China Blockchain Conference

区块链与未来网络基础设施

雷 凯
leik@pku.edu.cn

北京大学深圳研究生院
深圳市内容中心网络与区块链重点实验室

2018年11月25日，杭州

报告内容：

- 区块链的见解
- 区块链中网络基础问题
- 内容中心网络（ICN）与区块链的结合优势
- 案例：区块链与无人机
- IEN -- 智能生态网络的核心理念和构想

China Blockchain Conference

区块链 VS 西游记

灵明石猴

如来才道：“周天之内有五仙，乃天地神人鬼；有五虫，乃羸鳞毛羽昆。这厮非天非地非神非人非鬼，亦非羸非鳞非毛非羽非昆。

哪里冒出来的

好奇心

通变化，
识天时，
知地利，
移星换斗

China Blockchain Conference

区块链 VS 西游记

- 美猴王 -> 弼马温 -> 大闹天宫 -> 孙悟空

美

乐

认可
（部分）

招安

对抗

打压

共赴

求索
（取经）

China Blockchain Conference

区块链 VS 西游记

- 群魔乱舞 – 图啥?

China Blockchain Conference

区块链 VS 西游记

口块游记（探索众产众生、共识共能之真经）

“悟空”，佛空、道无。
放下执着、返璞归真；
体验自我、追求自由

“悟能”，能力。另称 “八戒”。
守戒即是悟能。
小说把“悟能”设计成猪，无知和贪欲

“悟净”，修行尚浅，求静心，净是果
芸芸众生、大众形态；
欲速则不达、求心净；

“空”乃是天地万物的本体；
“色”乃是万物本体（空）的瞬息生灭的假象；
“情”乃是人对此等假象（色）所产生的种种欲念
-- 冥思 万物之道

China Blockchain Conference

区块链 VS 西游记

- 成佛正果之路 - 路漫漫，求索 神权、皇权、民权…

敢问路在何方？ 路在脚下

未来网络基础设施

和海量能的

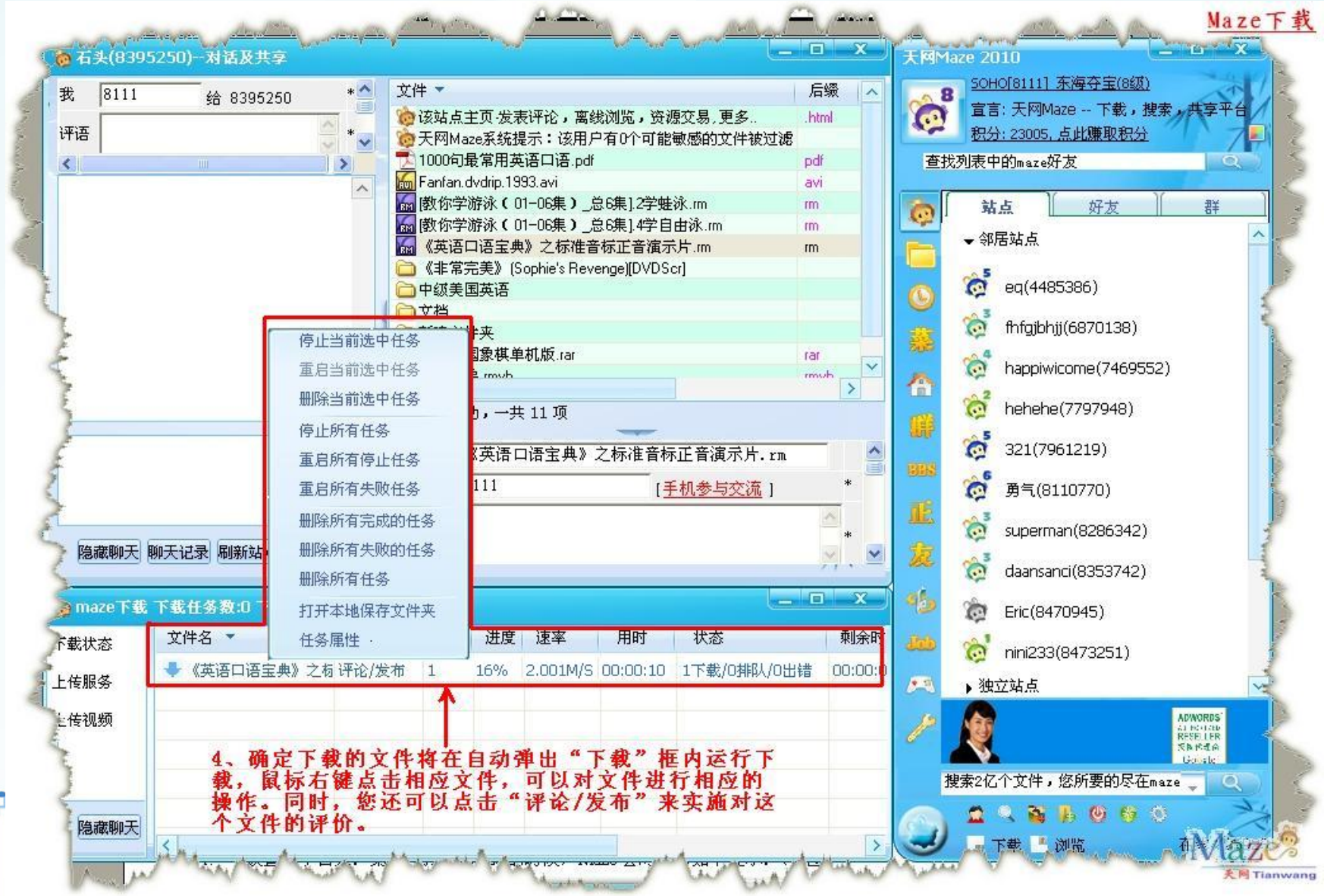
分布式

区块链网络基础问题

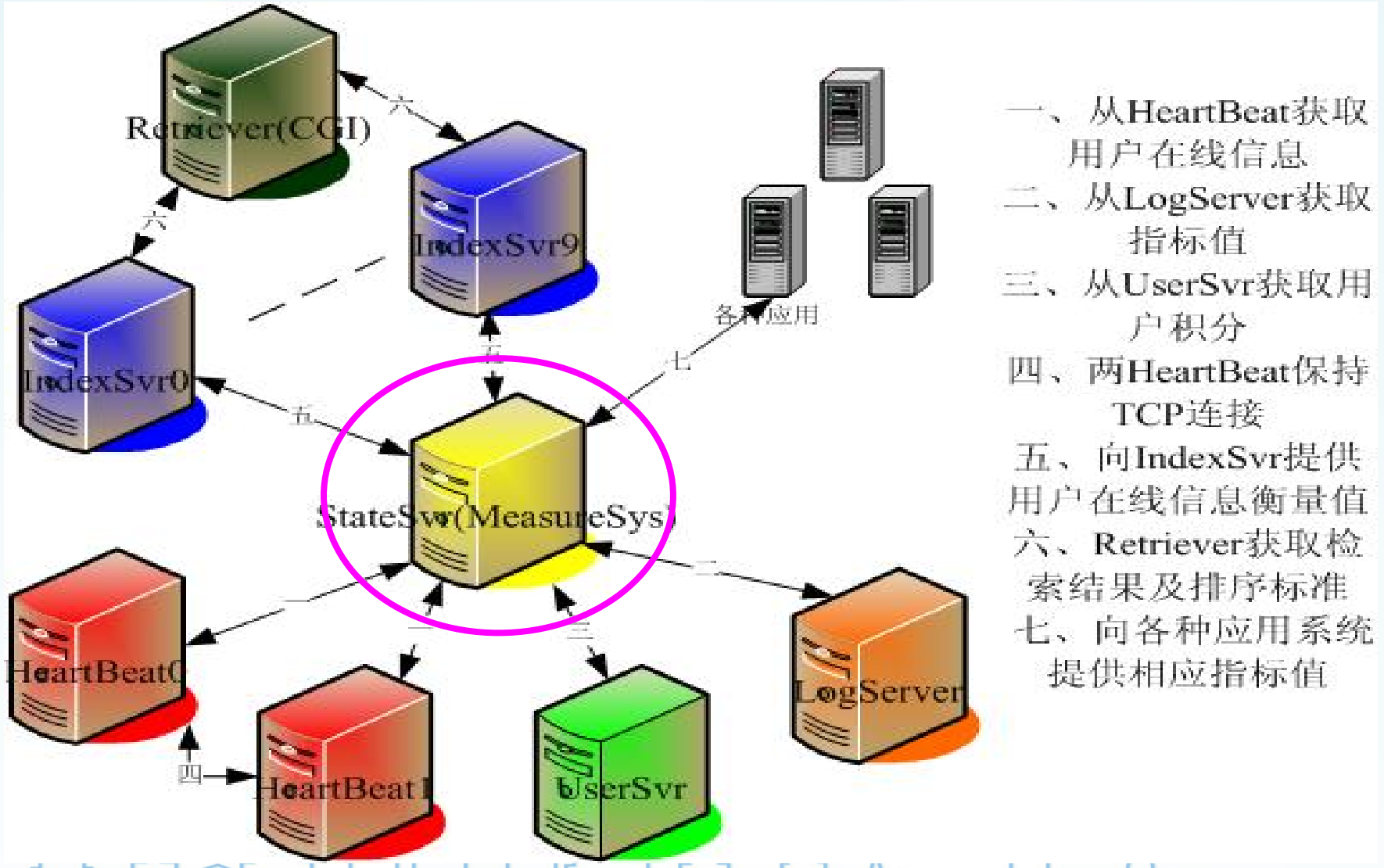
- P2P网络与分布式:过去

- 天网Maze是北京大学网络实验室开发的一款资源和功能非常强大的PIC（Personal Information Center 个人信息中心）p2p文件存储共享系统。
- 2004-2011年，累计注册850万、教育网最大

