

区块链开启可问责服务新时代

邹均

海纳云 CTO

QCon

全球软件开发大会

10月17-19日 上海·宝华万豪酒店



扫码锁定席位

九折即将结束

团购还享更多优惠，折扣有效期至9月17日

扫描右方二维码即可查看大会信息及购票



如果在使用过程中遇到任何问题，可联系大会主办方，欢迎咨询！

微信：qcon-0410

电话：010-84782011

ArchSummit

全球架构师峰会 2017



扫码锁定席位

12月8-9日 北京·国际会议中心

七折即将截止立省2040元

使用限时优惠码AS200，

以目前最优惠价格报名ArchSummit

仅限前20名用户，优惠码有效期至9月19日，

扫描右方二维码即可使用



如果在使用过程中遇到任何问题，可联系大会主办方，欢迎咨询！

微信：aschina666

电话：15201647919

极客搜索

全站干货，一键触达，只为技术

s.geekbang.org



扫描二维码立即体验

有没有一种搜索方式，能整合 InfoQ 中文站、极客邦科技旗下12大微信公众号矩阵的全部资源？

极客搜索，这款针对极客邦科技全站内容资源的轻量级搜索引擎，做到了！

扫描上方二维码，极客搜索！

这里只有 技术领导者

EGO会员第二季招募季正式开启



E小欧

报名时间：9月1日-9月15日

扫描添加E小欧，
邀您进入EGO会员预报名群

立即报名



TABLE OF CONTENTS

1 : 背景介绍

2 : 区块链与金融科技

3 : 区块链与监管科技

4 : 区块链可问责服务

5 : 小结

互联网金融及对金融行业的冲击

• 互联网金融

- 互联网技术和金融功能的有机结合
- 依托大数据和云计算形成的功能化金融业态及其服务体系
- 普惠金融、平台金融、信息金融和碎片金融等金融模式。

• 互联网金融形式

- 第三方移动支付、征信、众筹、P2P、互联网保险、互联网理财、数字货币

• 互联网金融对银行的冲击

- 客户流失、缺少客户数据、收入、利润减少
- 蚂蚁金服、微众银行、众安保险迅速成长

• 银行业的互联网金融变革

- 中信银行异度支付、POS网贷
- 招商银行智慧供应链金融2.0、小企业E家
- 平安银行橙子银行，橙E网

互联网金融发展出现的问题

- **宏观经济背景**
 - 美国缩表引起全球金融格局的震荡
- **互联网金融快速无序发展，集聚系统性风险**
 - P2P网贷跑路现象不断
 - 客户丧失数据主导权，隐私数据被滥用
 - 无现金运动引起的争议
 - 部分企业过度扩张、资本外流，形成债务危机
- **问题的根源**
 - 缺乏服务问责机制
 - 缺少透明度
 - 缺少风险模型和风险实时管控

金融监管力度骤然提升，重塑金融体系

- **资本外流控制**
 - 资本出境审批空前严格
- **加强第三方支付监管**
 - 交易额限制
 - 成立网联，统一监管资金流向
- **整治P2P乱象**
 - 2016年10月13日，国务院办公厅发布《互联网金融风险专项整治工作实施方案的通知》
- **加强数字货币交易所监管**
 - KYC，AML纳入数字货币交易所监管要求
- **成立金融工作小组**
 - 加强互联网金融监管
- **引入科技监管（RegTech）**
 - 央行金融研究所所长孙国峰表示金融科技发展需引入科技监管（RegTech）体系

金融行业关注点转向金融科技

• 金融科技 (FinTech) 定义

- 遵从金融本质
- 以数据为基础
- 以技术为手段，为金融行业服务
 - 帮助金融行业提升效率、降低成本、增加收入

• 典型金融科技

- 大数据风险模型；
- AI理财顾问；
- 机器学习预测；
- 区块链跨境支付/清结算

互联网金融vs金融科技vs监管科技

• 互联网金融

- 是金融场景的拓展
- 将互联网作为金融产品的销售渠道，更多是卖产品；

• 金融科技

- 以数据为基础、技术为手段，改变金融行业的成本结构和收入结构
- 帮助金融机构设计产品
- 帮助金融机构节省成本

• 监管科技 (RegTech)

