万维网 (WWW) 的历史，
区块链 (Blockchain) 的未来

Welcome to PPk pub!

ppkpub@gmail.com
http://ppkpub.org
ppk:0

关于 PPkPub

PPk 这个名称来源于 Peer-Peer network 即“对等去中心化网络”的缩写。

我们不是一个创业团队，而是一个兴趣驱动的专注“创造”的开放技术极客小组，依托北京邮电大学网络与交换技术国家重点实验室网络管理研究中心的深厚学研资源，集合了一群对比特币等加密货币感兴趣的 P2P 技术爱好者，小组成员多具有 10 多年以上通信和互联网行业技术研发从业背景，对于互联网业态的发展趋势有着独立判断和独特理念。相比数字加密货币的价格起伏，我们更关注其中以区块链为代表的创新技术的潜在价值，并尝试将区块链与网络通信领域跨界融合来做一些有意思的事情！

分享主题

- 回顾万维网成功对区块链发展的启示
- 网络通信 + 区块链的跨界融合
- 实践案例分享

区块链技术存在的价值基础

- 互联网：改变传统电路通讯的分组转发通讯机制

  → 支持全球点对点、高效可靠的数据传递

- 比特币：第一个组织形式上去中心化，逻辑上却能达成一致性的点对点电子现金系统

  → 全球点对点、可信的支付

- 区块链：改变传统中心化信用授权机制，自主、无需第三方达成共识的信息权属证明

  → 全球点对点、可信的价值信息传递

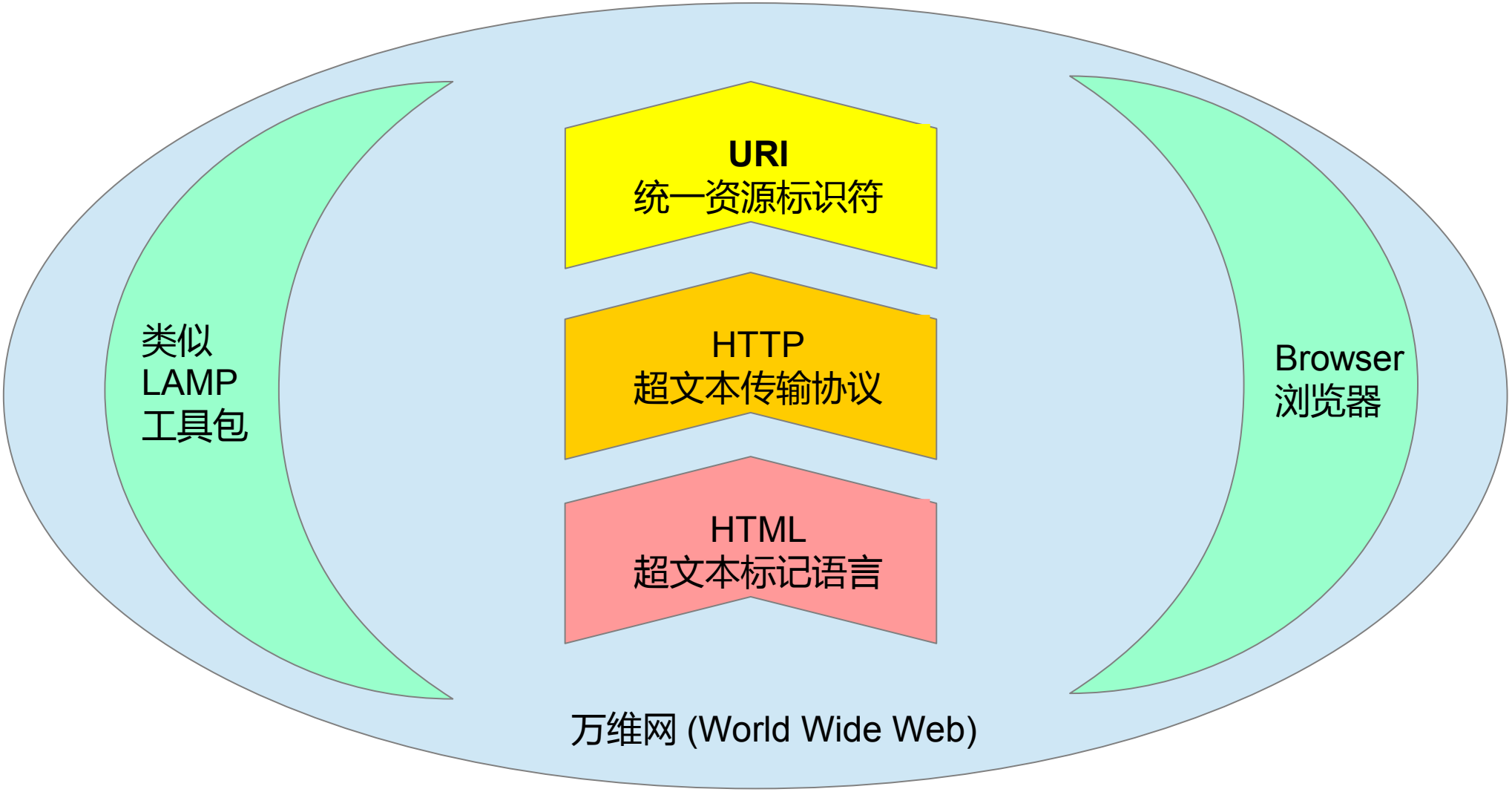
PPIC

万维网发明的背景

- 1945 年，范内瓦 · 布什（ Vannevar Bush) 提出 “ Memex” 设想，基于微缩胶卷交叉引用查询的信息系统
- 1965 年，泰德 · 尼尔森（ Ted Nelson ，超文本发明人）的仙那度计划 (Project Xanadu) ，第一个超文本项目