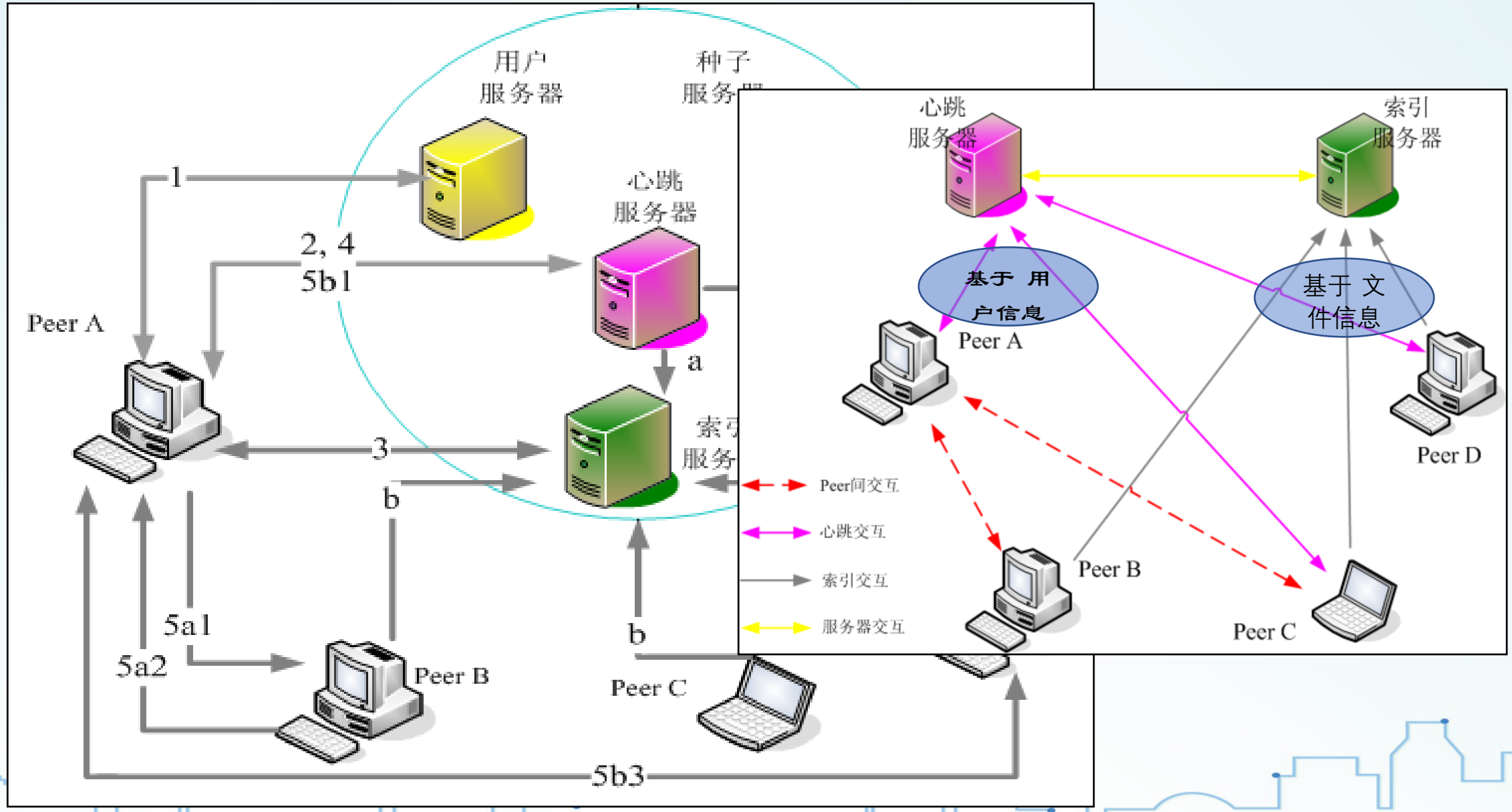
天网Maze系统实例



Maze系统架构 - 混合式构架



Maze系统资源/数据定位与分发



China Blockchain Conference

天网Maze激励与技术问题分析

- 《Maze 传销式积分规则的设计与实现》
  - 10648187 王珍 2009/05/27
- Maze 积分制度
  - 初始积分：10，000分
  - 加分：
    - 上传：+ 1.5 分/M
    - 在线：+0.5 分/2min
  - 减分：
    - 下载：- 1 分/M [0 ，100]
      - 0.7分/M (100,400]
      - 0.4分/M (400,800]
      - 0.1 分/M (800, +∝)
  - 差异性服务:
    - 下载队列排队

- 初始积分设置不合理
  - 创世币
  - 用户注册是零代价的，没有proof of work
- 下载/上传的非价值维护模式
  - 上传者获得的积分比下载者支付的积分至少多出50%
  - 每一次下载，都会通货膨胀
  - 积分规模的增长超过了文件规模的增长，缺乏价值维护
- 之前有不少技术不成熟的地方
  - 内容审计 （交易正确性）
  - 文件确权 （集中式）
  - 粒度计量 （无共识）
  - Free Rider （无社区责任感）

问题总结

- 积分的“价值性”没凸显
- 流通不方便
- 用户没有表达需求的途径
- 资源没有表现自己“资产”的途径
- 过于集中化的设计理念

总之，没有给用户提供一个可靠的、价值的、共识的、规范的底层支撑系统

互联网金融：去中介、普惠

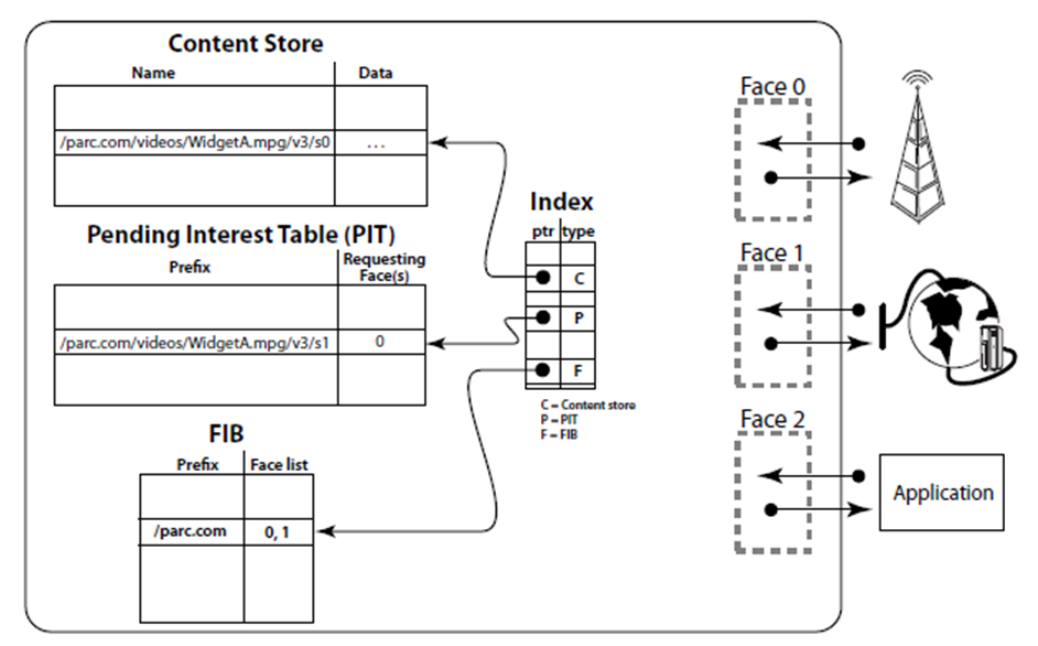
- 据网贷之家不完全统计，2018年6月停业及出现其他问题的P2P网贷平台数量为80家，其中问题平台63家（提现困难60家、跑路3家）、停业转型17家。
- 而到了7月份，仅7月11日一天，江浙沪一带就有10几家网贷平台接连被爆出现问题。 -- 运营监管之难

