区块链与网络通信的跨界融合

Welcome to PPk pub!

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

关于 PPkPub

About 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“ PPkPub”是一个开放的兴趣小组，集合了一群对比特币等加密货币感兴趣的 P2P 技术爱好者。相比加密货币的价格起伏，我们更关注以区块链为代表的新兴技术的潜在价值！

PPkPub is a public group with a few P2P technology fans.

Through years practice to digital encryption currency field, PPkPub found the special value of blockchain technology, which would be the next generation network infrastructure. Now we are focus on open source projects to push together the blockchain and network communication technologies such as IPFS,NDN,etc.

区块链技术简介

区块链技术的价值分析

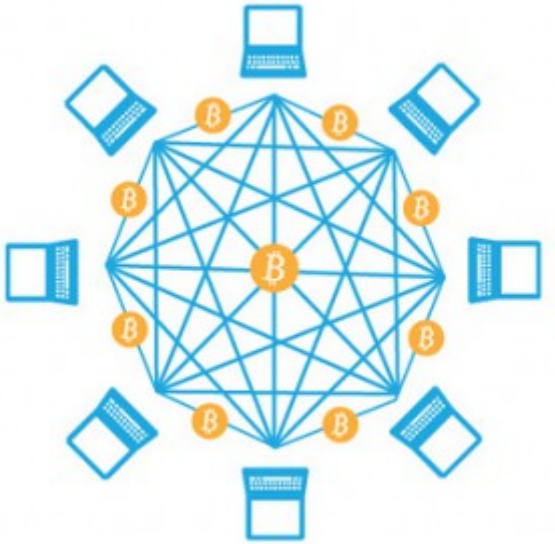
互联网 + 区块链的独到思路

区块链（ Blockchain ）是什么？

一种在

对等网络环境下，多节点参与，
通过特定的一致性算法达成共识，
拥有不可伪造、不可篡改和可追溯特性，
承载可信数据和计算业务的

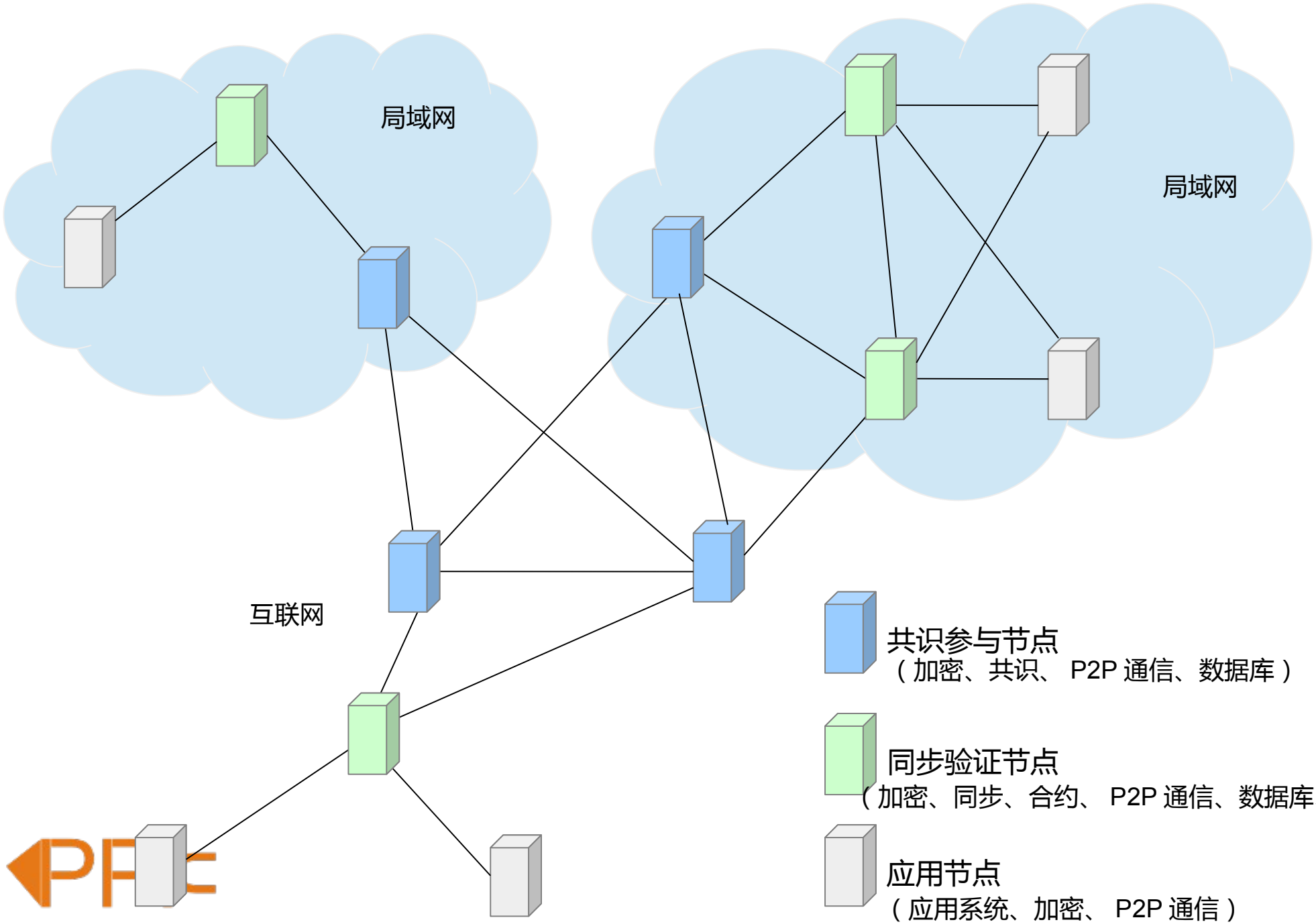
分布式平台



不同层次的定义：
一种块链式数据结构。
一种解决了一致性问题的分布式通讯协议。
一种实现共识、满足可信业务需求的软件系统。
一种去信任达成价值交换的生态系统。

区块链的技术原理：功能架构

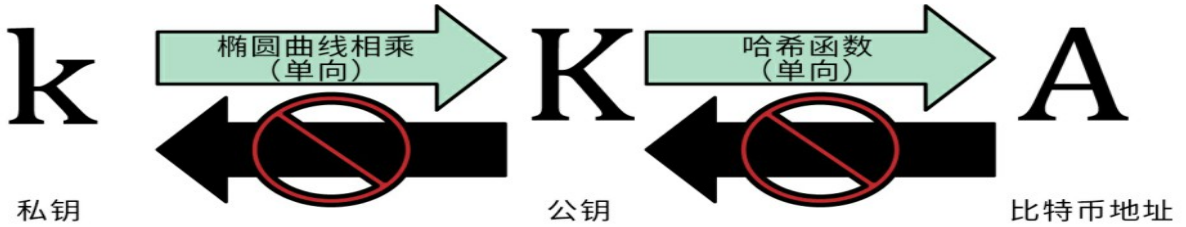
区块链的技术原理：部署架构



区块链的技术原理：数字加密技术

- 哈希算法
  - SHA256
    - 由随机数产生私钥
    - 产生交易标识
    - 产生区块标识
  - HASH160
    - 基于公钥生成不可逆公开地址