- “RegTech”概念最早由英国行为监管局提出，是指“运用新技术，促进达成监管要求”
 - 监管沙盒
- 监管科技的目的是用技术手段建立问责机制
 - 区块链是监管科技的一个重要技术手段

TABLE OF CONTENTS

1 : 背景介绍

2 : 区块链与金融科技

3 : 区块链与监管科技

4 : 区块链可问责服务

5 : 小结

金融科技发展对金融行业的技术变革

第一代 银行业务电子化

- 业务办理电子化
- 全国联网对账
- 资金划拨

80~90年代中期

第二代 银行业务综合化

- 综合柜员制
- 统一财务核算
- 资金汇款清算
- 24小时业务处理

90年代中期~00年代中期

第三代 数据大集中

- 数据大集中
- 以客户为中心
- 核算、清算体制改革
- 多渠道支持能力
- 大运营、集约化管理

00年代中期~2010

第四代 互联网+、数据驱动

- 互联网+
- 开放互联
- 数据驱动
- 全面风险管理

2011~至今



2005~2007

电商支付
万笔->百万笔
峰值数百笔/秒
可用率99.9%

IOE+开源

一代架构

2008~2010

互联网支付
百万笔->千万笔
峰值3800笔/秒
TB/天->PB/天
可用率99.9%+

IOE+自主中间件
+HADOOP

二代架构

2011~2014

互联网金融
千万笔->亿笔
峰值3.85万笔/秒
PB/天->EB/天
毫秒级实时数据

云计算+自主中间件
+自主数据库
+自主大数据平台

三代架构

2015~

微服务
应用容器
数据驱动
区块链
开放互联
生态圈建设

四代架构

金融科技赋能的互联网+金融系统架构

丰富的应用场景

存款

支付

生活

保障

融资

理财

投资

现金管理

同业

多终端\多渠道



金融应用云
(SaaS)

- 为客户提供3A随时随地可用的银行金融服务
- 安全、易用、开放的金融应用开发平台、公共金融业务组件与服务

存款服务

信贷服务

结算服务

数据服务

互联网金融
业务支撑平台

金融业务云
(BPaaS)

- 金融通用业务组件

个人
征信

在线
风控

网上
开户

网上
支付

电子
保全

金融数据云
(DaaS)

- 海量数据处理与计算能力
- 实时数据处理与流转能力

数据
获取

数据
建模

离线/实时
数据处理

商业
分析

数据
服务

离线、流处理、图计算、机器学习引擎

金融云平台
(PaaS)

- 大数据基础架构
- 高度集成能力的开放平台

应用
容器
平台

大数据
处理平
台

通讯
平台

安全
平台

区块链
平台

自动化
运维体系

互联网+
基础环境
运行管理
平台

基础设施云
(IaaS)