- 1968 年，道格拉斯 · 恩格尔巴特（ Douglas Engelbart ，图灵奖得主，鼠标发明人）的 oN-Line System (NLS)
- 1969 年， ARPANET 启用
- 1971 年，电子邮件 (Email) ，文件传输协议 (FTP)
- 1974 年，传输控制协议 (TCP)
- 1978 年，网络互联协议 (IP)
- 1979 年， UNIX 至 UNIX 拷贝协议 (UUCP)
- 1980 年， Tim 在欧洲核子研究组织 (CERN) 写了 Enqiure 超链接程序，但还只是本地单机程序
- 1984 年， CERN 开始建立自己的 CERNET
- 1984 年，域名系统 (DNS) 实现
- 1980 年代中期， ARPANET 逐渐进入民用
- 1980 年代晚期， TCP/IP 逐步取代其他协议，成为因特网的共同基础
- 1989 年，边界网关协议 (BGP) ，因特网的路由成为一个去中心化自治的分布式系统
- 1989 年， CERNET 终于通过 TCP/IP 和外部网络接通
- 1989 年， Tim 提出 Web 计划
- 1990 年， ARPANET 停止，被民用的 NSFNET 取代（后者在 1995 年被停止，因特网全面完成民用化）
- 1990 年， Dynatext ，标准通用标记语言 (SGML) 发布工具出现。 SGML 影响了 HTML 的发明。
- 1990 年， Tim 开始开发 Web
- 1991 年， Gopher 协议在明尼苏达大学被发明和实现出来
- 1991 年， Think Machines 公司开发了 WAIS （ Wide Area Information Servers ）协议，在 Unix 上开源

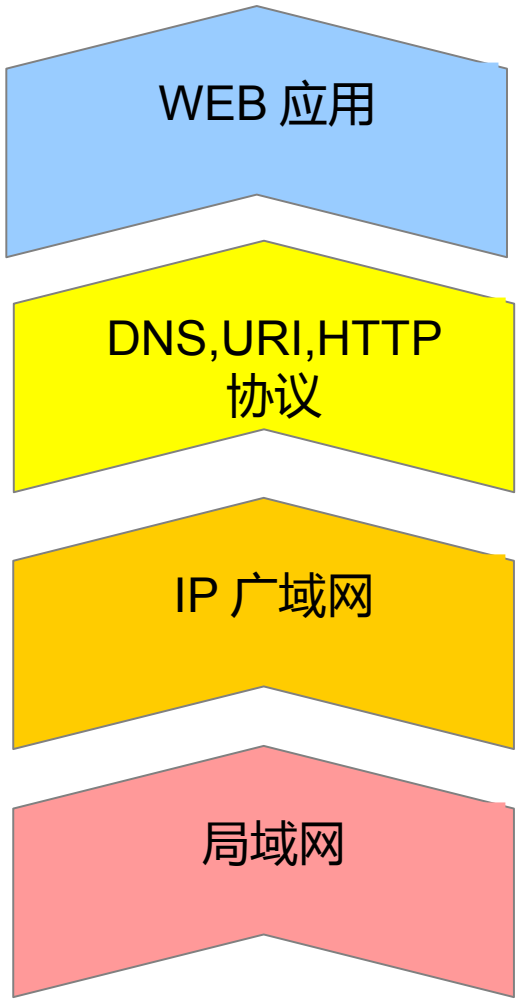
- 1991 年， Tim 正式对外发布了万维网 (WWW)

