

区块链与网络通信的跨界融合和实践

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

- ▣ 区块链技术的关键价值
- ▣ 网络通信 + 区块链的跨界融合
- ▣ 实践案例分享

比特币 / 区块链：开天辟地

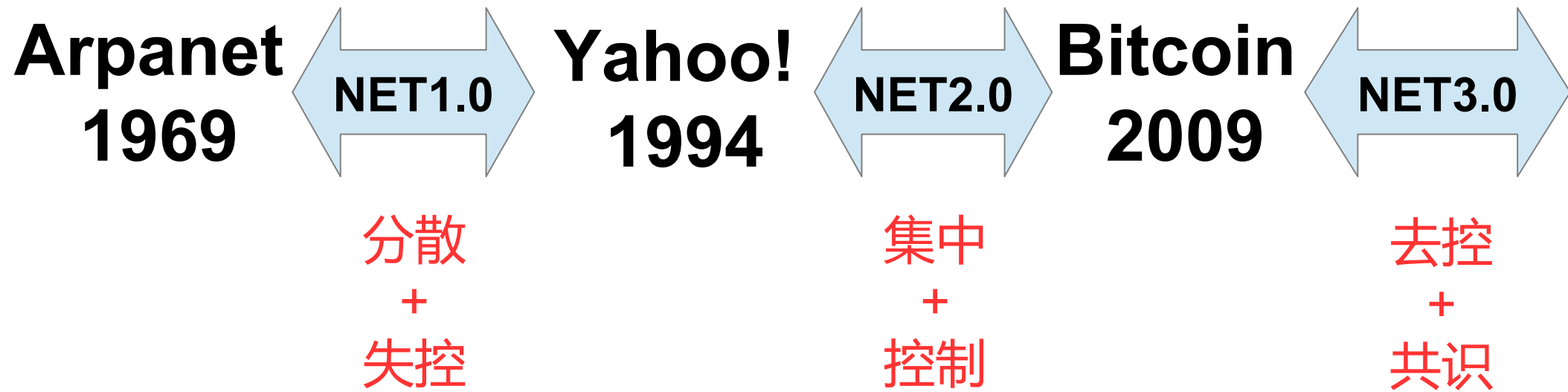
比特币 / 区块链是历史上第一个



组织形式上去中心化，
业务逻辑上达成一致性

的源创案例。

互联网的历史和趋势



万维网的历史和趋势

WWW
Mosaic
1990s



GET

Facebook
Twitter
2000s



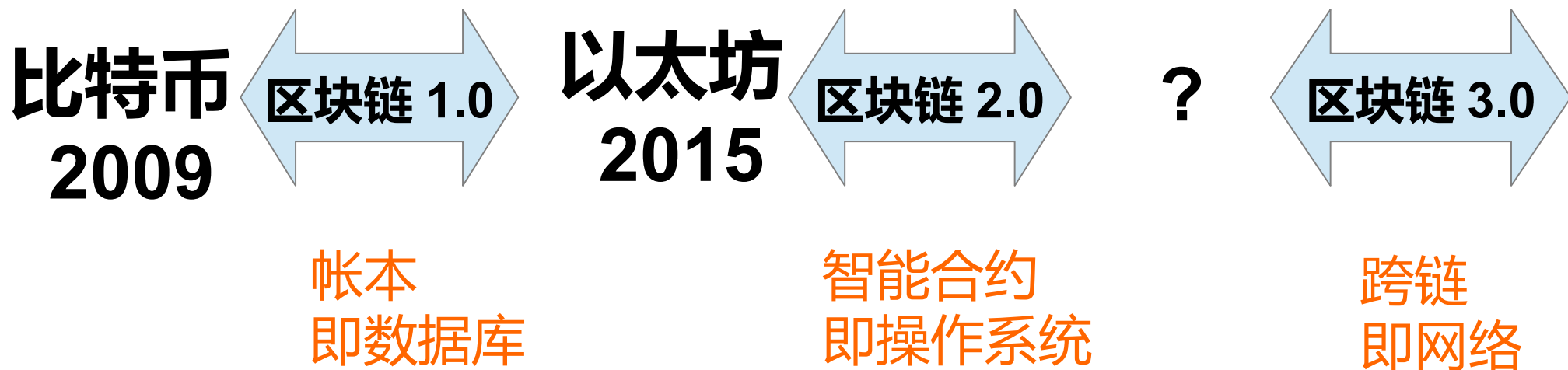