- 高度安全管理体系
- 多云异构伞形云管
- 灵活可扩展的存储架构
- 高效的自动化运维体系

弹性
计算

分布式
存储

网络
虚拟化

监控
管理

高可
用性
保障

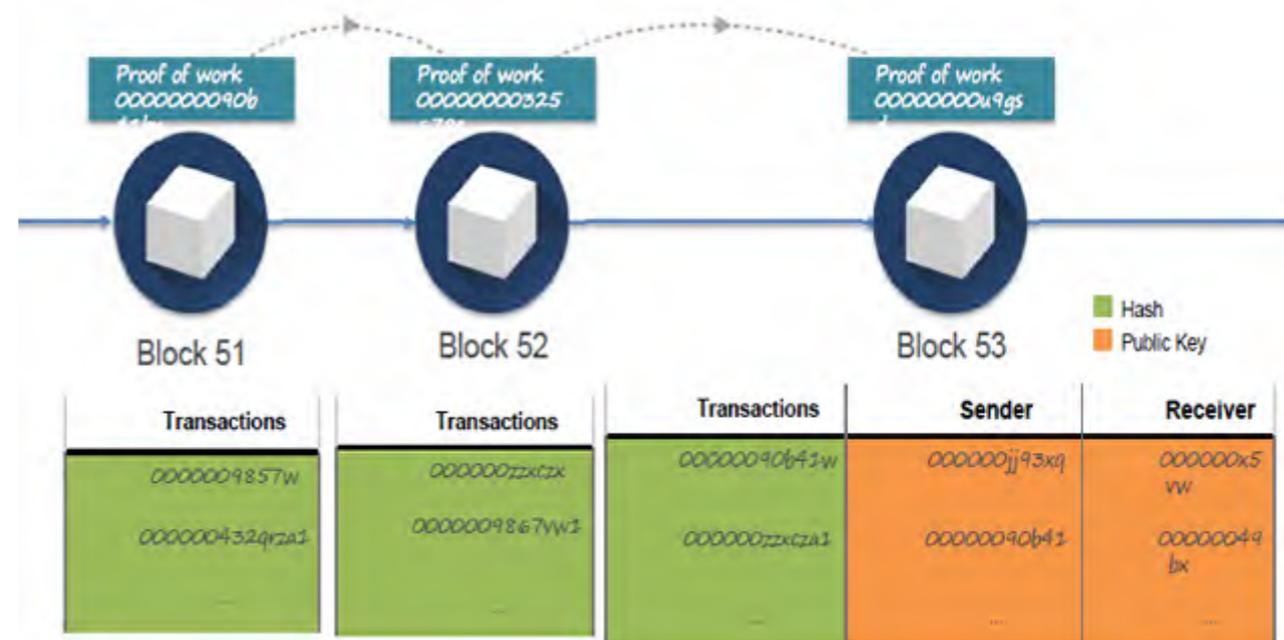
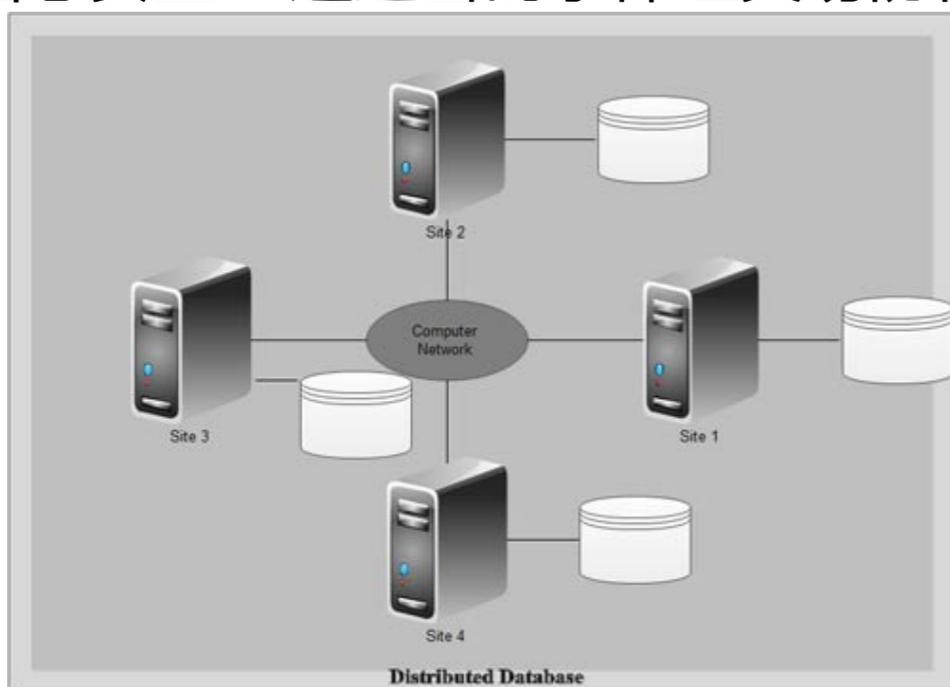
区块链介绍