万维网成功的核心要素



开放、自由互联的可扩展性

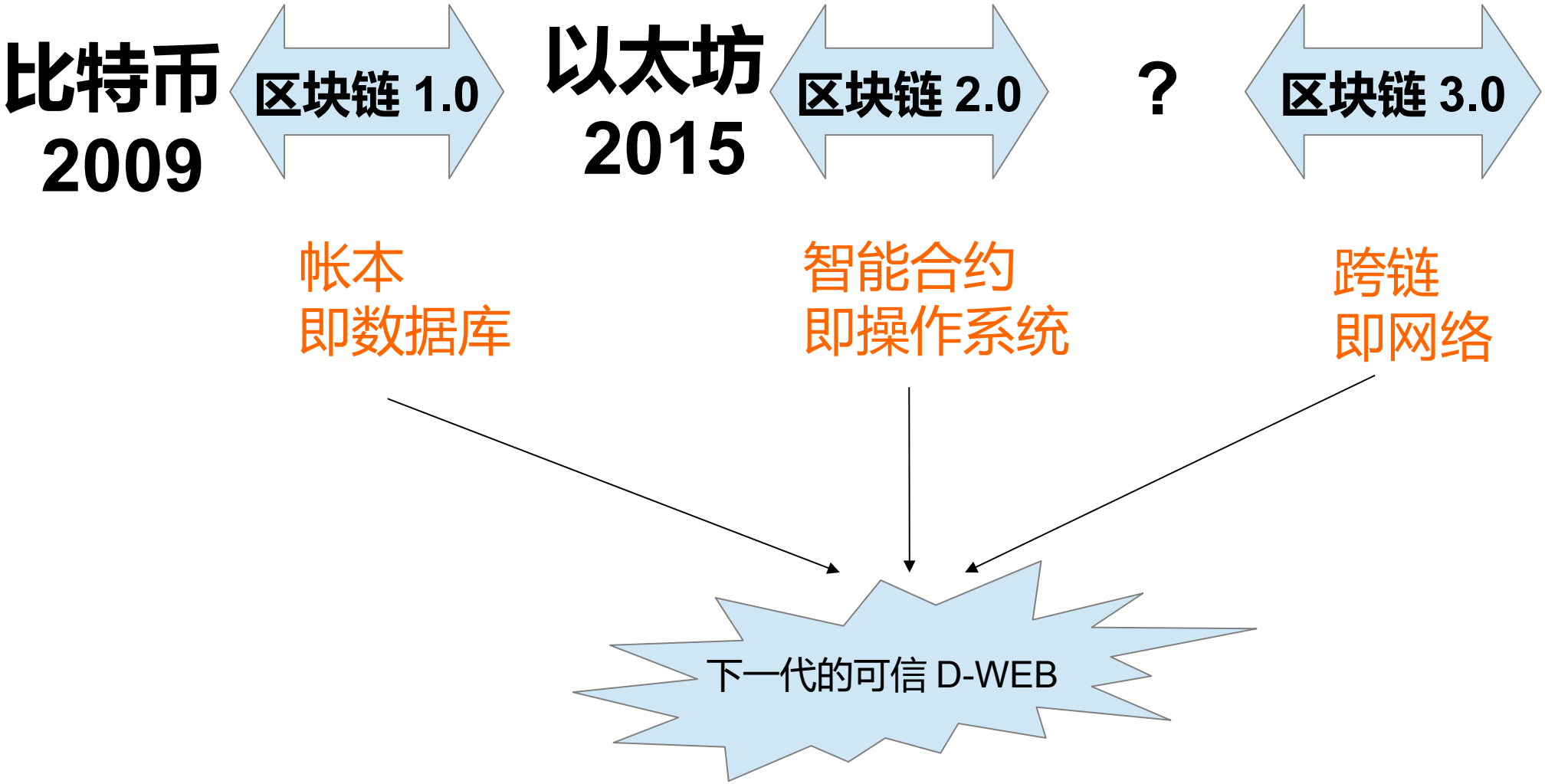
1+1>2：万维网对区块链业态的启示



传统互联网

对等可信的下一代互联网

区块链技术发展趋势


比特币
2009
区块链 1.0
以太坊
2015
区块链 2.0
？
区块链 3.0
帐本
即数据库
智能合约
即操作系统
跨链
即网络
下一代的可信 D-WEB

当前，互联网基于 IP 网络，
是传输通道。
不会变吗？

IP 体系结构面临的问题

1 ）可扩展性问题

网络流量激增的速度远远超过摩尔定律与路由器性能提升速度。

2 ）安全性问题

目前互联网针对安全问题不是一个系统性的解决方案，基本处于被动应对状态。

端到端的通信模式注定了只能提供数据安全通道，无法实现针对服务及内容的个性化安全服务

3 ）动态性问题

互联网终端形态发生了很大变化，动态性显著增加。

IP 地址既表征身份又表征位置，导致对移动性支持能力不强。

多种解决思路

- 演进式：
  - IPSec
  - DNSSec
  - IPv6
  - .....
- 变革式：
  - ICN/NDN ：面向可扩展性
  - MobilityFirst ：面向动态性
  - Nebula ：以云计算为中心的结构
  - SOFIA ：面向服务
  - ……