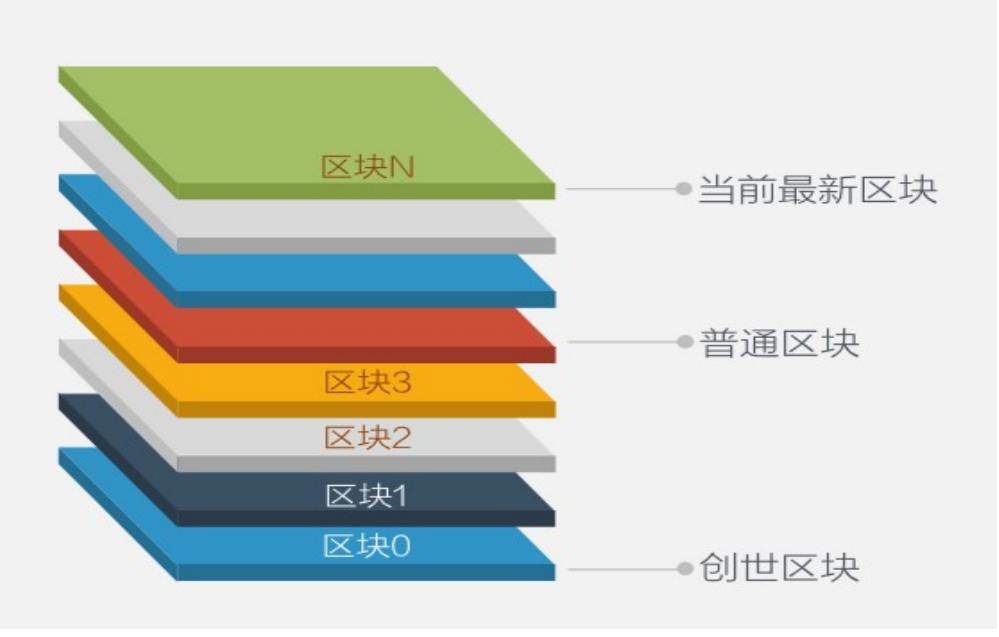
- 非对称加密



  - 椭圆曲线加密算法（特殊的 Secp256k1 椭圆曲线）
    - 由私钥生成对应公钥
    - 用私钥对交易签名、公钥开放验证

区块链的技术原理：账本结构

注：以比特币为例



区块链的技术原理：新区块的产生

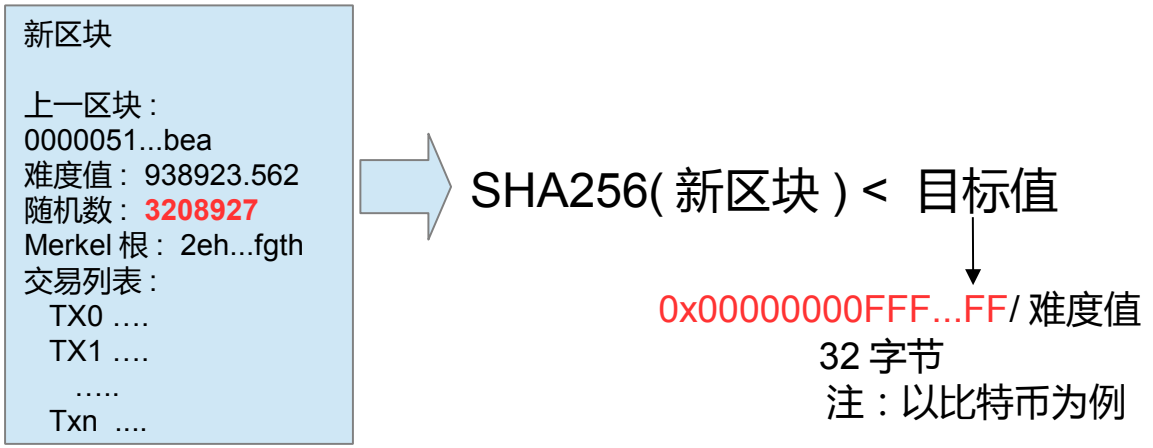
用工作量证明的方式创建新区块的过程被形象的比喻为 挖矿

区块链的技术原理：共识算法

在分布式环境下，多节点间依靠透明规则消除分歧，就数据或计算达成一致性结果的算法。

- POW （ Proof of Work ，工作量证明）

以投入算力来寻找随机数让哈希值匹配特定目标值、计算成本透明、可自主验证的数学规则来达成一致性结果。

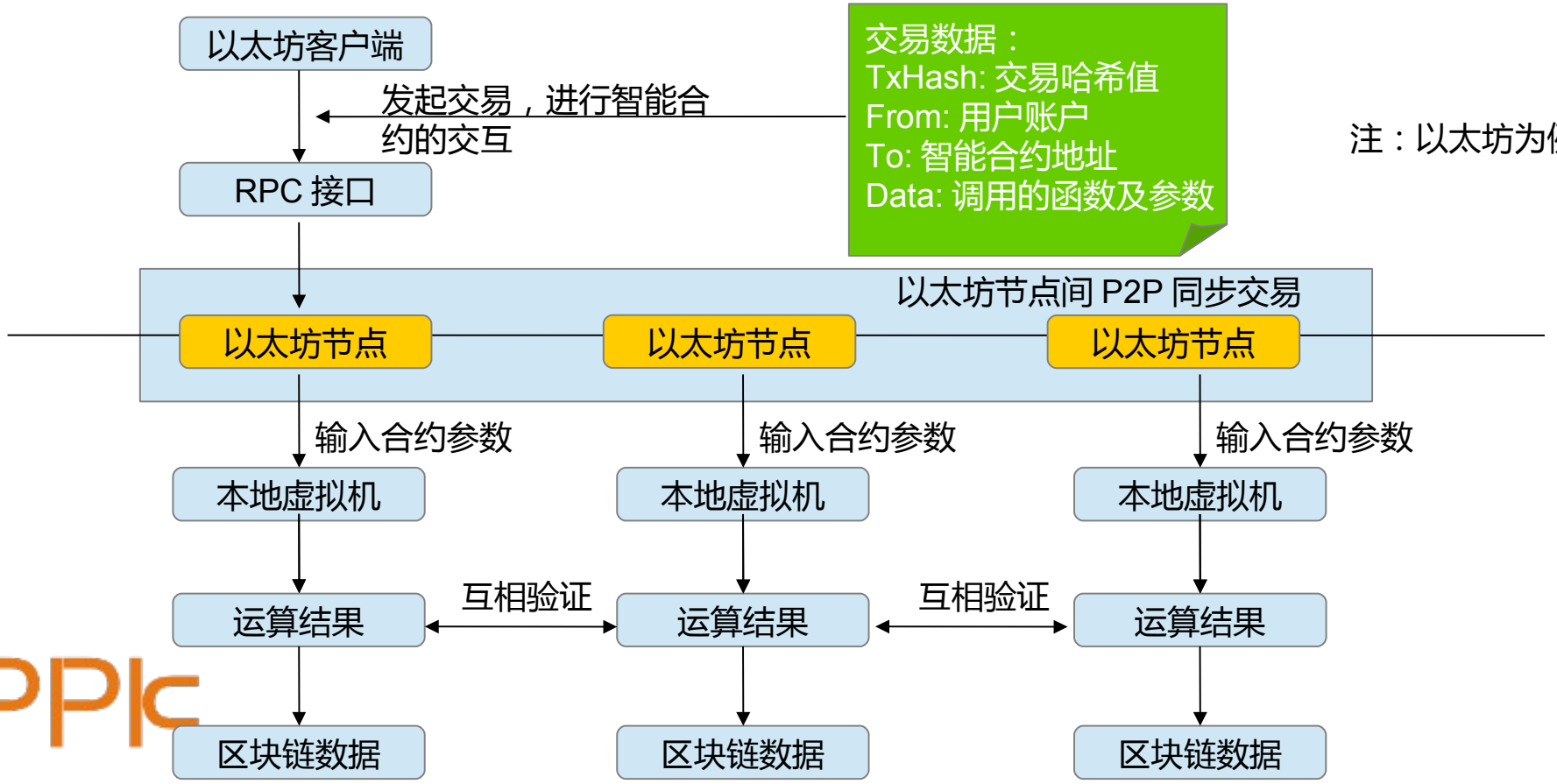


- POS （ Proof of Stake ，权益证明）
- DPOS（ Delegated Proof-of-Stake, 授权型权益证明）
- PBFT（ Practical Byzantine Fault Tolerance ，实用拜占庭容错）

区块链的技术原理：智能合约

智能合约可视作一段部署在区块链上可自动运行的程序，其涵盖的范围包括编程语言、编译器、虚拟机、事件、状态机、容错机制等。

程序本身记录在区块链上，具备透明、持久、不可篡改等特性；
程序可以控制区块链资产，比如可以存储和转移加密货币；
程序由区块链协调执行并获得一致性结果，避免人为干涉。



区块链产品形态

- 区块链平台
  - 比特币、以太坊
  - 超级帐本 HyperLedger
  - 杭州复杂美 Chain33 链、云象区块链
  - 北京布比区块链、北航链
- 数字货币
  - 比特币、莱特币、未来币、比特股
  - 以太坊、 LISK
- 数字资产
  - OMNI,XCP
  - Argur, Ark

区块链平台分类

公有链

参与节点是对等的，没有主导角色
共识机制的参与规则是透明、开放的
对区块链的读写权限都开放
一般采用 POW 、 POS/DPOS 共识算法，共识效率偏低

联盟链

参与节点是对等的，可以有主导协调角色
共识机制的参与规则是透明的，但限定若干参与者
对区块链的读权限开放，写权限限定若干参与者
一般采用类似 PBFT 共识算法，共识效率较高

私有链

有主导控制角色
共识机制的参与规则是私有不透明的，限定若干参与者
对区块链的读写权限都限定若干参与者
可以灵活采用类似 PBFT 共识算法或者其它传统的分布式一致性算法，共识效率较高

区块链产业生态

- 币圈
  - 矿机设备商：比特大陆
  - 矿厂和矿池：银鱼
  - 交易所： Bitstamp, Okcoin, 火币网
  - 支付服务商： Bitpay
  - 钱包： Blockchain.info ， Electrum, Armory

- 链圈
  - 标准联盟： Hyperledger ，中关村区块链产业联盟
  - 平台型企业：
    - 开发： Hyperledger，比原链，复杂美，云象，布比
    - 运营： Fatcom, 比原链，复杂美，布比
  - 技术服务型企业： Blockstream
  - 应用型企业： Filament 、水滴互助