什么是区块链

- 区块链是一个基于密码学和分布式共识算法，不可篡改的点对点分布式账本系统

区块链特点概览

- 业务网络 – 点对点架构，每个业务参与者是一个节点；
- 共享账本 – 记录业务网络中所有的交易，在所有参与方节点复制，只有相关方才有权限访问数据；
- 共识机制 – 账本中的记录需要在网络中得到确认，并同步到各节点；
- 智能合约 – 一个在区块链上部署的，运行在各节点虚拟机上的一段程序。其运行结果需要在区块链上形成共识；
- 信息安全 – 通过密码学保证交易防伪，数据不可篡改，隐私信息得以保护



区块链-去中心化信任建立

• 区块链信任的含义

• 真实性

- 私钥签名保证交易不能伪造；

• 透明性

- 交易记录在交易相关方公共账本

• 溯源性

- 账本交易可追溯；

• 不可篡改性

- 账本只能追加，不能删改；

• 客观性

- 账本状态是共识结果
- 推翻共识结果成本高昂

• 权益确定性

- 私钥决定数据权益

• 唯一性

- 价值权益只可转移，而不可复制



区块链价值 – 构建低成本诚信体系，实现价值传递

- **解决了中心化信用机构成本高昂脆弱问题**
 - 中心化的信用机构安全脆弱，易受攻击，存单点故障
- **解决了互联网上造假容易，难以杜绝的问题**
 - 解决在互联网上难以保护个人隐私的问题
- **区块链共享账本方式节省对账，清结算成本**
 - 避免多方各自对账的成本
 - 同时减少中介环境，降低清结算成本
- **从信息传递的网络，提升到价值传递网络**
 - 区块链解决了互联网上难以解决虚拟货币的“双花”
 - 区块链的智能合约，解决了承诺和交付不一致的问题。



区块链在金融行业应用

• 银行

- 征信、支付、汇兑、结算、清算
- 贷款、抵押、承兑、托收
- 虚拟货币、票据、凭证、理财
- 审计、AML

• 保险

- 理赔、定损
- 智能合约保险产品
 - 农业保险
 - P2P互助保险

• 证券

- 交易、资产虚拟化

• 信托

- 基金投资管理

• 众筹

- 资金管理



国内金融行业区块链应用

● 清算、结算：招商、微众、
华瑞

● 票据：农业银行、交通银行、
浙商

● 资产交易：平安银行、工商
银行

● 抵押贷款估值信息：中国银
行、汇丰

● 征信：平安银行

● 资产托管：中国储蓄银行

● 通用存证、防伪：兴业银行

● 信用证：中信银行

● 可信POS电子签购单：光大、
银联

● 积分：江苏银行

国外金融行业区块链应用

序号	银行	系统名	领域或业务	内容	类型
1	英格兰银行	RSCoin	央行发行数字货币	货币的发行是由bank完成	数字货币
2	纽约梅隆银行	BK Coins	员工酬劳系统	兑换礼品卡, 优惠券以及其他津贴	数字货币
3	花旗银行		花旗币		数字货币
4	厄瓜多尔		国家版数字货币	让偏远地区无法拥有银行资源的民众也能通过数字化平台, 获得金融服务	数字货币
5	突尼斯		国家版数字货币	让国民通过数字货币买卖商品, 还能缴付水电费账单等	数字货币
6	澳新银行、西太平洋银行	Ripple Labs 系统	区块链分类帐系统	小额国际支付	支付与清算
7	澳大利亚联邦银行	Ripple Labs 系统	区块链分类帐系统	附属机构之间的支付结算	支付与清算
8	CBW银行	ONE Card	实时支付系统	实时结算, 使得客户可以即时取回资金。	支付与清算
9	澳洲证券交易所			考虑使用区块链来替代原有清算和结算系统	支付与清算
10	印度商业银行	Hyperledger技术	供货商融资系统	构建了基于区块链的供应商融资解决方案	票据与供应链
.....					