NDN ：启引下一代互联网

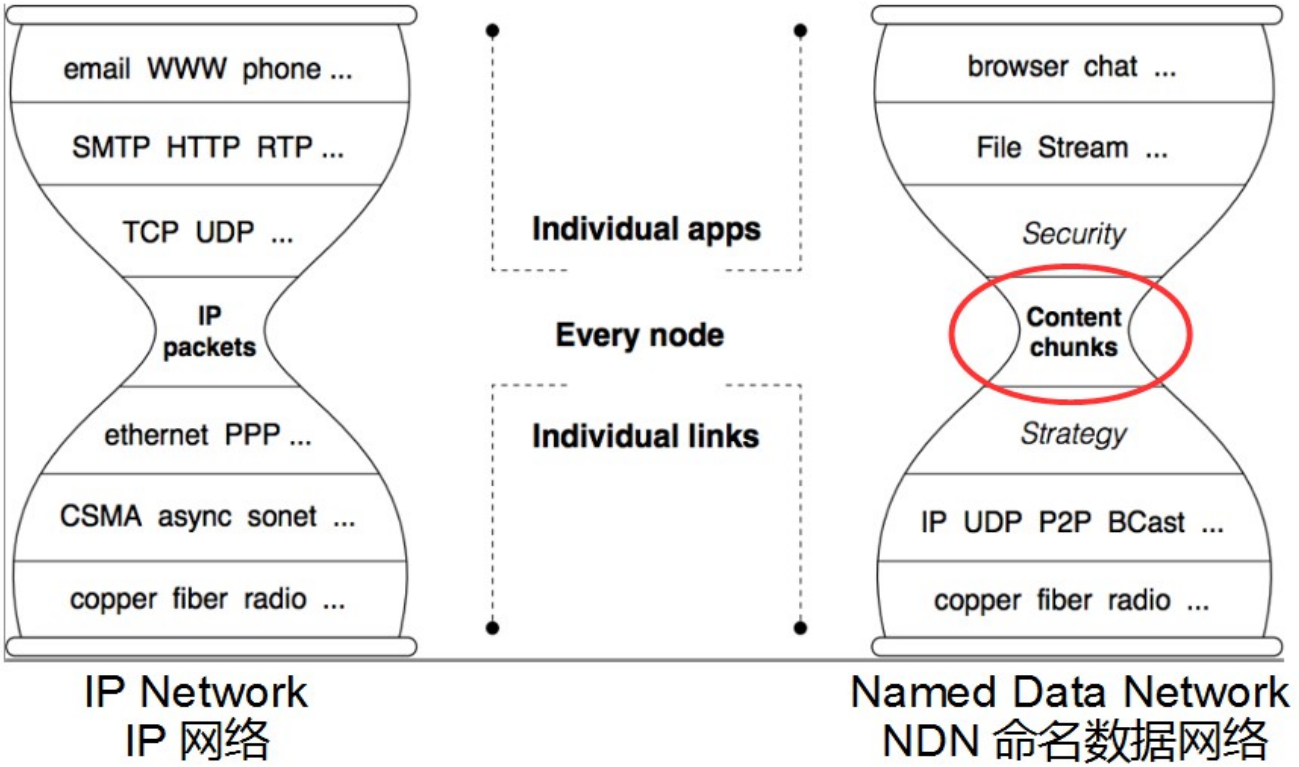
- NDN （ Name Data Network ，命名数据网络）：
  未来互联网体系架构 (FIA) 研究项目之一， 2010 年由美国国家自然科学基金会（ NSF ）设立。