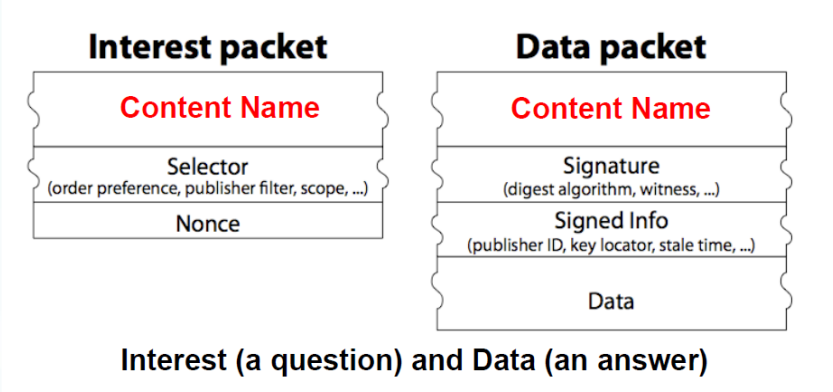
互联网金融科技：去中心、价值

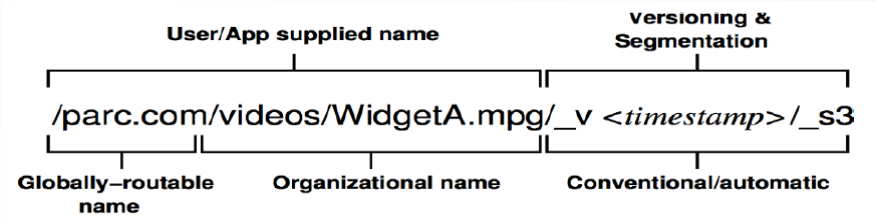
- 15年兴起的金融科技：云计算、大数据、AI、区块链、未来网络
- 真正科技主导金融
- 周小川：金融业有一半左右干的是和IT行业差不多的事情，可以说是半个IT行业，金融服务价值体现越来越依赖IT技术

内容中心网络（ICN）与区块链的结合优势

- 以内容为中心的未来互联网构架







内容中心网络主要特性与IP对比

当今IP互联网	未来内容中心互联网
拓扑不一致，重复传输 (P2P、CDN)	网络传输层加入Cache
IP网络骨干网压力大、路由表巨大	分布式、去中心化构架
面向链接为主（类似铁路、死板）	路由、智能转发灵活适应（类似快递）
移动性（受位置限制、IP语义过载）	数据包，与位置无关 (车、物联网)
多网络支持能力弱	多网络、多路径并行（WIFI、3G、4G）
安全基于系统、链路 （天然气管道）	安全基于数据自身（跨存储、跨协议）