区块链研究和应用现状


Blockchain Consulting/ App Dev
consensys
BTL
LedgerLabs
appliedblockchain
Payments
CIRCLE
bitpay
ABRA
CoinPip
vogogo
Align Commerce
Identity & Reputation
NETKI
uport
ShoCard
civic
BLOCKSCORE
Governance & Transparency
OTONOMOS
BoardRoom
BITNATION
BALANCE
Mining
BITMAIN
BitFury
Genesis Mining
Exchange, Trading & Investing
coinbase
LedgerX
GEMINI
Mirror
BITSTAMP
BTCC
coinfloor
POLONIEX
bitFlyer
kraken
SHAPE SHIFT
KCoin
BITFINEX
Media
coindesk
Crypto Compare
BTC MEDIA
BRAVE NEW COIN.
COINTELEGRAPH
Legal, Audit & Tax
PEERNOVA
Libra
clause
Content Management
ALEXANDRIA
LBRY
Revelator
OD JAAK
res( )nate
MUSIC
DC
SINGULAR
Data Analytics, Compliance & Security
Elliptic
simplex
Skry
CHAINALYSIS
coinfirm
airbitz
Social Network
synereo
AKASHA
steemit
Wallet
xapo
Jaxx
BLOCKCHAIN
TREZOR
BITX
CiPHREX
colu
Data Provenance & Notary
factom
blockai
BLOCKVERIFY
PROVENANCE
bitproof.io
everledger
guardtime
TIERION
Supply Chain & Logistics
FILAMENT
Hijro
Blocktrelight.
skuchain
@vijaymichalik @Frost_Sullivan
@lawrencelundy @OVioHQ
Prediction Markets
GNOSIS
augur
Hivemind
Public Chain Infrastructure
Bitcoin Foundation
CASH
MONERO
Blockstream
ethereum
LISK
parity
blockstack
Commerce & Advertising
OB1
Purse
SAFEMARKET
brave
Financial Services Infrastructure
ripple
SETL
Digital Asset Holdings
PAXOS
symbiont
R
clearmatics
TALLYSTICKS
UBIDI
Chain
AXONI
Enterprise Infrastructure
Gem
Filecoin
Tendermint
STORJ
CREDITS
nuco
bloq
HYPERLEDGER PROJECT
BIGCHAINDB
MONAX