面向主机→面向内容（ where → what ）

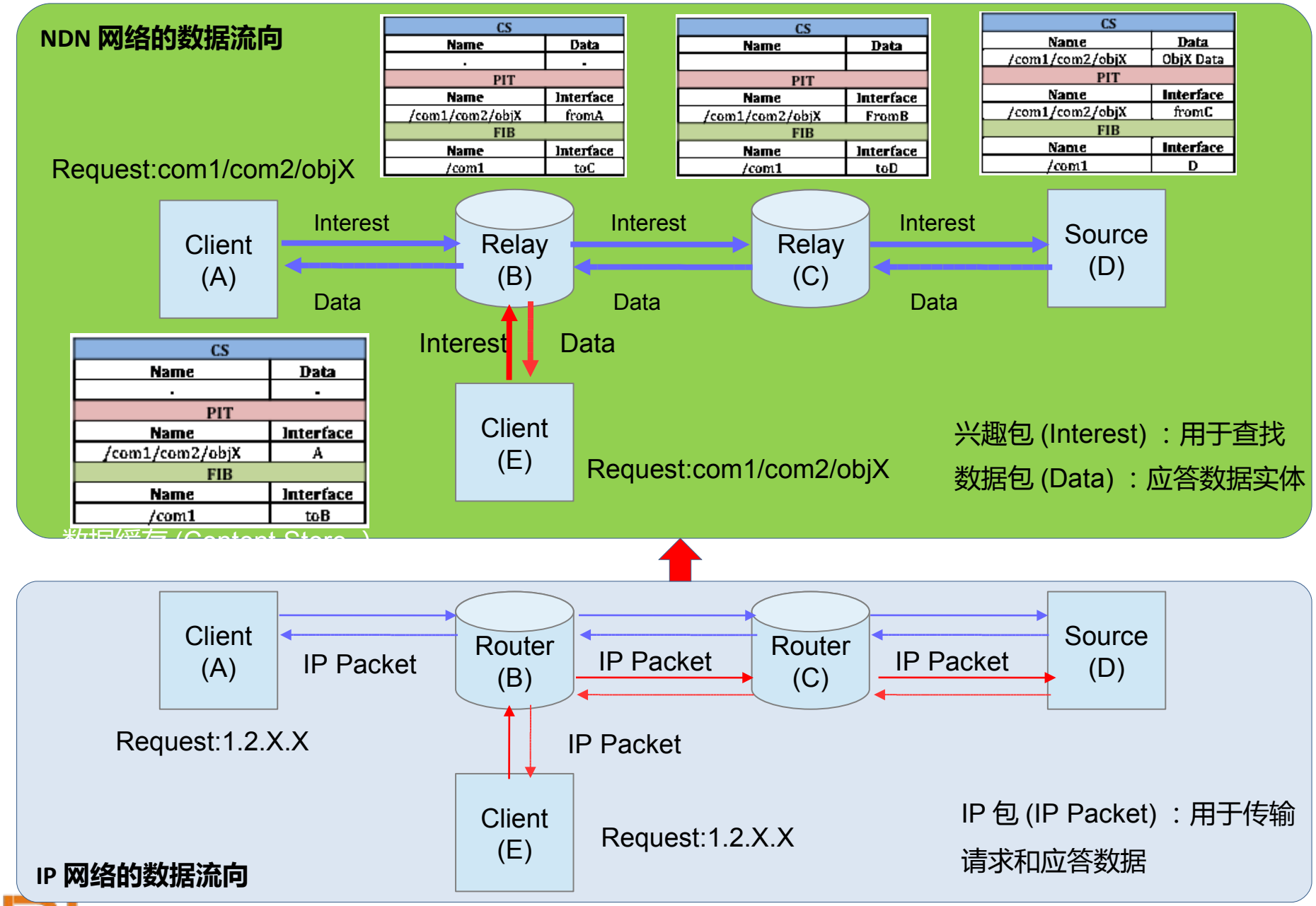
Named host → Named data ，变为以内容为中心

以内容标识定位内容，不需要位置相关地址

缓存复用