ICN适用于多对多动态发布订阅网络

高效安全的内容分发区块链网络

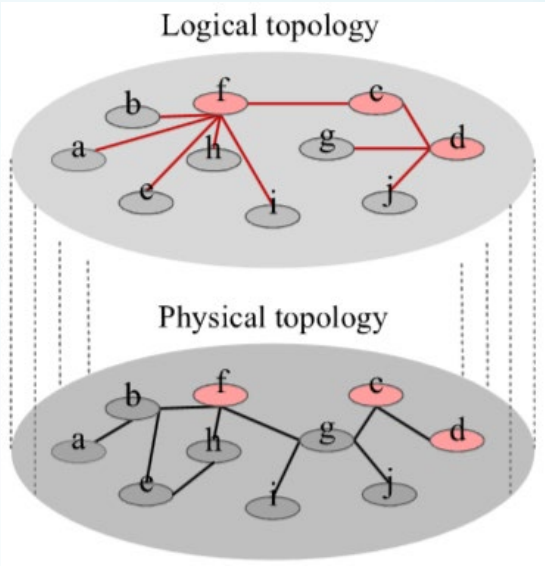
BlockNDN – 数据命名网络NDN上的比特币原型系统

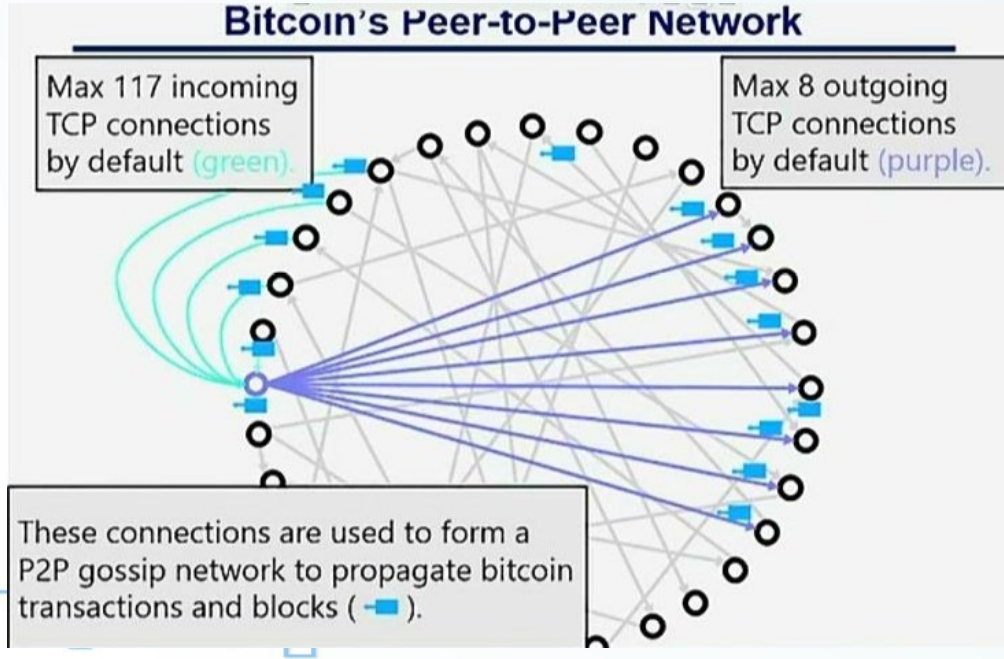
- 上下拓扑一致，更低的多多、广播开销，更快的区块传播
- 去中心化的系统，不需要超级节点建立连接（闪电网络）
- 匿名安全，防止针对于IP地址的嗅探与监听，保护隐私
- 解决诸如比特币中日蚀攻击（Eclipse attack）等问题

攻击者可以提供错误的账本状态信息，攻击者可以控制某个节点的通信，然后欺骗该节点接受看似是来自网络其他节点的虚假数据，这样攻击者就可以欺骗节点浪费资源，或者确认虚假交易；

日蚀攻击将使攻击者更容易发起双重支付攻击

IP下的P2P系统上下拓扑





区块链增强网络基础层的信任

Blockchain – 去中心化维护的安全总帐、分布式共识+密码学技术保证数据安全且一致、…

基于区块链的NDN密钥管理与访问控制方案

- 提出了基于区块链的密钥管理机制，语义层次化授权认证模式将用户公钥及其哈希记到链上
- 设计了公钥的认证、验证、撤销机制
- 解决NDN多层次公钥链的单点失效及独立信任域在没有信任锚情况下相互验证的问题

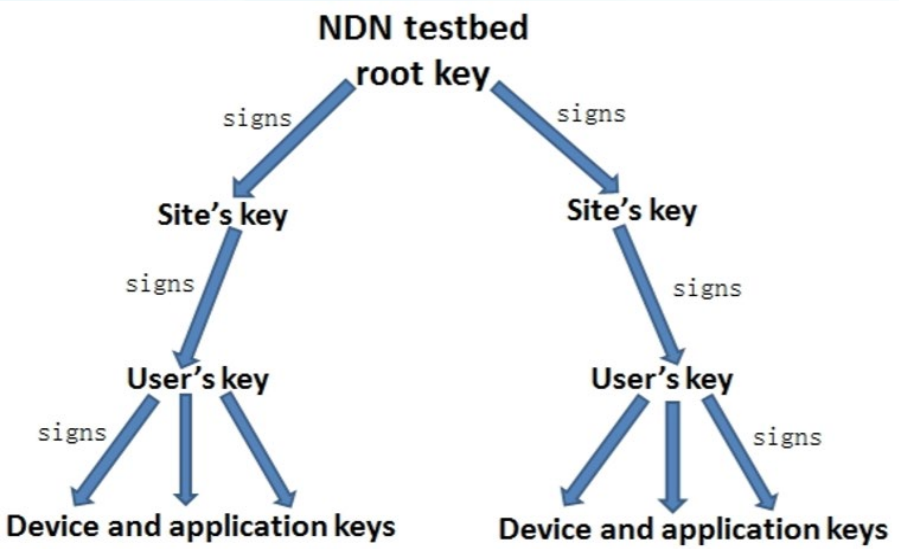


Fig. 1. Key trust model on NDN testbed.