TABLE OF CONTENTS

1 : 背景介绍

2 : 区块链与金融科技

3 : 区块链与监管科技

4 : 区块链可问责服务

5 : 小结

监管科技核心 - 可问责 (Accountability)

• 历史起源

- 《汉谟拉比法典》

- 公元前1772年，人类历史上已知的第一部法典《汉谟拉比法典》在古巴比伦第六代王朝由国王汉谟拉比公布

• 可问责 (Accountability) 概念

- “有把行动和决定告知其他相关方的义务，或者告知原委，如果存在不当行为愿意接受处罚” - 安德雷斯·赛德勒

• 问责产生根源

- 由生产关系产生
 - 社会关系
 - 合同关系
 - 上下级关系
 - 其它关系

问责为什么重要，怎样才能做到可问责？

- 问责制是维持社会和商业运转的基础
 - 维持社会公平、公正的基石
 - 王子犯法，与民同罪
 - 商业信任的基础
 - 会计记账、账务审计、信息披露
 - 问责缺失，是造假、丑闻和危机的根源
 - 全球金融危机、安龙、泛亚等事件的发生
- 建立问责制的要素
 - 完全的信息披露以提供透明度；
 - 监控并记录义务完成情况；
 - 公平的罚则和纠纷解决
 - 如果义务未能兑现，愿意提供补偿措施

问责要求

- **传统行业问责制要求 – 通过监管强制实行**
 - **政府行业**
 - 财务预算、结算；
 - 各类数据公布；
 - **金融行业**
 - 监管资本充足率（巴塞尔协议）；
 - 信息披露（萨班斯法案）；
 - **医疗行业**
 - 病人隐私保护；
 - 医疗记录保全
 - **其他行业**
 - 质量监管；
 - 信息披露；

IT问责存在的问题

- 传统IT问责存在的问题

- 概念不清

- 对IT问责的误解

- 很多学者把IT问责与QoS、安全性、不可抵赖性等概念混淆

- 忽略问责

- 人们常常愿意追求新技术而忽略对问责的要求

- 相对于传统行业，人们更倾向在IT服务方面让步

- 缺乏监管

- 传统IT问责手段

- 工作任务声明 (SOW)

- 服务水平协议 (SLA)

- 运维监控是实现问责要求的重要手段

缺乏问责的后果

- **服务计算 (Service Computing) 发展将业务和IT紧密联系**
 - 业务云化 - 业务流程即服务
 - 云服务即业务
- **缺乏问责的严重后果**
 - 服务质量难以保证
 - 服务质量缺陷造成业务损失
 - 缺乏透明度
 - 缺乏信息披露导致误导和不公平交易
 - 安全隐患
 - 账号信息泄露造成的财产损失
 - 隐私信息泄露和滥用造成声誉破坏
 - 消费者利益难以保证
 - 缺乏合理的补偿机制以保护服务消费者利益
 - 企业关键业务不敢转移到云上
 - 制约云计算发展

区块链作为监管科技的价值 – 赋能自动化可问责机制

- **交易记录存证**
 - 区块链利用密码学技术保证交易不能伪造，过往记录不能修改
- **历史交易记录可追溯**
 - 所有交易记录在按时间顺序链接的块数据上，可以追溯，以便审计
- **公共账本使得交易具有透明性**
 - 利于监管机构监控账户交易
- **避免中心化的主观性**
 - 去中心、弱中心避免主观独断，保证公平性和客观性
- **隐私保护**
 - 密码学技术保障隐私信息
- **自动化监管**
 - 通过条件触发智能合约自动监管