UGC

?
201X

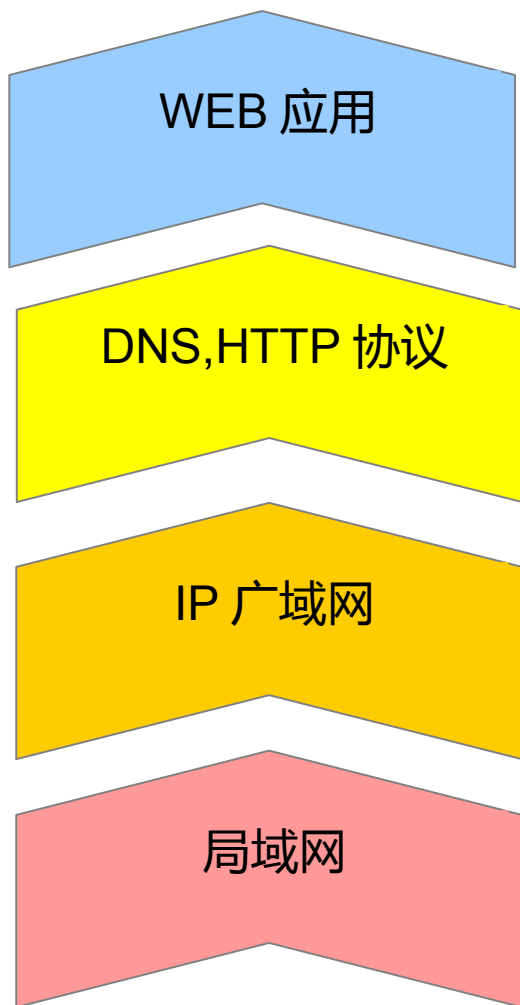


Peer-Peer

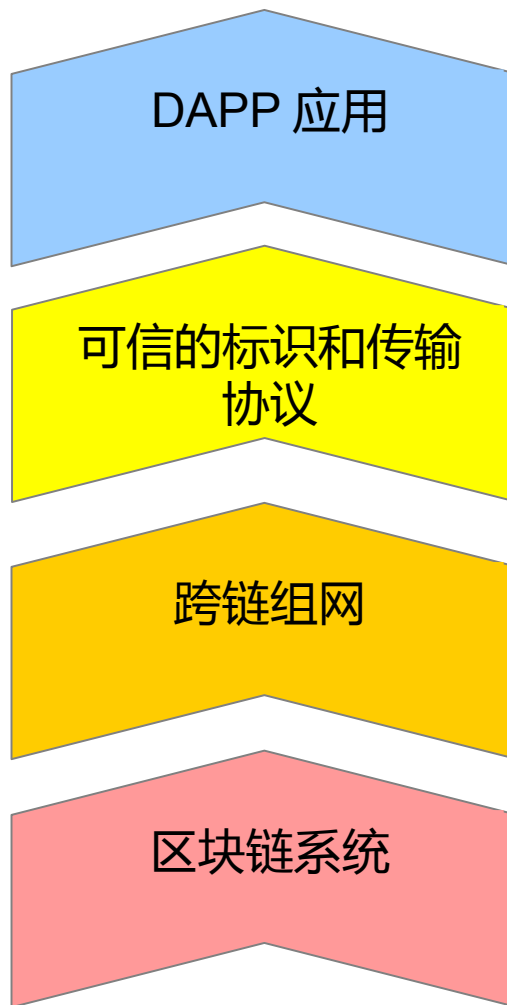
区块链技术发展趋势



1+1>2: 区块链价值发挥关键



传统互联网



可信互联网

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
-

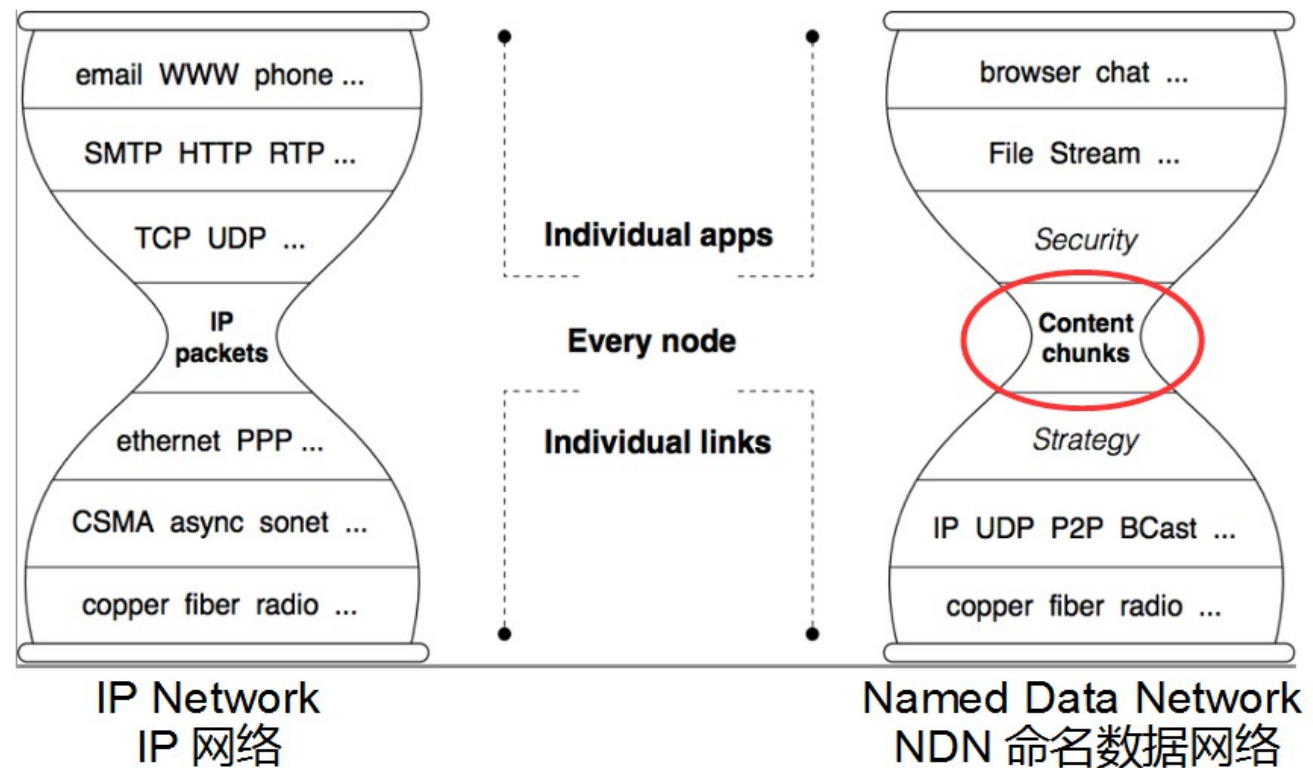
NDN : 启引下一代互联网

- 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

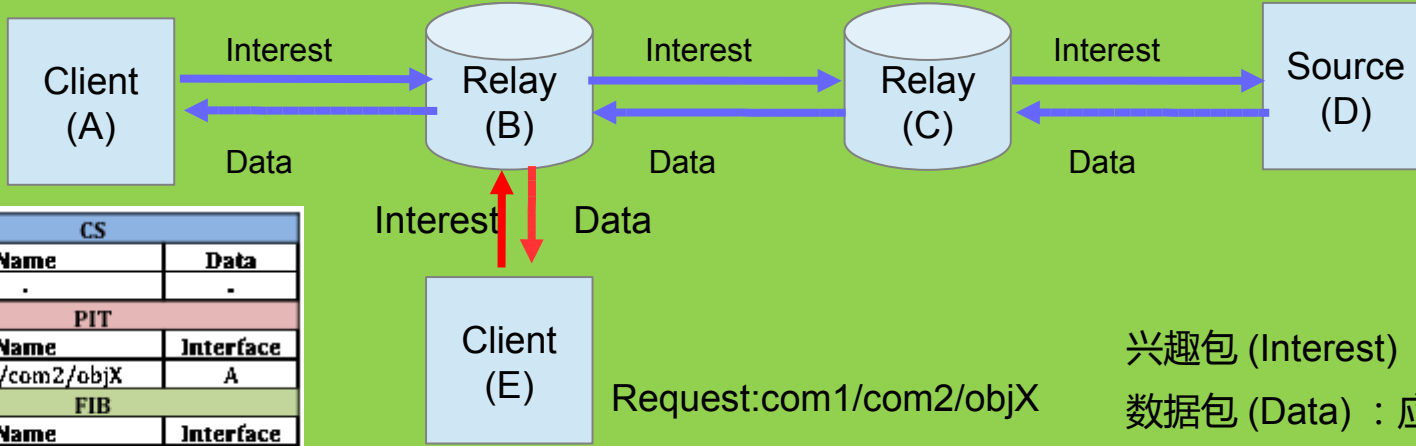
NDN 网络的数据流向

Request:com1/com2/objX

CS	
Name	Data
.	.
PIT	
Name	Interface
/com1/com2/objX	fromA
FIB	
Name	Interface
/com1	toC

CS	
Name	Data
.	.
PIT	
Name	Interface
/com1/com2/objX	FromB
FIB	
Name	Interface
/com1	toD

CS	
Name	Data
/com1/com2/objX	ObjX Data
PIT	
Name	Interface
/com1/com2/objX	fromC
FIB	
Name	Interface
/com1	D