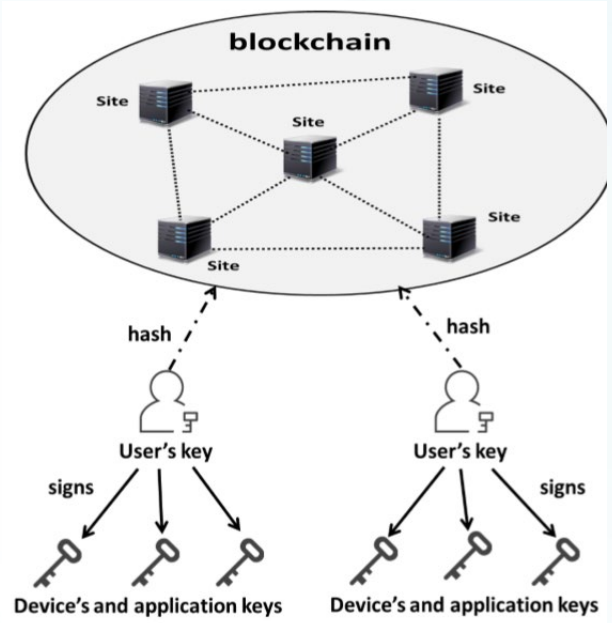
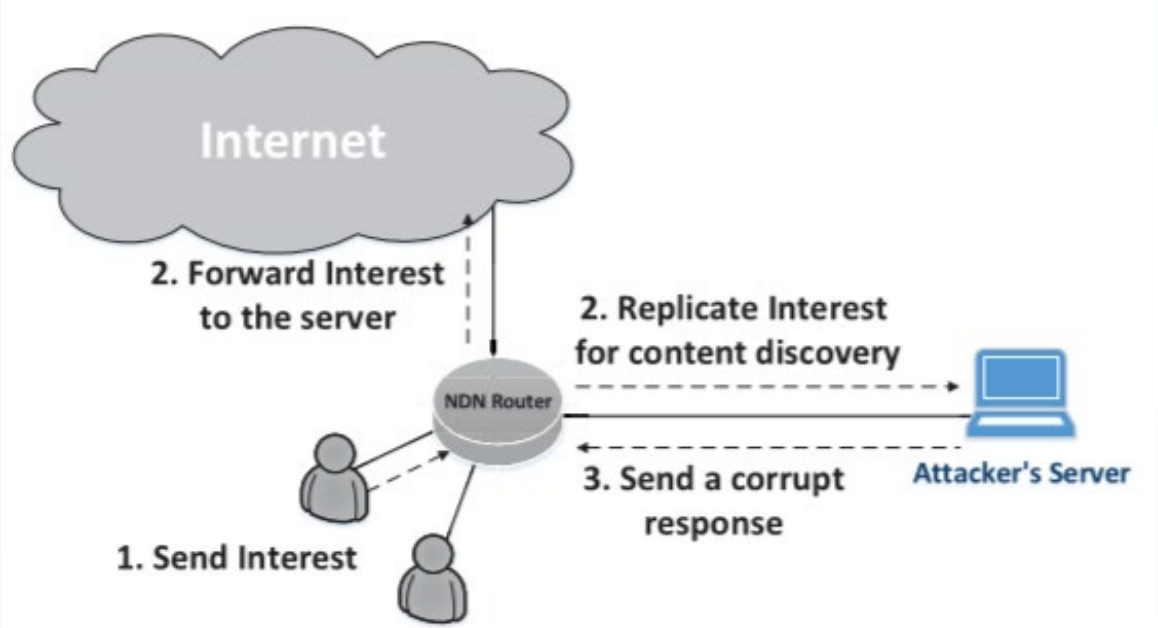


Fig. 3. Blockchain-based key management model for NDN.

案例：区块链与集群无人机

- 使用NDN构建无人机自组网，实现高效内容分发和强数据安全
- 区块链增强NDN-based无人机自组网信任，解决分布式缓存中毒（内容/交易块篡改污染）攻击
  - NDN本身的缓存与数据检索机制带来缓存中毒攻击（信任问题）
  - 需要高效的防御方案来识别和排除假数据



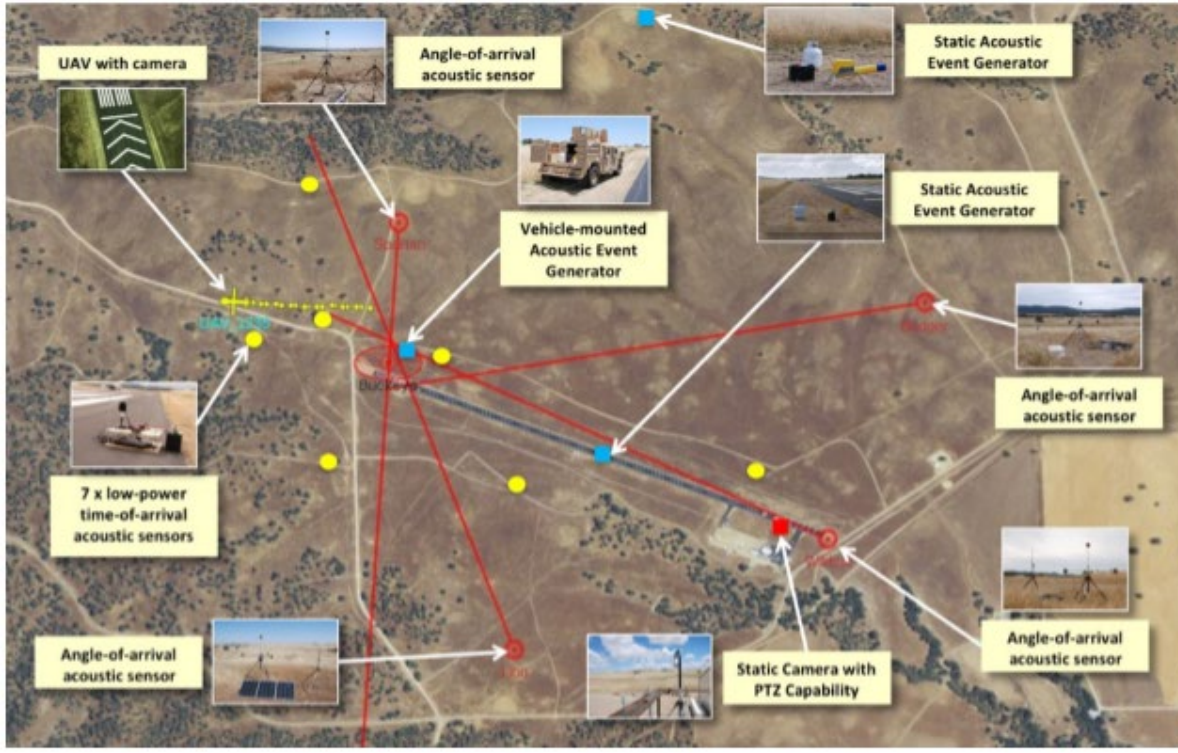
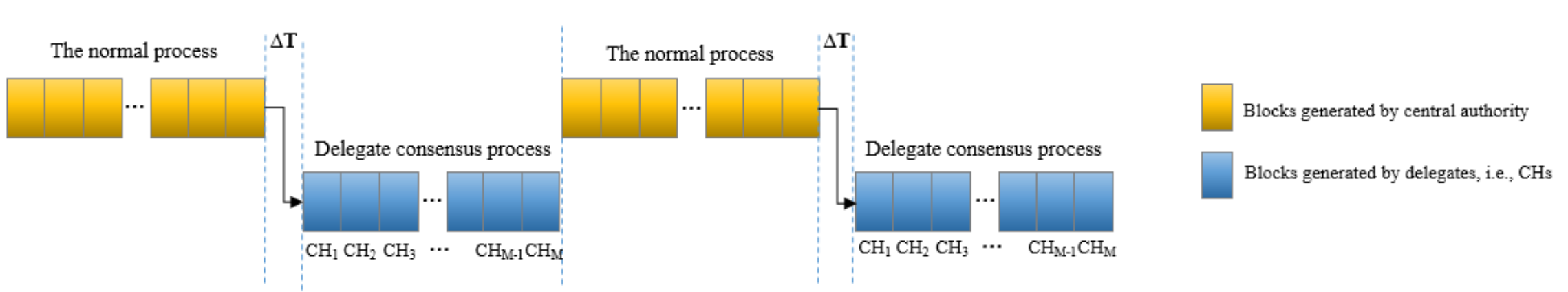