区块链技术简介

区块链技术的价值分析

互联网 + 区块链的独到思路

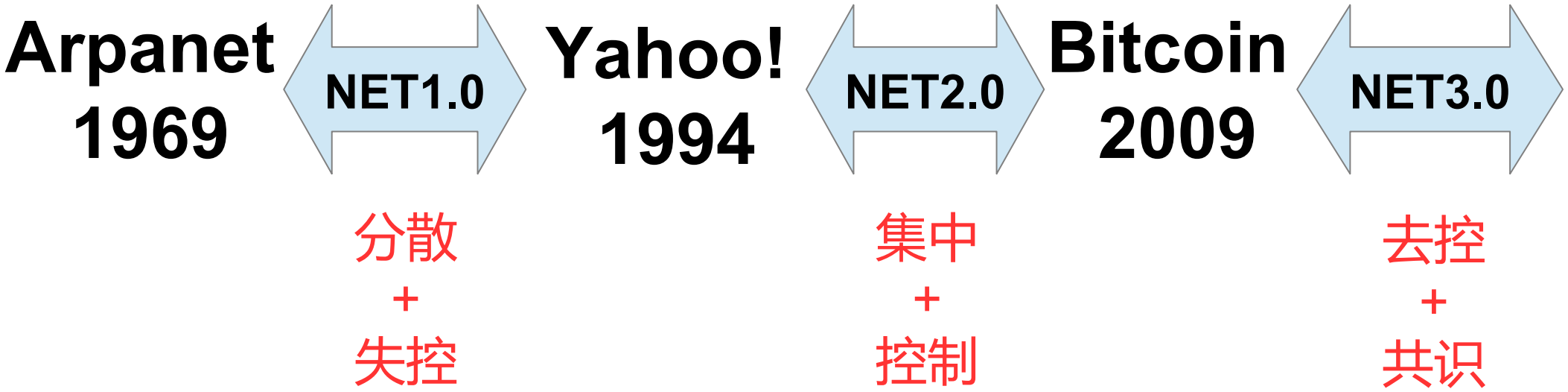
比特币 / 区块链： 开天辟地

比特币 / 区块链是历史上第一个

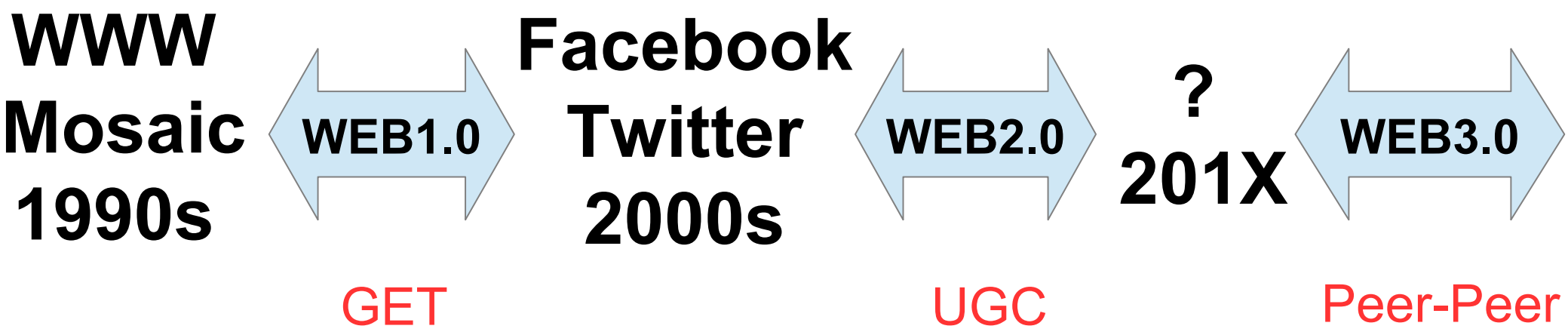
组织形式上去中心化，
业务逻辑上达成一致性

的源创案例。

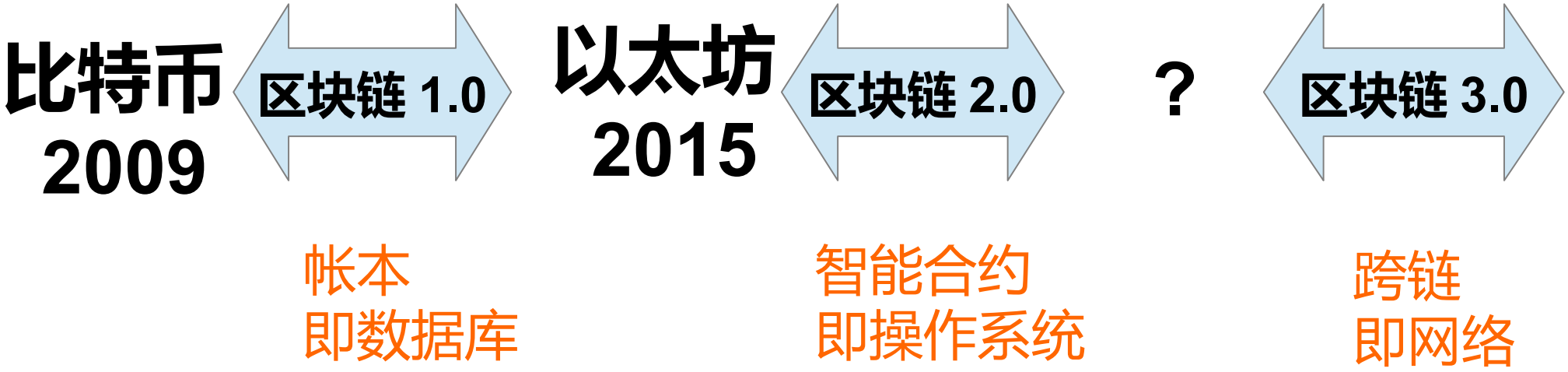
互联网的历史和趋势


Arpanet
1969
NET1.0
Yahoo!
1994
NET2.0
Bitcoin
2009
NET3.0
分散
+
失控
集中
+
控制
去控
+
共识