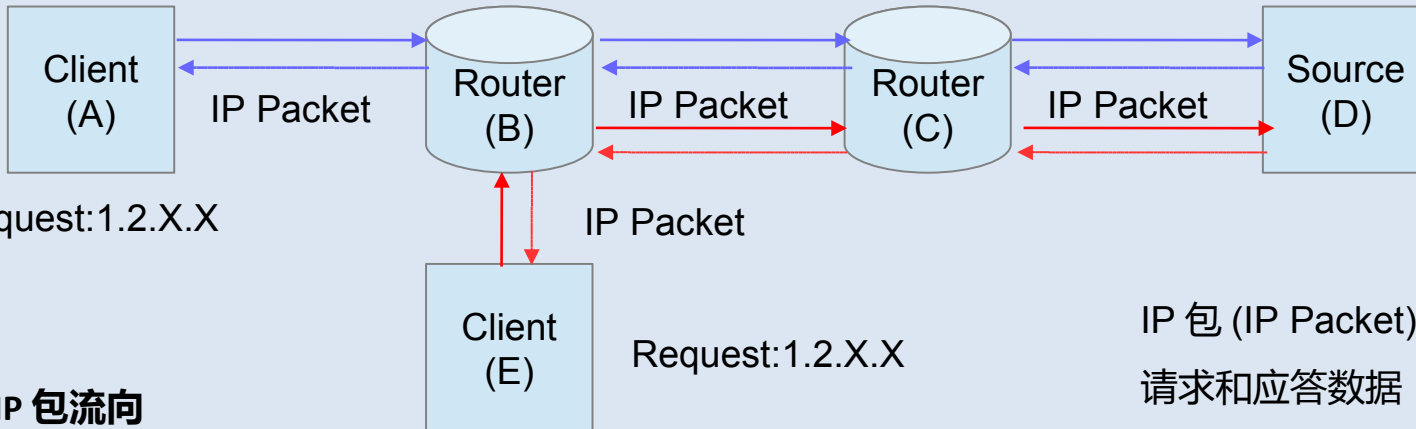


兴趣包 (Interest) : 用于查找
数据包 (Data) : 应答数据实体

IP 网络的 IP 包流向

Request:1.2.X.X

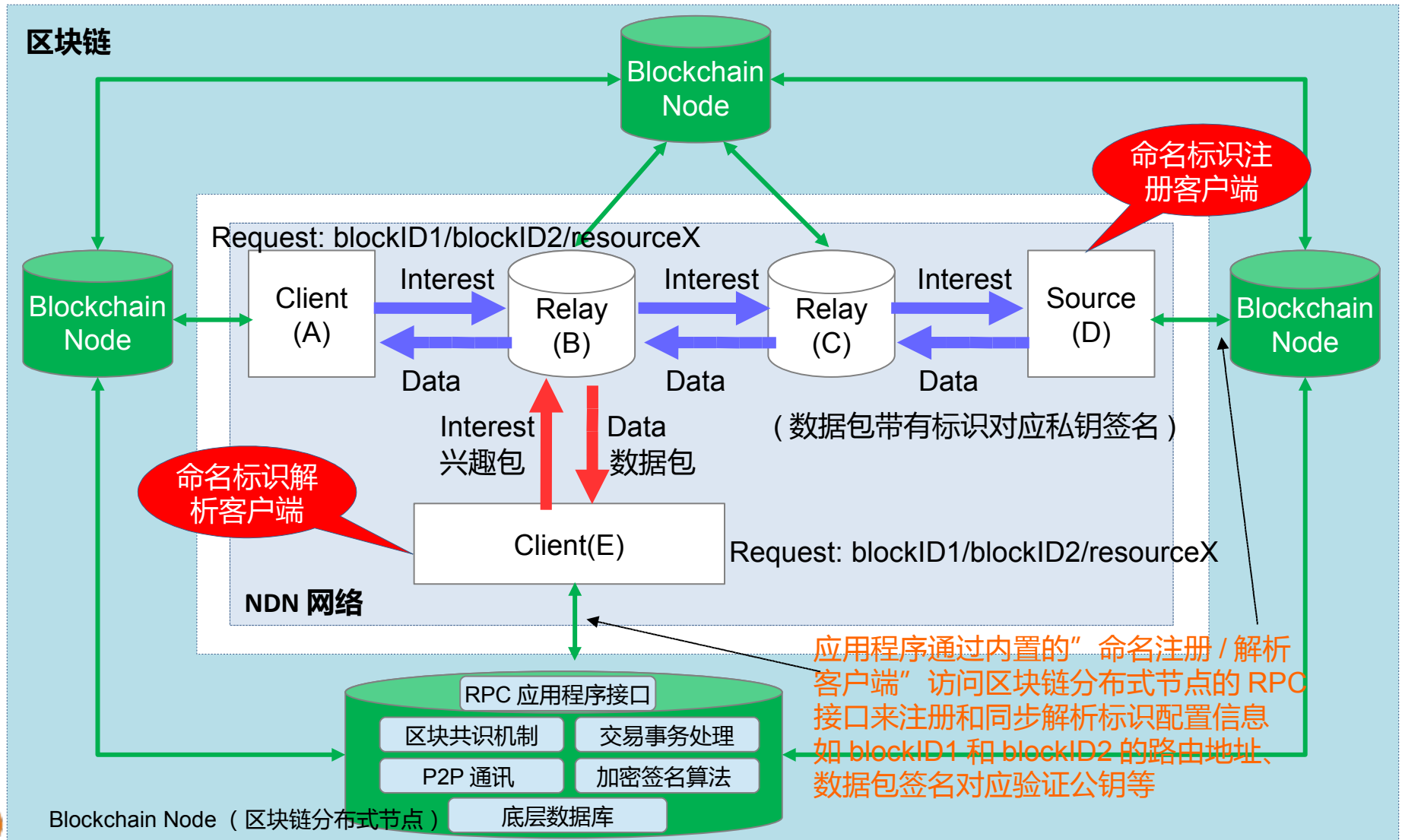
Request:1.2.X.X



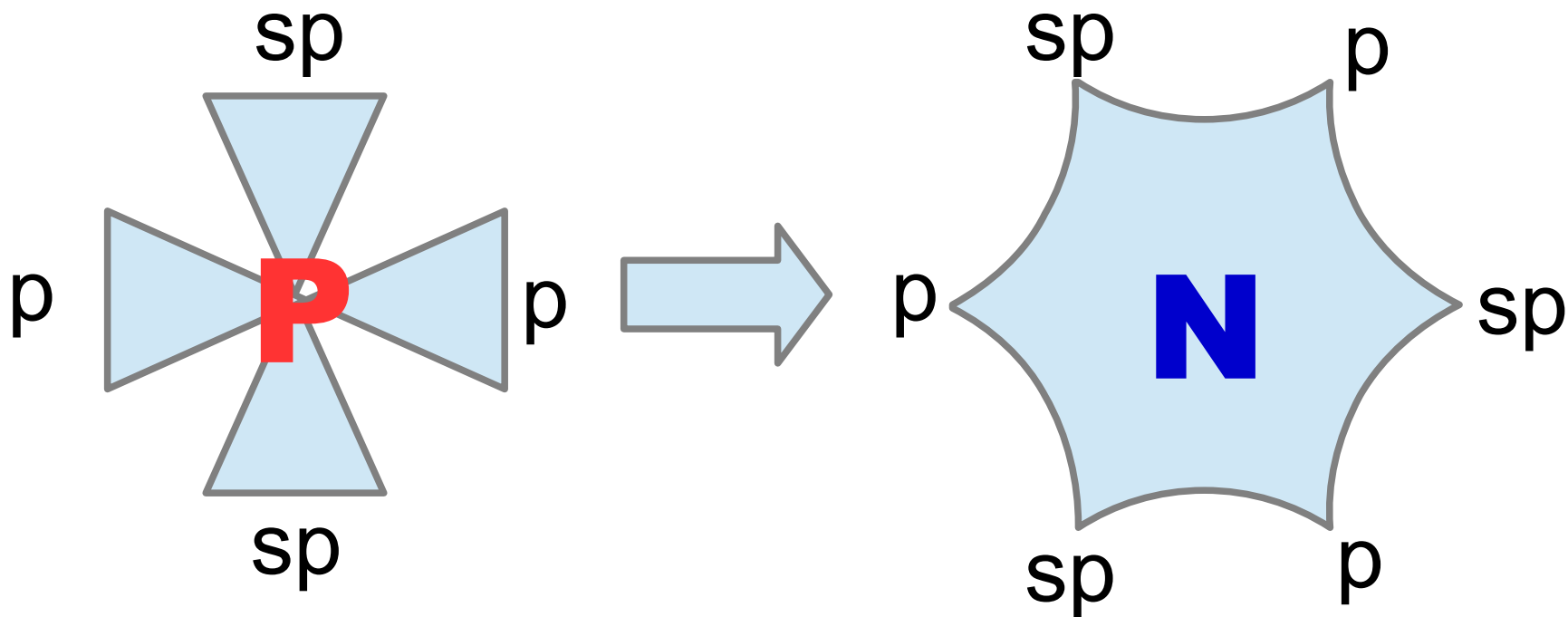
IP 包 (IP Packet) : 用于传输
请求和应答数据

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

更多应用自由采用 ODIN 和 AP 协议，
共同构建自主、对等、开放、可信的下一代互联网

应用 PPk ODIN 与 AP 协议的若干原型示例

发布融合 ODIN 与 IPFS/NDN 等技术的自主、对等信息交换协议 (AP)