Fig. 1. An example scenario of battlefield information capture and collection from a combination of statically placed and mobile multimedia sen

区块链无人机网络高效防御方案：构建自认证命名来指定所要检索内容的哈希或者发布者身份

- 利用区块链认证用户（CERTIFICATE交易）
- 利用区块链分布式安全存储名字-公钥-哈希的绑定键值对（REGISTER交易）
- 利用区块链共识来确定系统中恶意攻击者的身份（SUSPECT交易）
- NDN上区块链性能优化：自适应代理共识算法（ADCA）



Adaptive delegate consensus algorithm（ADCA）：适用于有中心但中心不完全可靠的场景（协调）

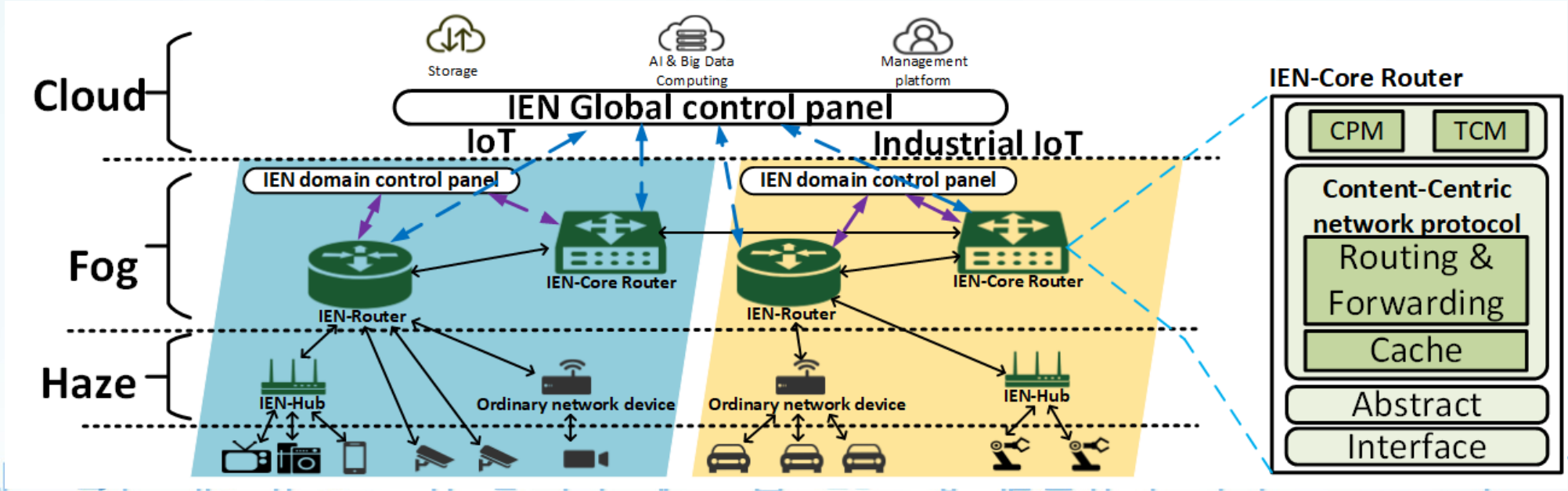
IEN（Intelligent Eco Networking） -- 智能生态网络

核心理念和构想

IEN（Intelligent Eco Networking）是一个以价值内容数据为中心、数据交易驱动、人工智能控制与决策，基于软件定义、虚拟化、可编程设备的技术路线，逐步演进的智联网基础设施；同时综合考量存储、计算、网络成本与收益，融合区块链去中心化共识信任维护、Token化细粒度分配机制构建而成的众享协作联盟、共产共惠的价值互联网产业生态。

IEN 架构和设备

- 网络全维可云化（网络虚拟化硬件设备，兼容异构网络、异质通信）
- 多重控制器系统（负责网络流量的智能控制）
- 内容中心网络协议（实现数据为中心的传输范式）
- 信任管理（保障网络数据包的权责真实可信）
- 云/雾/霾计算组（为网络提供多层级计算资源，公链与子链）



