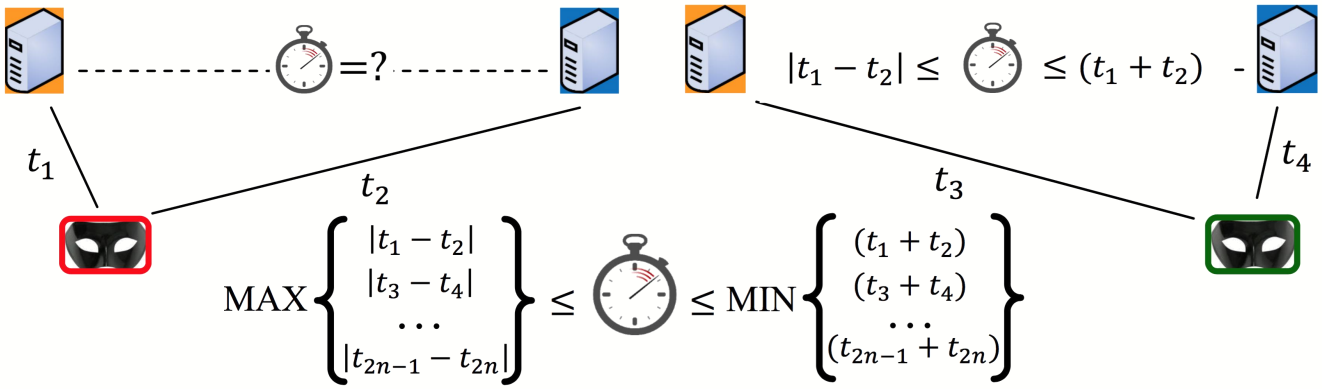
通过区块链的防篡改、不可删除、防抵赖的特性提高机构间信息共享的特性

测试重点	能力指标	指标描述	候选厂商
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	vechain 中国平安 PINGAN 物链 uChain PICC 中国人民保险集团股份有限公司 THE PEOPLE'S INSURANCE COMPANY (GROUP) OF CHINA LIMITED
	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）