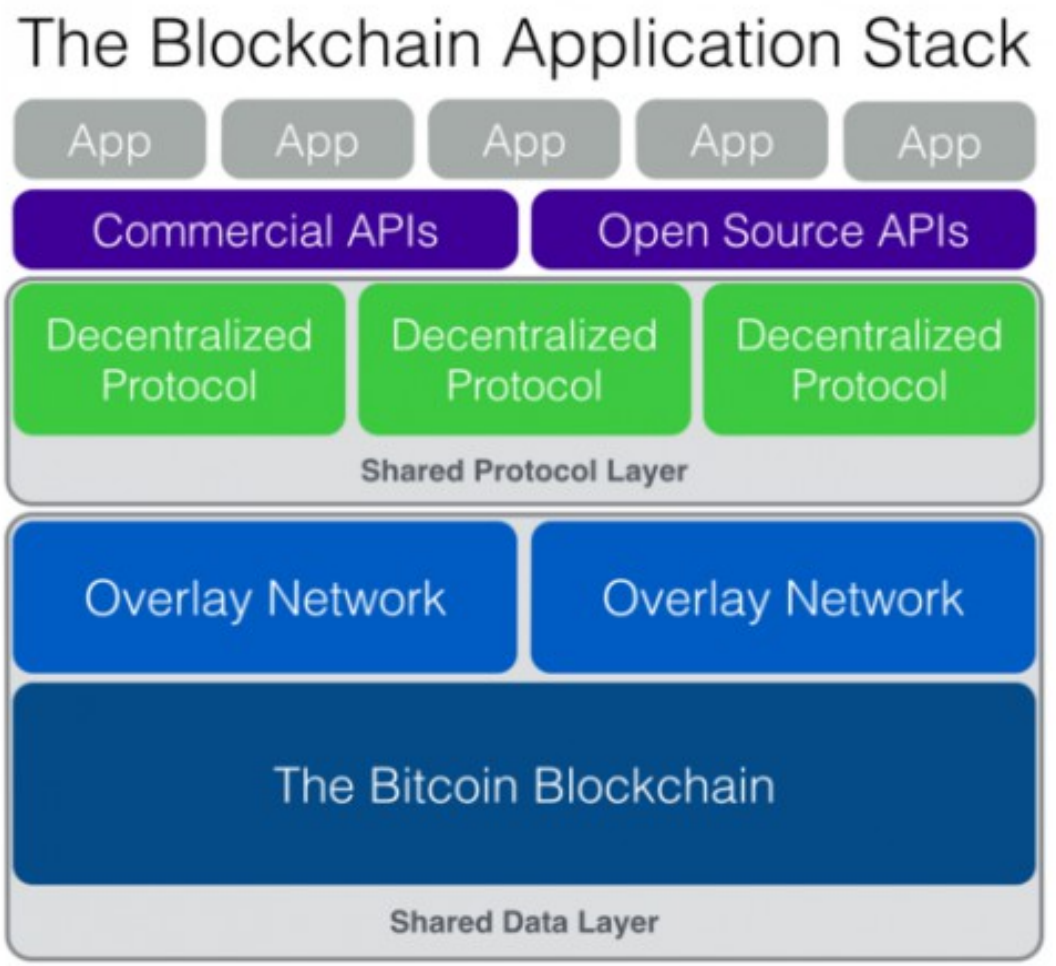
万维网的历史和趋势


WWW
Mosaic
1990s
WEB1.0
Facebook
Twitter
2000s
WEB2.0
?
201X
WEB3.0
GET
UGC
Peer-Peer

区块链技术发展趋势



1+1>2： 区块链技术的价值体现



区块链的真正价值不是在于能带出来多少个去中心化的具体应用，
而在于让未来的无数去中心化和中心化应用能拥有一个自主、统一的全新底层协议，
自组织产生 1+1>2 的合力，破除“围城”困境。

区块链技术简介

区块链技术的价值分析

互联网 + 区块链的独到思路

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

- 设计新的 Internet 体系结构
  - 演进式： “打补丁”
  - 变革式（ clean slate ）
    - 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 简介

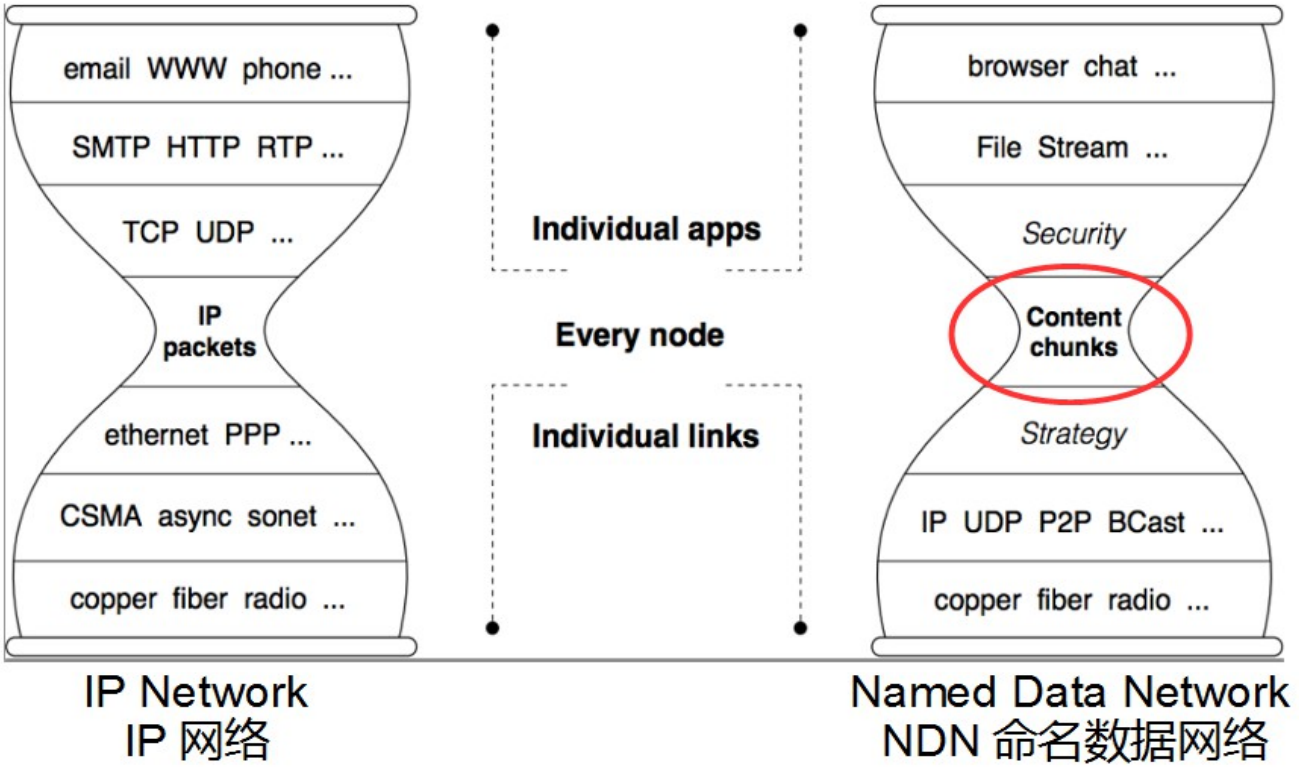
- NDN （ Name Data Network ，命名数据网络）：
  未来互联网体系架构 (FIA) 研究项目之一， 2010 年由美国国家自然科学基金会（ NSF ）设立。