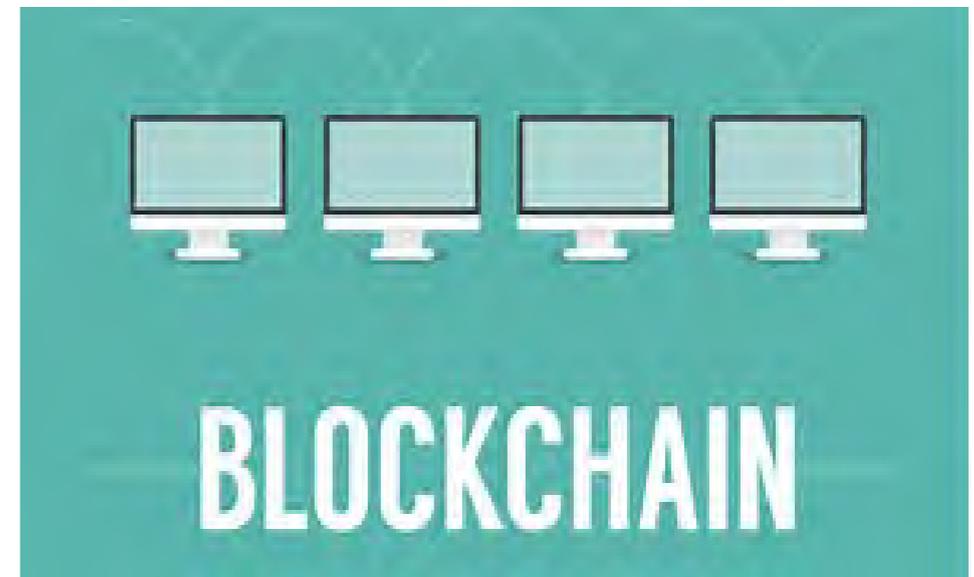


TABLE OF CONTENTS

1 : 背景介绍

2 : 区块链与金融科技

3 : 区块链与监管科技

4 : 区块链可问责服务

5 : 小结

传统IT服务管理最佳实践及云时代局限

• 传统ITSM采用ITIL最佳实践

• 服务支持

- 配置管理
- 变更管理
- 发布管理
- 事件管理
- 问题管理

• 服务交付

- 服务级别管理
- 财务管理
- 可持续性管理
- 能力管理
- 可用性管理

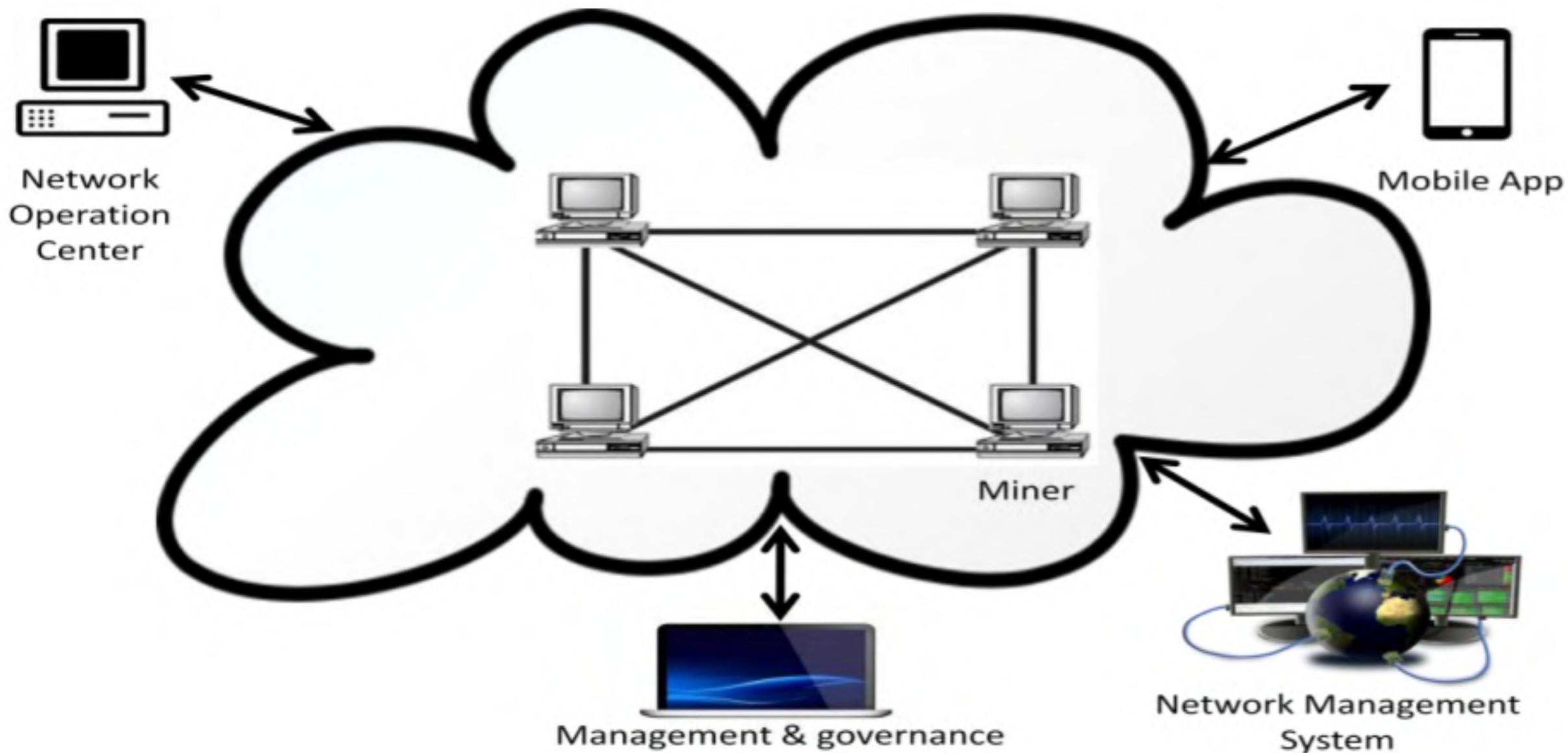
• 云时代ITSM局限

- 局限于企业内部视角
- 缺少外部视角和客户角度
- 不具备透明性
- 缺乏保证公平和客观性
- 缺乏可问责机制

ITIL核心流程



区块链应用于服务管理



区块链服务管理架构

应用层

服务监控，服务审计，服务仲裁，区块链浏览器，钱包

数据访问层

Oracle机制，数据上链API，链上搜索

区块链数据结构层

块链结构，共识机制，密码学，智能合约

网络层面

p2p网络协议，网络安全

基础设施层

云平台，BaaS，数据中心，计算、存储、网络

TABLE OF CONTENTS

1 : 背景介绍