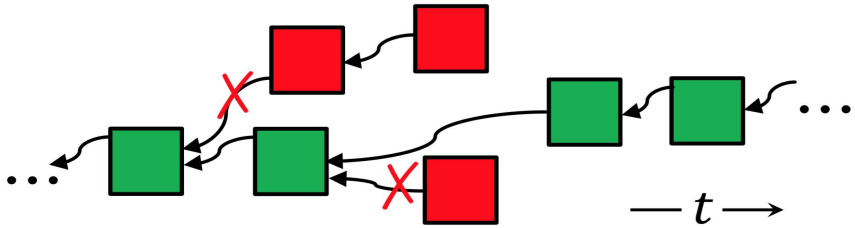
延　迟

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

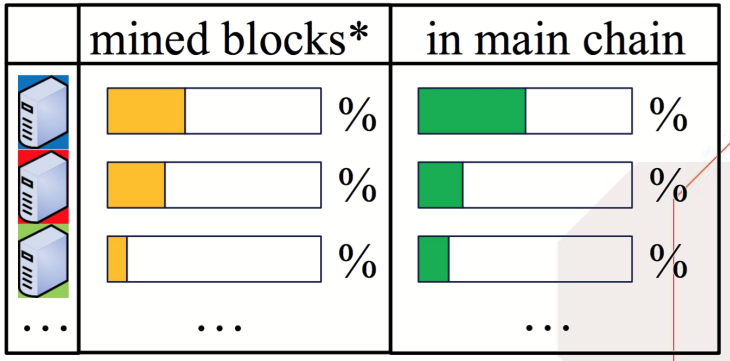
系统中设定一些节点，故意篡改释放假数据，看是否成功。



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

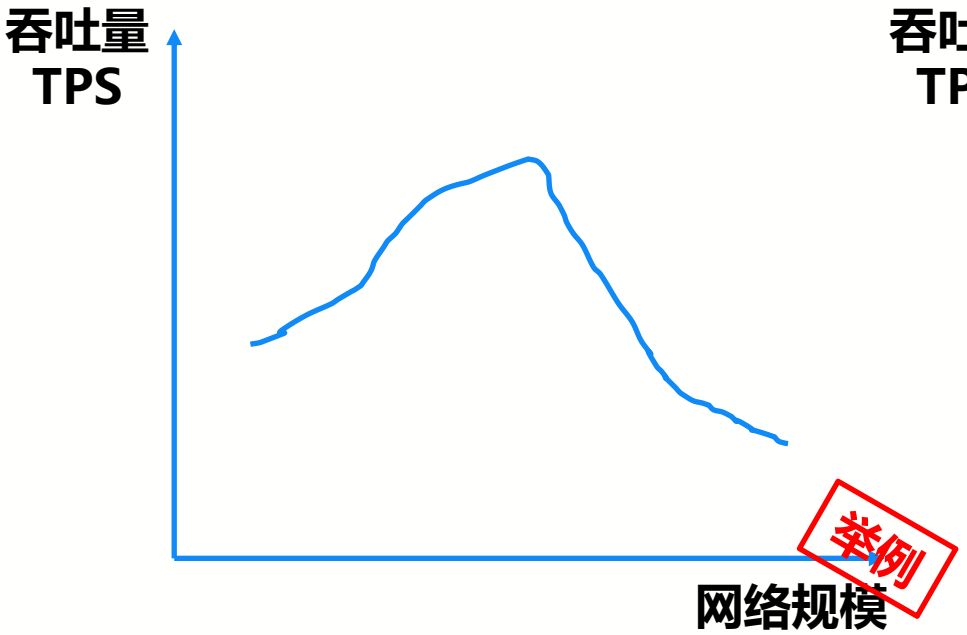
吞吐率

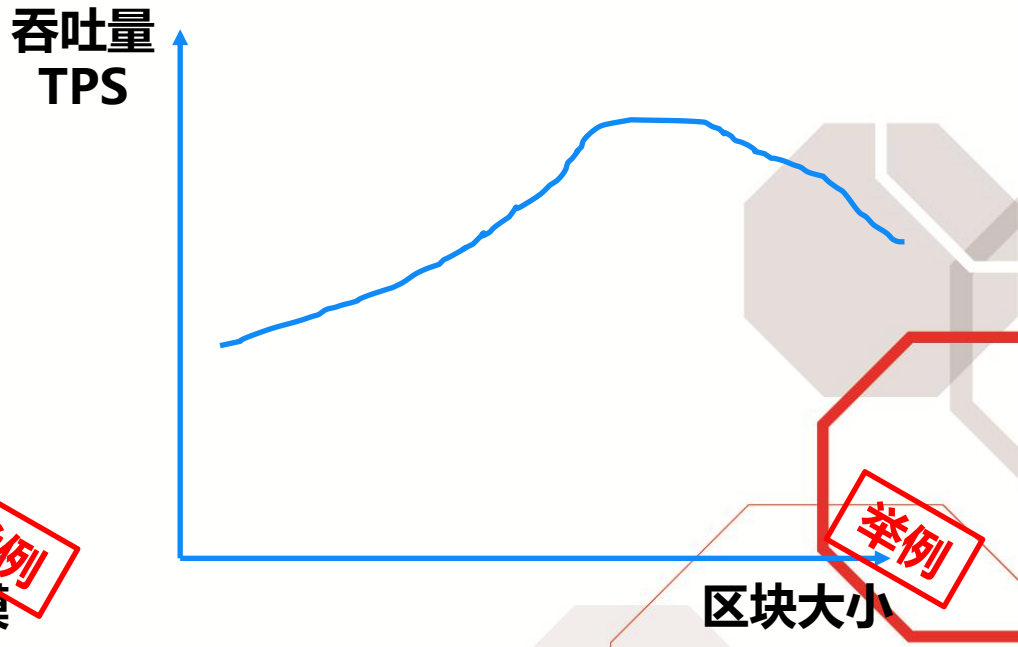
检查矿工的效率，即整个系统每秒的有效交易数。



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。





未来的工作

- ✓可信区块链预测试的全面开展
  - ◆ 9月12日召开可信区块链峰会，成立可信区块链联盟，并对测试通过的厂商颁发评测证书，宣布十大区块链应用案例。
  - ◆ 根据可信区块链预测试的结果和经验，不断丰富和迭代可信区块链标准
- ✓区块链测试平台的搭建
  - ◆完成许可型的区块链测试平台搭建（含联盟链和私有链）
- ✓区块链测试工具的研发
  - ◆研发支持多种区块链系统接入的交易模拟发送器

期待合作，携手共进！

谢谢聆听，
期待合作！

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

卿苏德（博士，高级工程师）
中国信息通信研究院
电话：18800027056
邮箱：qingsude@ritt.cn