面向主机→面向内容（ where → what ）

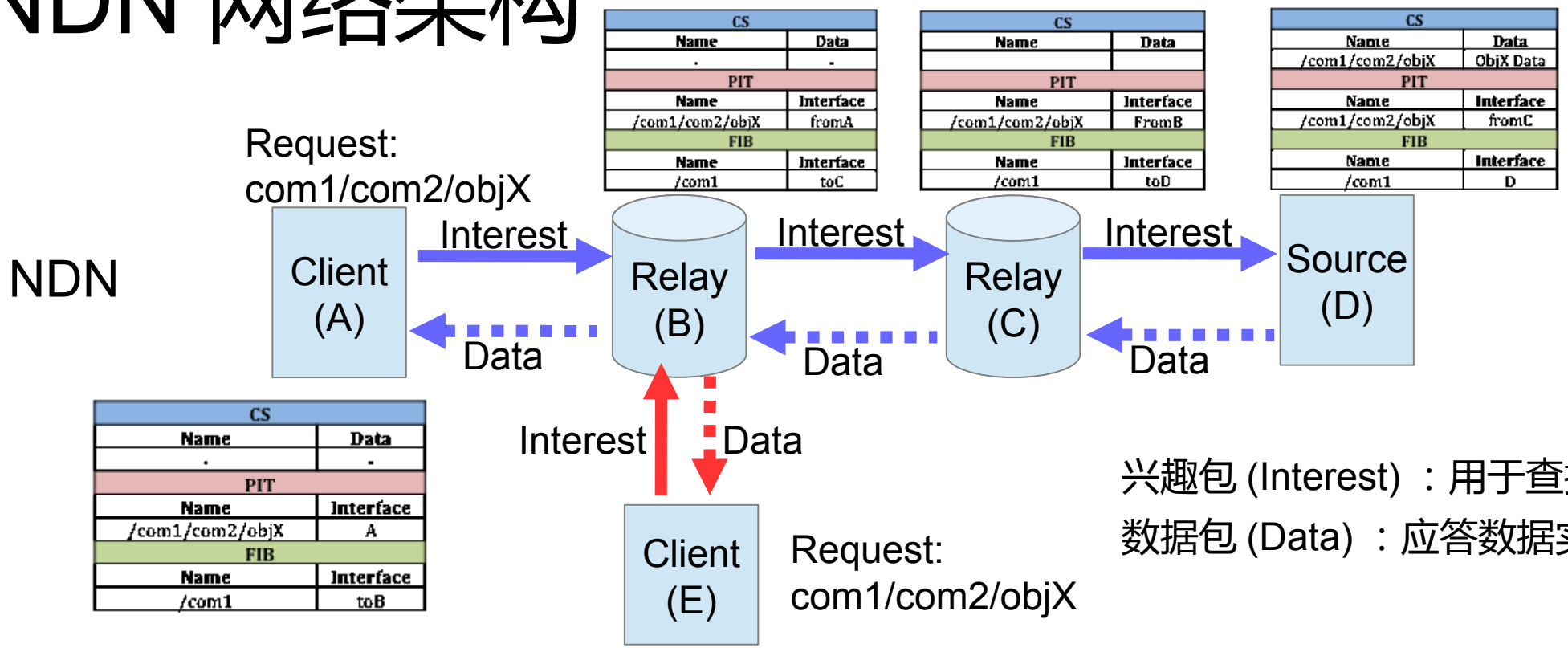
Named host → Named data ，变为以内容为中心

以内容标识定位内容，不需要位置相关地址

缓存复用

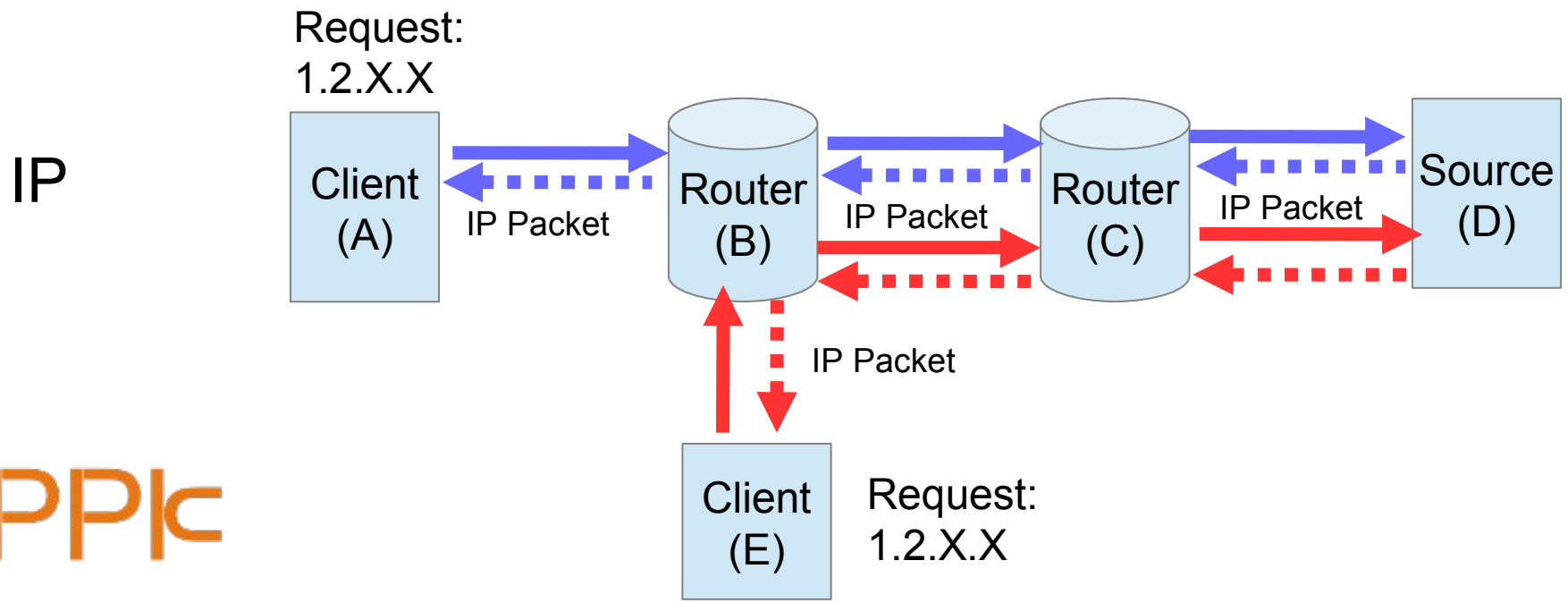


NDN 网络架构



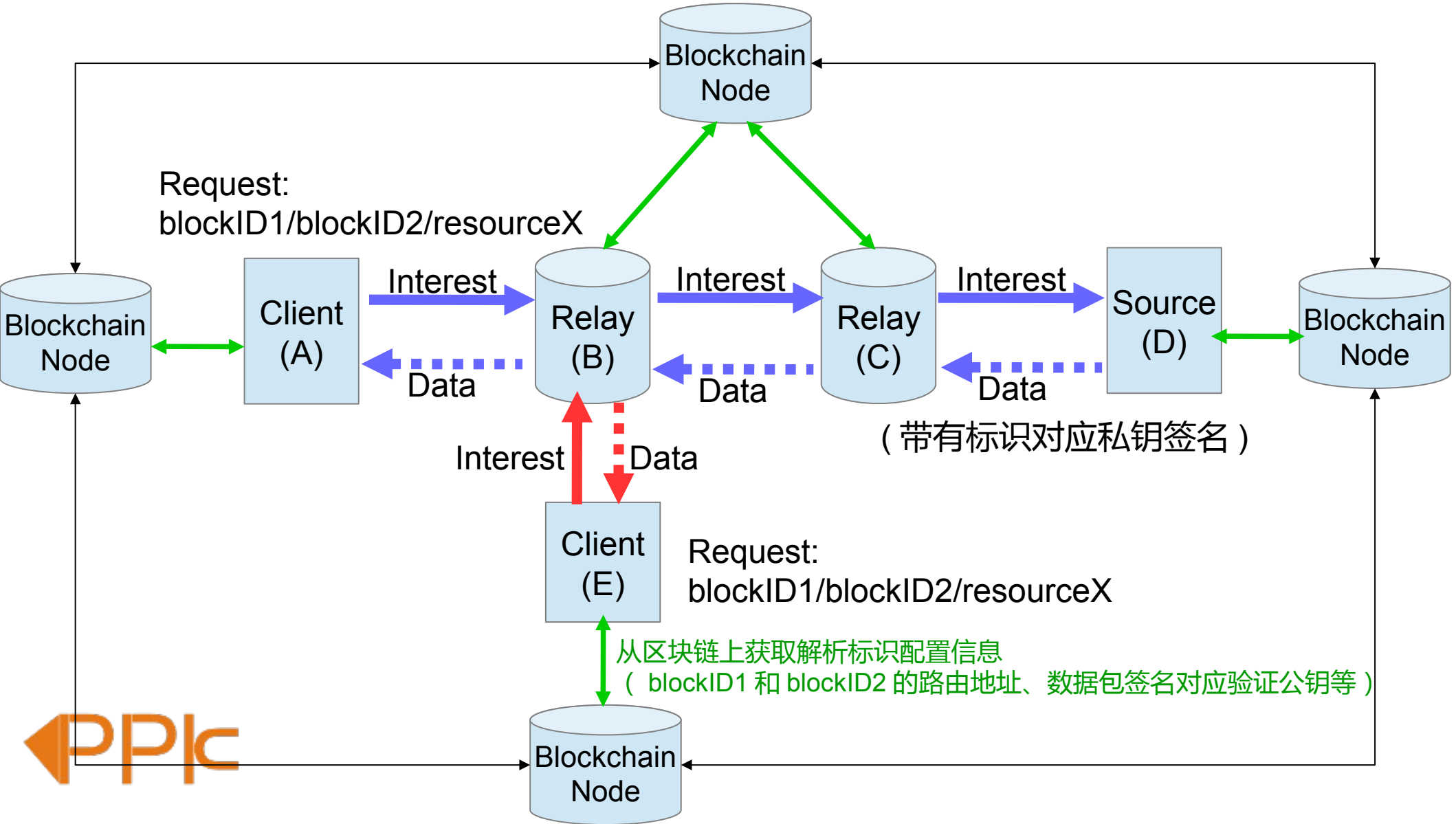
兴趣包 (Interest) ：用于查找

数据包 (Data) ：应答数据实体

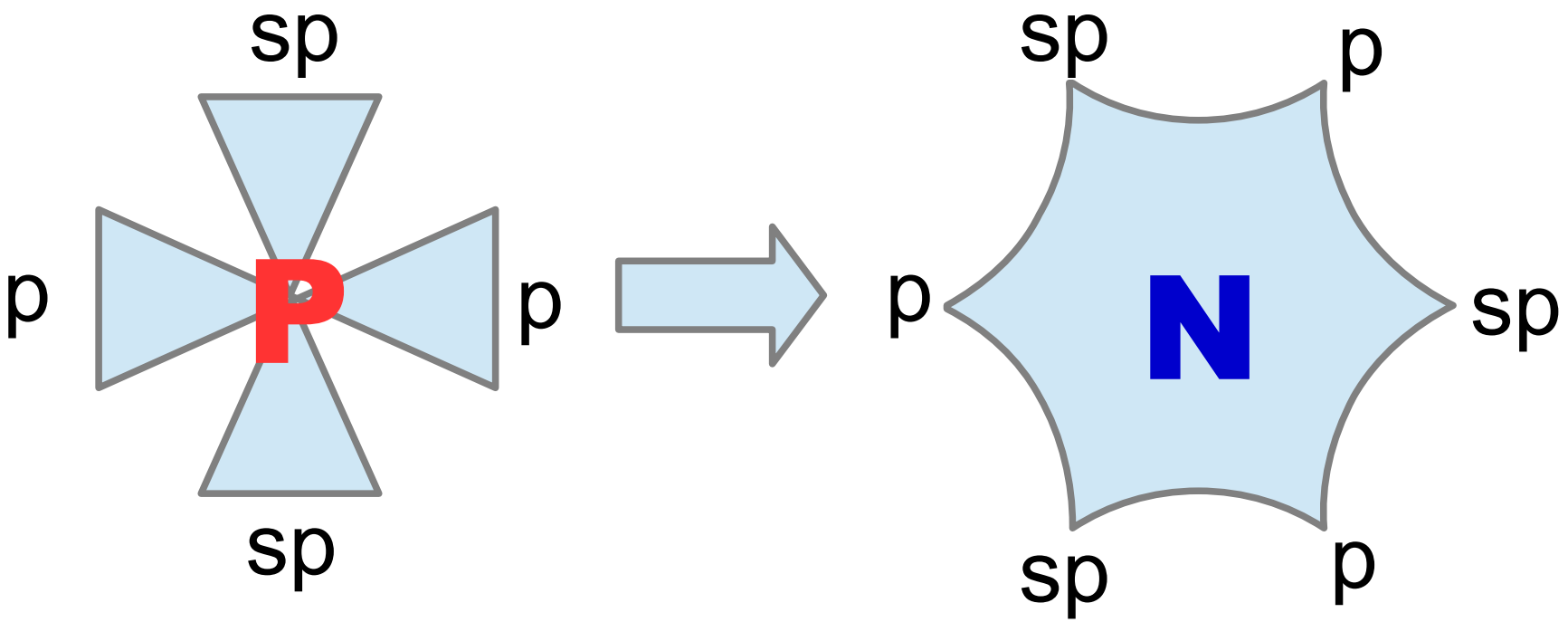


NDN+Blockchain: 融合的关键点