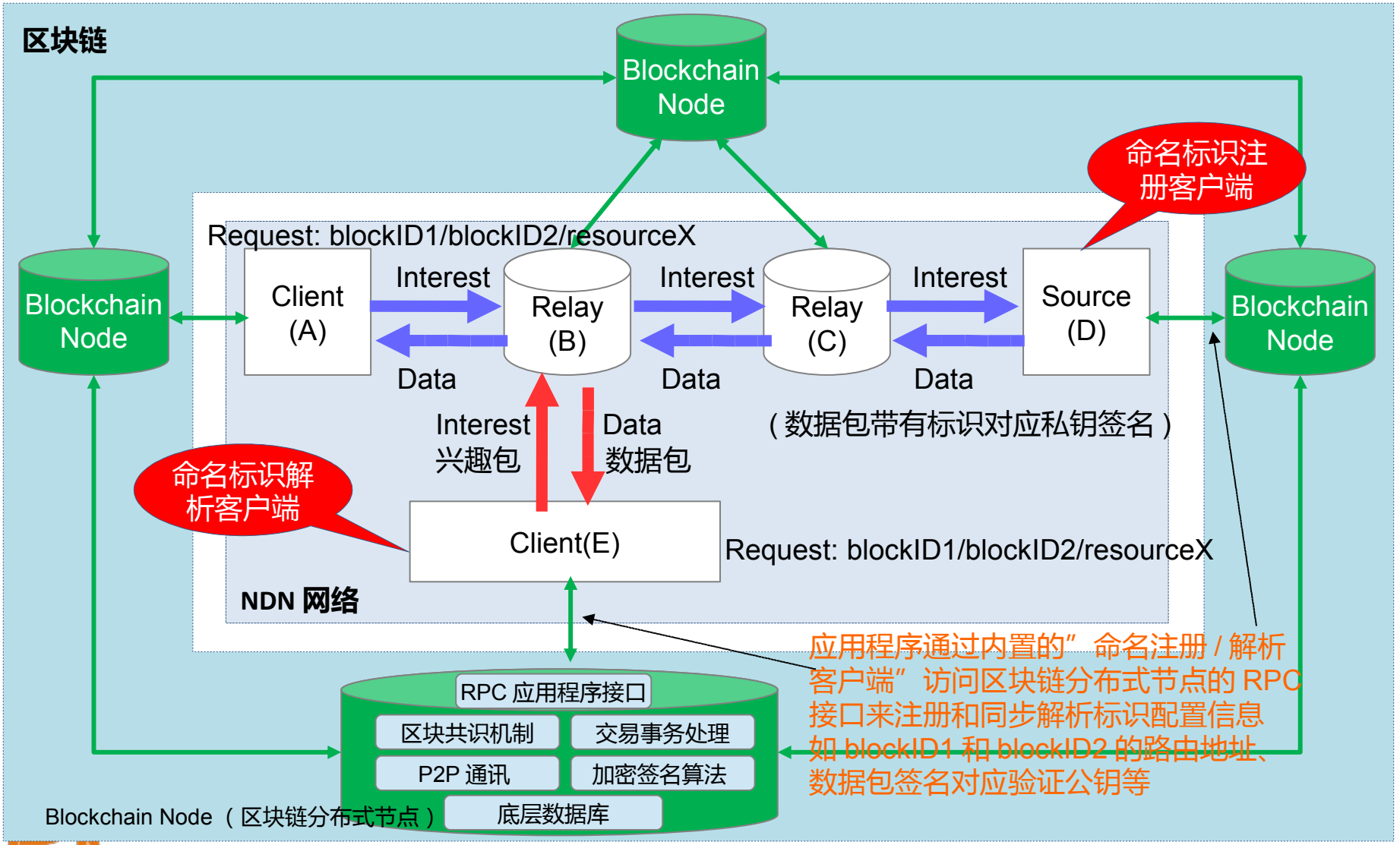


NDN 与 IP 网络架构对比

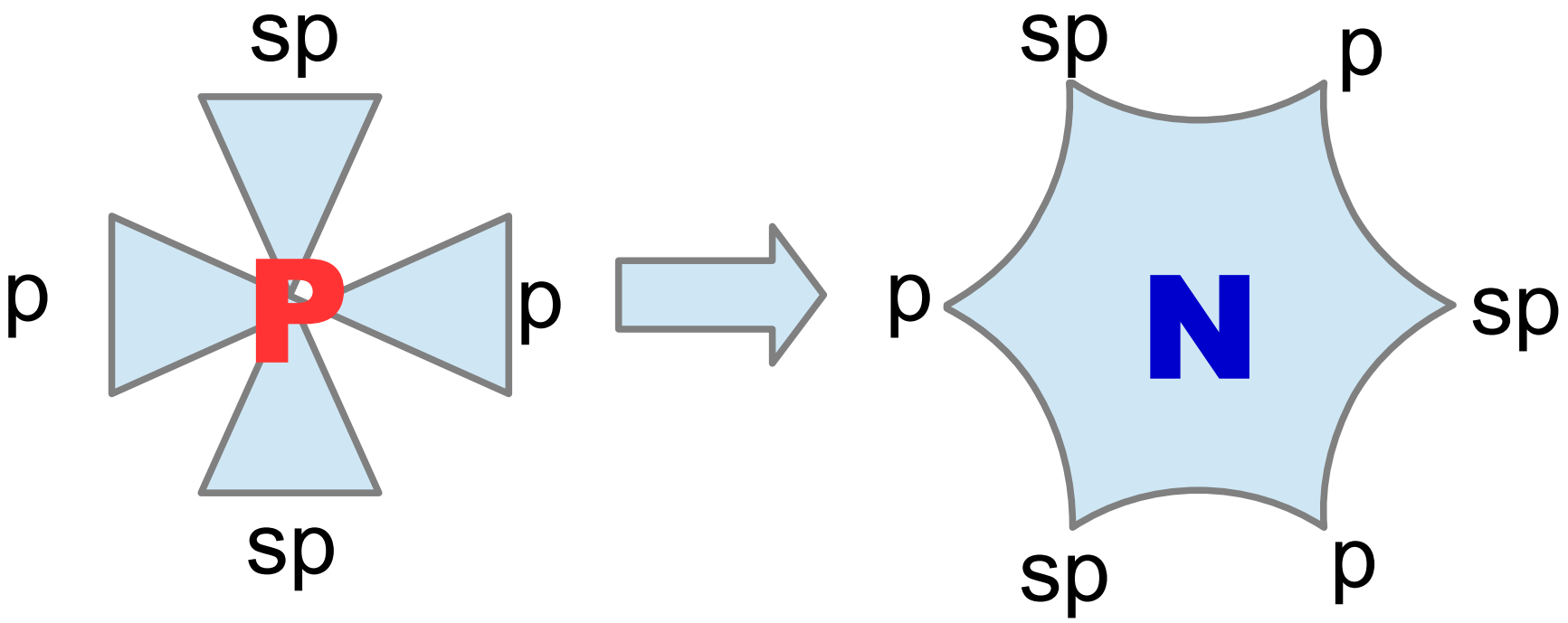


NDN+Blockchain: 融合的关键点

将基于区块链的命名标识和寻址解决方案融合到 NDN 体系框架，充分发挥区块链技术的可信、不可篡改特性。