2 : 区块链与金融科技

3 : 区块链与监管科技

4 : 区块链可问责服务

5 : 小结

小结

- **互联网金融面临监管趋严形势**
 - 金融监管力度加大
- **金融科技和监管科技成为关注焦点**
 - 区块链是金融科技 (FinTech) 的核心技术
 - 区块链同时是监管科技 (RegTech) 的核心技术
- **监管科技的目的是提高服务的可问责能力**
 - 可问责 (Accountability) 是传统行业的基石
 - 在IT服务方面，问责一直没受到重视
 - 区块链技术可用于建立自动化问责机制
- **区块链技术应用于服务管理**
 - 提升IT服务的可问责能力

关于我和我的书

个人简介

邹均，澳大利亚麦考瑞大学电脑PhD、麦考瑞工商学院MBA，资深云计算专家、区块链技术和应用爱好者。邹均曾任IBM澳洲软件部金融行业首席架构师，现任海纳云计算有限公司CTO。多年IT经验，研究的方向是区块链监管科技，区块链共识算法。

2016年出版图书《区块链技术指南》，重点介绍各类区块链技术的特征和开发方法，包括比特币、以太坊、超级账本、共识算法、闪电网络、比特币开发技术、以太坊智能合约开发等。对区块链技术感兴趣的朋友，欢迎阅读反馈。



扫描二维码购买

THANKS!

智能时代的新运维

CNUTCon 2017