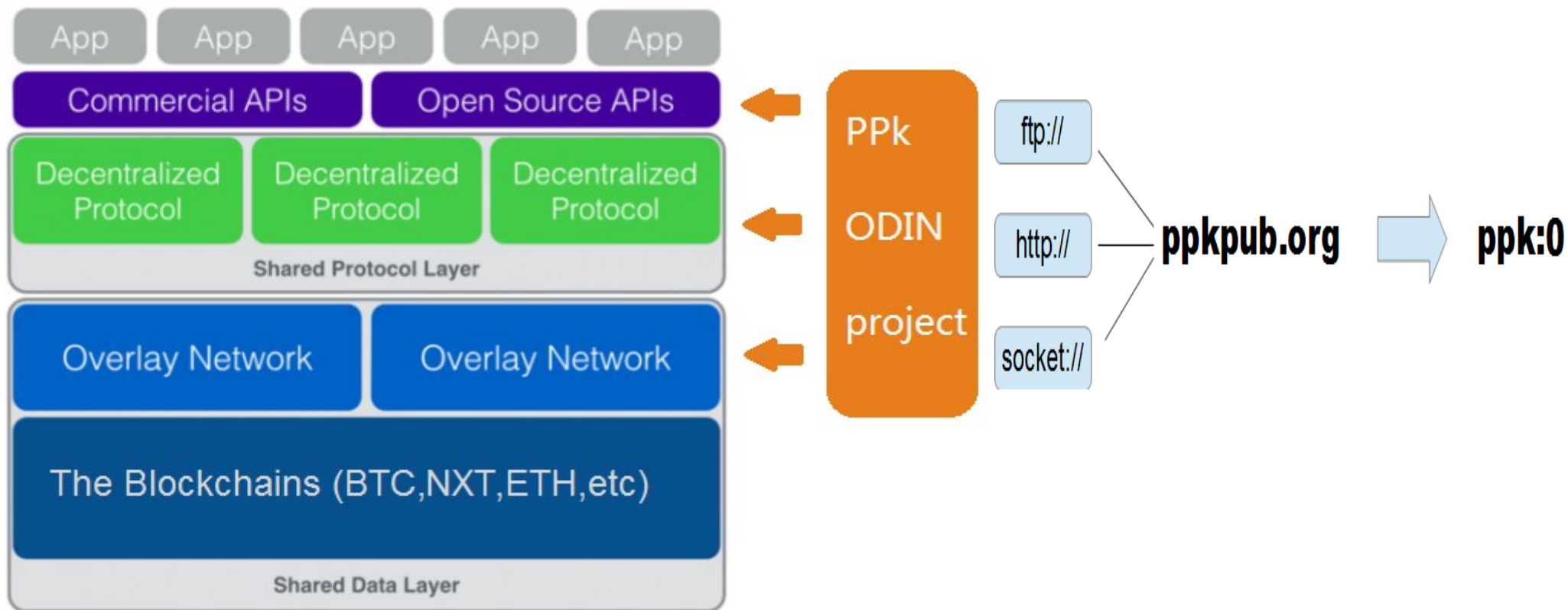
以超级账本承载多级标识的开源示例

在比特币区块链上实现一级标识的开源代码

发布基础的标识协议 (ODIN)