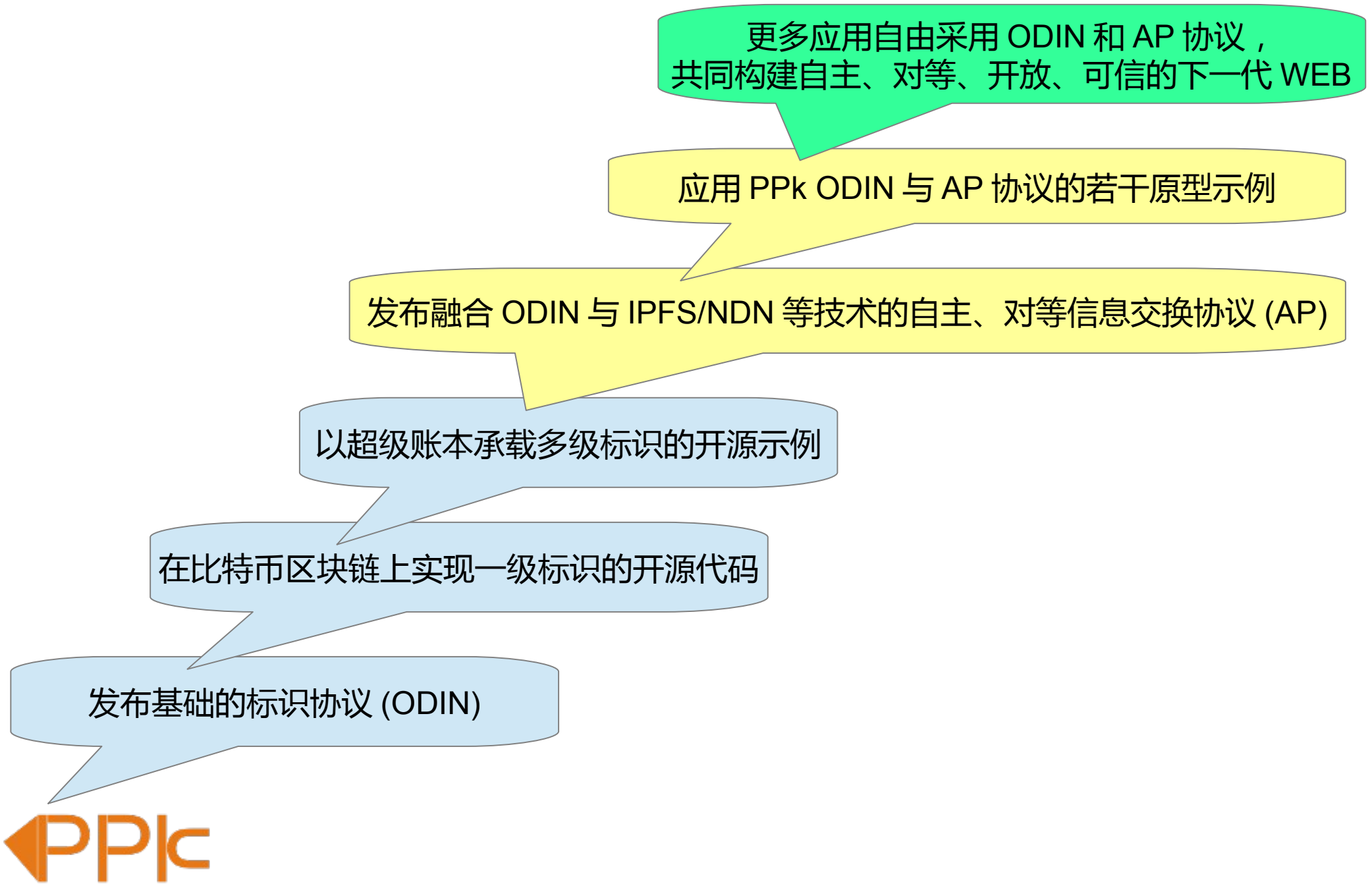
pNp: 网络即平台、网络即数据



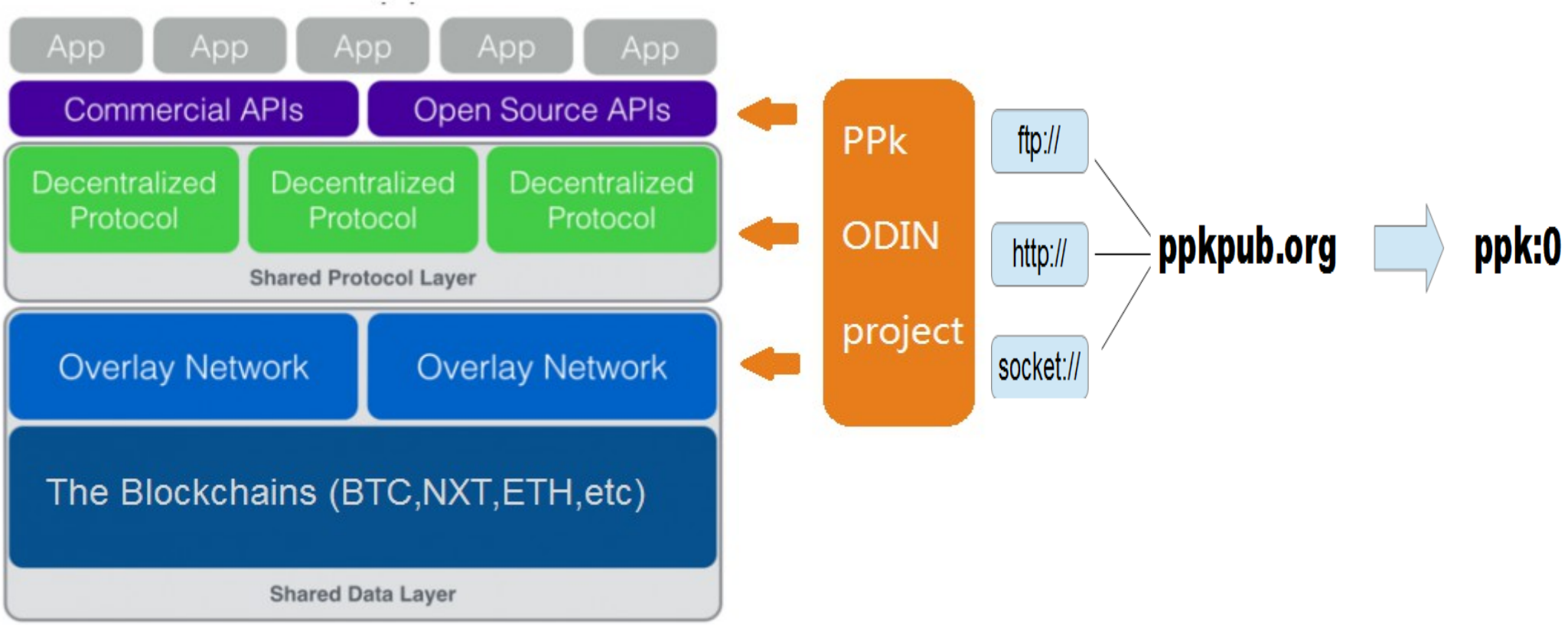
从“ pPp”这样的伪 p2p 到真正的失控“ pNp”