价值内容数据

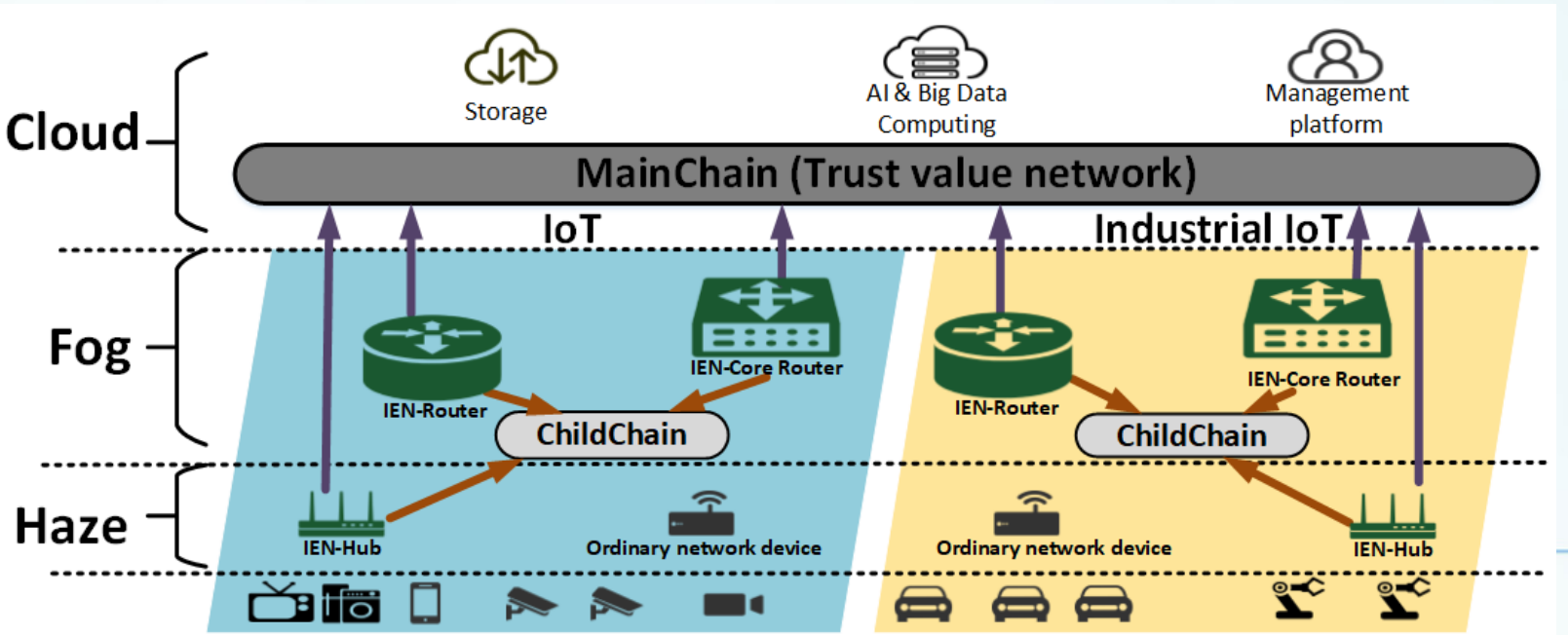
- 数据(data)作为首要考量对象；数据价值权（可复制、不可/不能/不怕复制）
- 为了构建公平互惠的良好联网产业经济，IEN聚焦于节点创造的信息本身带来的价值（去无效/垃圾流量），支持网络精确利用率的经济结算；
- 这些包含有价值的信息即以价值内容数据的形式呈现，有三个特点：

1. 多种不同的数据结构(来自不同物联网设备的有价内容数据采用不同编码或压缩格式)；
2. 网络节点共同认可和维护的数据价值评价计量体系；
3. 交易细粒度结算：价值内容数据直接用于交易。由于价值内容数据本身可以直接作为交易对象，实现跨价值系统的价值维护和流通。交换和共享数据是数字转型的规模化和更成熟阶段的创新和转型的关键。

IEN 区块链共识维护价值体系

- Proof of Valuable Content Sharing（PVCS）：核心思想是网络设备为有价值数据花费的计算和存储资源越多，越可能分配到记账权
- PVCS面向物联网采用Directed Acyclic Graph (DAG)的数据结构来实现分布式、不可逆的信息传递。同时VRF作为一种基于密码学的新型共识模型，PVCS算法可利用VRF增强物联网共识网络的可扩展性。
- 立体分层主/子链架构解决扩展性问题

- 数据需求方（云层）提供一个可靠的全局一致的主链；
- 数据拥有方（雾层）提供各种功能或业务的子链；
- 数据产生方（霾层）直接与主链或子链交互，数据上联盟或者私有链。



IEN 区块链的Token细粒度量化分配

- 联网产业经济实现共惠共利的首要前提是可信赖的数据内容的价值评估和有效的激励机制来计划token的发行与分配
- Token的作用：智能终端的激励、数据二次开发交易
  - 在生态内的流通代表了生态价值的形成过程，是token的一级市场；
  - 在生态外通过互联网流通和交易代表了生态的市场价值，是token二级市场
- 区块链中的Token承载可权益量化的价值。
- 通过区块链进行交易的流通过程实现了价值的维护和流通
- 内容中心未来网络与细粒度的Token联合解决了确权、量权、确责问题

China Blockchain Conference

Thanks for your attention!

Q&A

区块链 – 阿凡达梦境文明（和中心）之魂

信息中心网络 – 潘多拉世界砥砺之基（千里马）

leik@pku.edu.cn