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

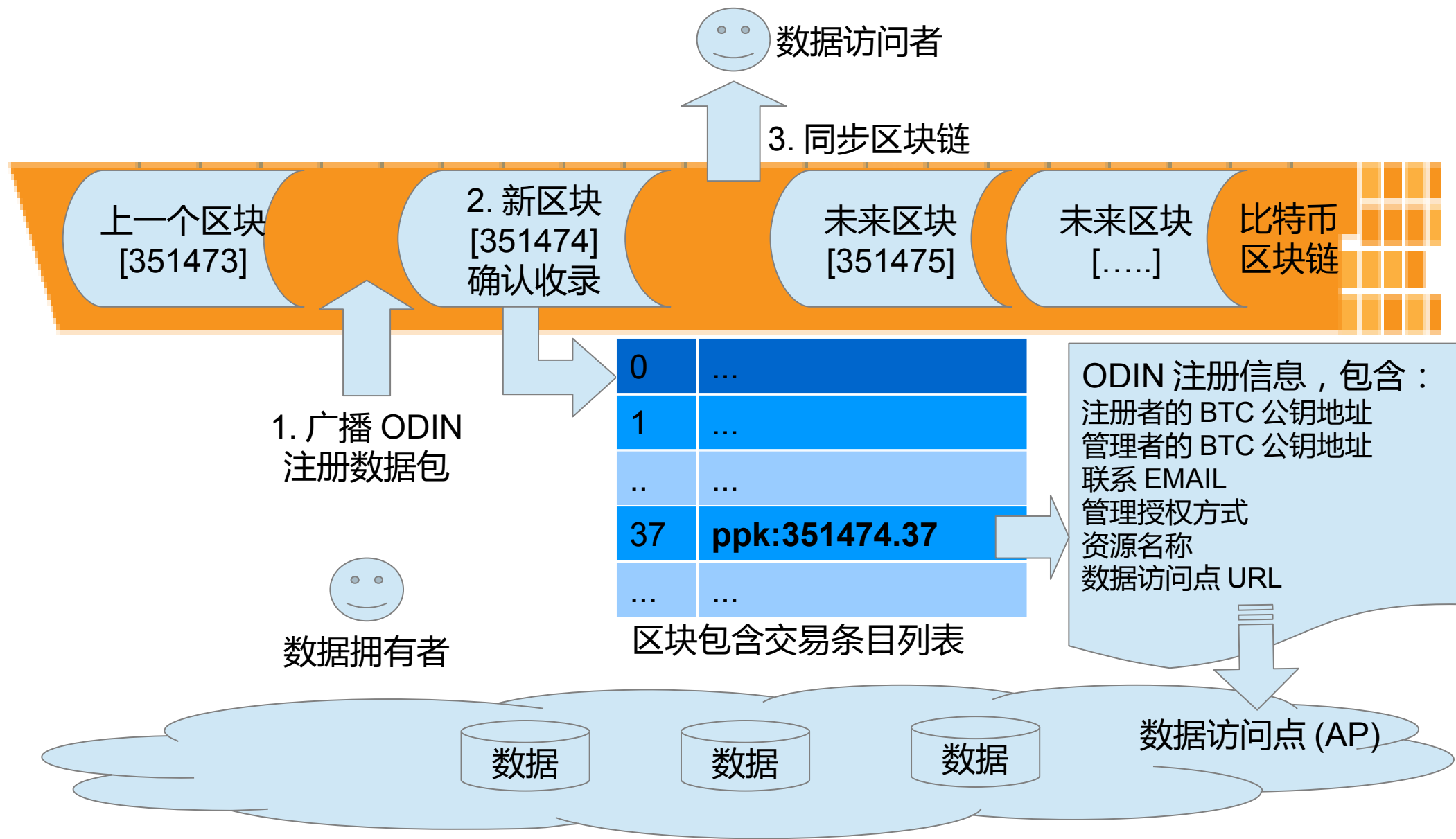
安全

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

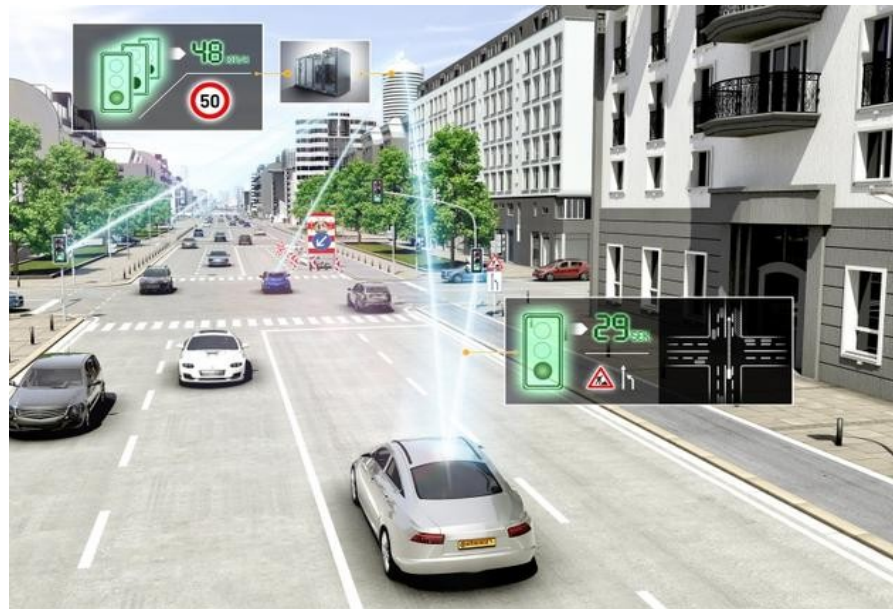
ODIN 运行机制



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。

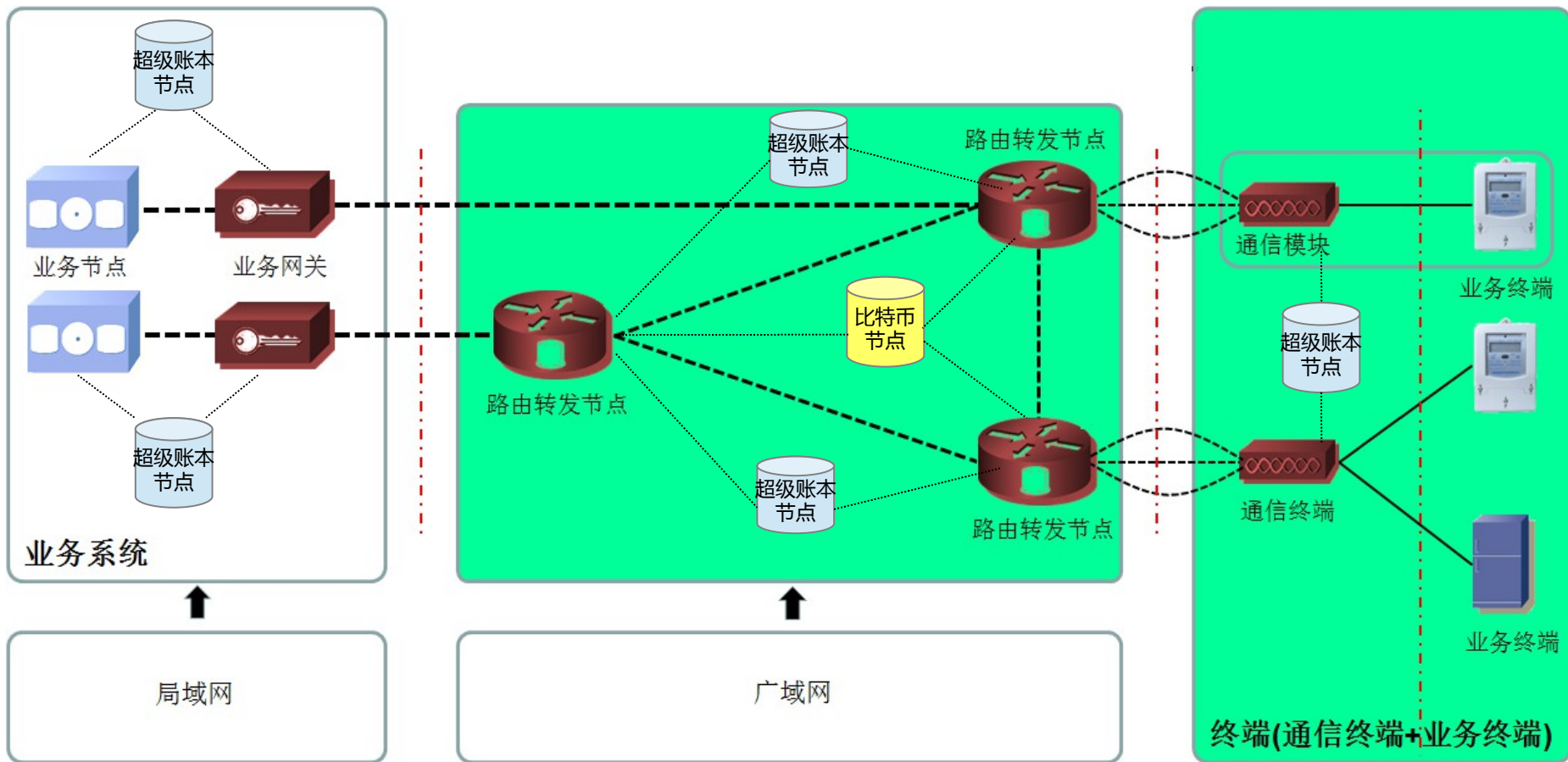