NDN+Blockchain 将推动互联网迈入“网络即平台、网络即数据”的新业态

从标识起步 ：PPkPub 的开放推进思路



ODIN: 融合多区块链的新型 DNS



ODIN(Open Data Index Name) 是基于区块链（ BlockChain ）定义的“数据时代的去中心化 DNS”，是在网络环境下自主命名标识和交换数据内容索引的一种开放性系统，遵从 URI(统一资源标识符) 规范。

ODIN 相比传统 DNS 的特点

自 主

唯 一

安 全

永 久

ODIN 与其它基于区块链的标识类解决方案的差异

	ODIN	Namecoin	Onename
基础区块链	Bitcoin	Namecoin	Namecoin → Blockstack based Bitcoin
多级扩展	灵活扩展多级标识引入其他区块链（公有链、联盟链、私链等）	--	--
命名方式	用区块记录位置作为名称标识，确保唯一性	抢注字符串	抢注字符串

可预见的应用场景之一：物联网

数据形态：数源孤立、信息孤岛

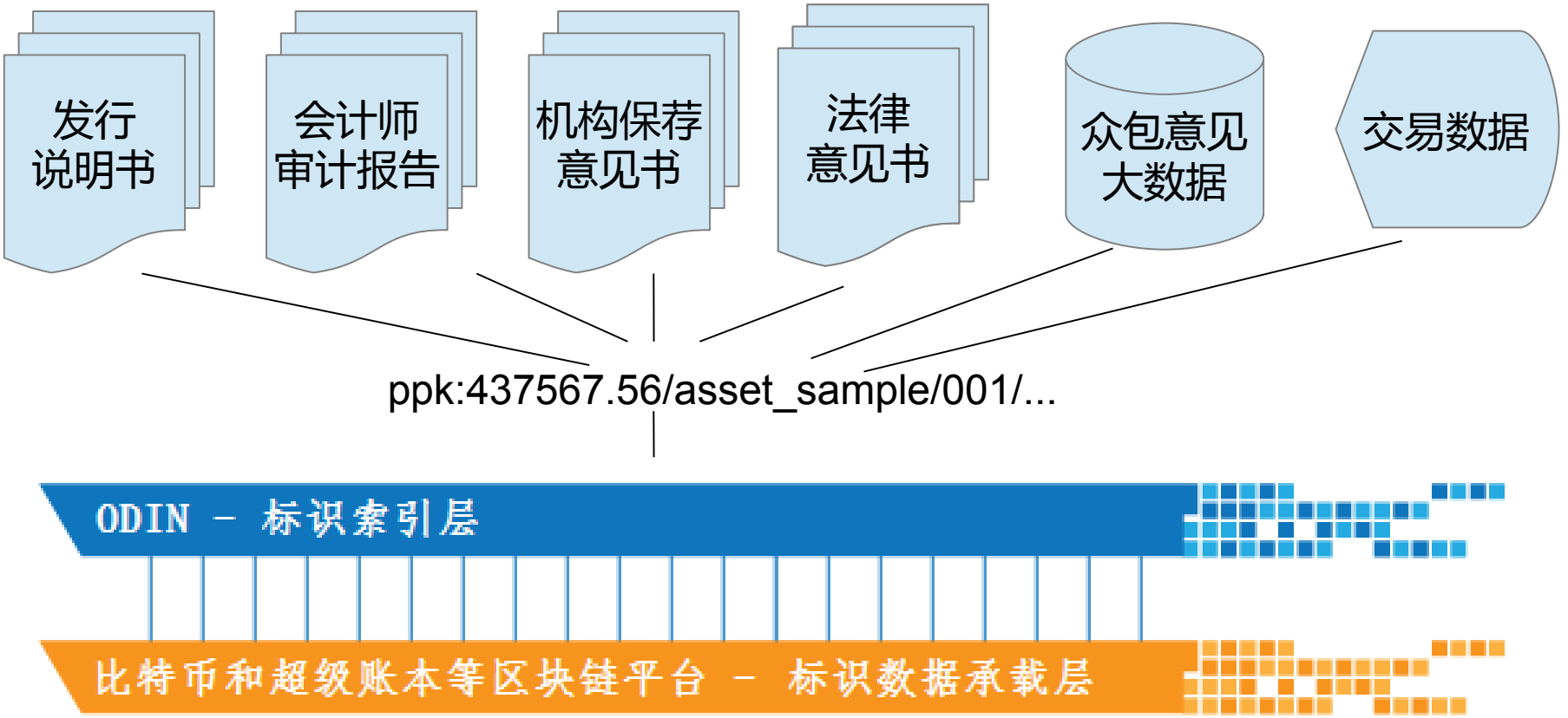
技术缺陷：采用传统的基于 MAC 地址的 IP 组网方式，应用层面对不同形态子网络，难以跨子网络灵活、实时访问所需数据。

+ ODIN/Blockchain

数据形态：万物互联、实时共享

技术优势：采用融合 ODIN/Blockchain 和 NDN 设计的网络通讯协议，实现跨动态网络、跨不同协议的平滑切换及达成数据交换。

可预见的应用场景 之二：数字资产市场



Welcome to **PPk** pub.

We love **P**2**P** networ**k**.

drive the future of P !

ppkpub@gmail.com
http://ppkpub.org
ppk:0