+ ODIN/Blockchain

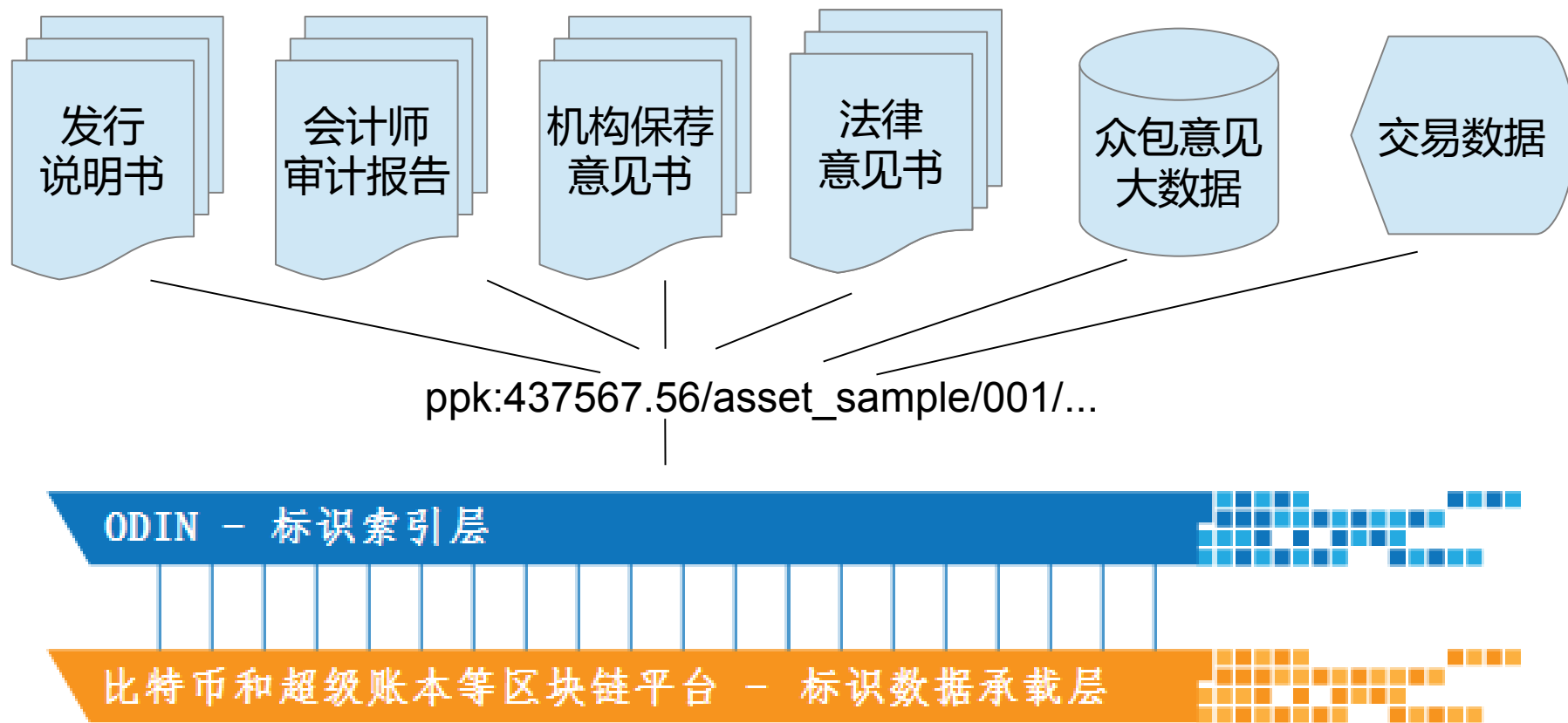
数据形态：万物互联、实时共享

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。

PPk 协议应用于物联网的原型示例



可预见的应用场景 之二：数字资产市场





Welcome to **PPk** pub.

We love **P2P** network.

drive the future of P !

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