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”

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 ： 我们的推进思路

Concept
- Define the basic protocol of ODIN
- Reference based on future internet(NDN, IOT etc.)

Prototype
- IoT prototype based on ODIN
- Core implementation on the bitcoin blockchain

We are here

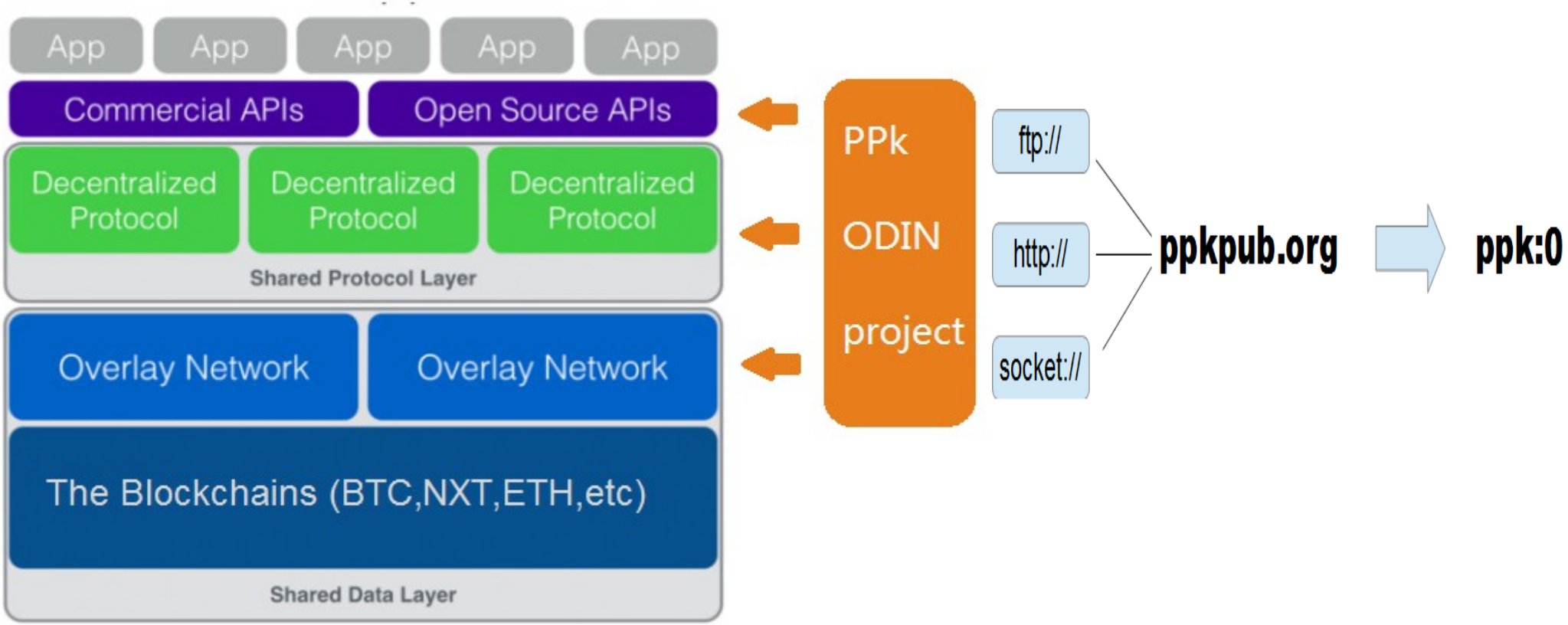
Popularize
- Cloud based ODIN publish
- Clients'(PC,Mobile,IoT hardware) ODIN add-on publish

Work with Future
- Update the protocol with Future Internet
- Open publish the updated protocol

PPIC

ODIN 开放项目：融合多区块链的 DNS

ODIN: New DNS based on multi-blockchains



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

Independence

唯　一

Uniqueness

安　全

Security

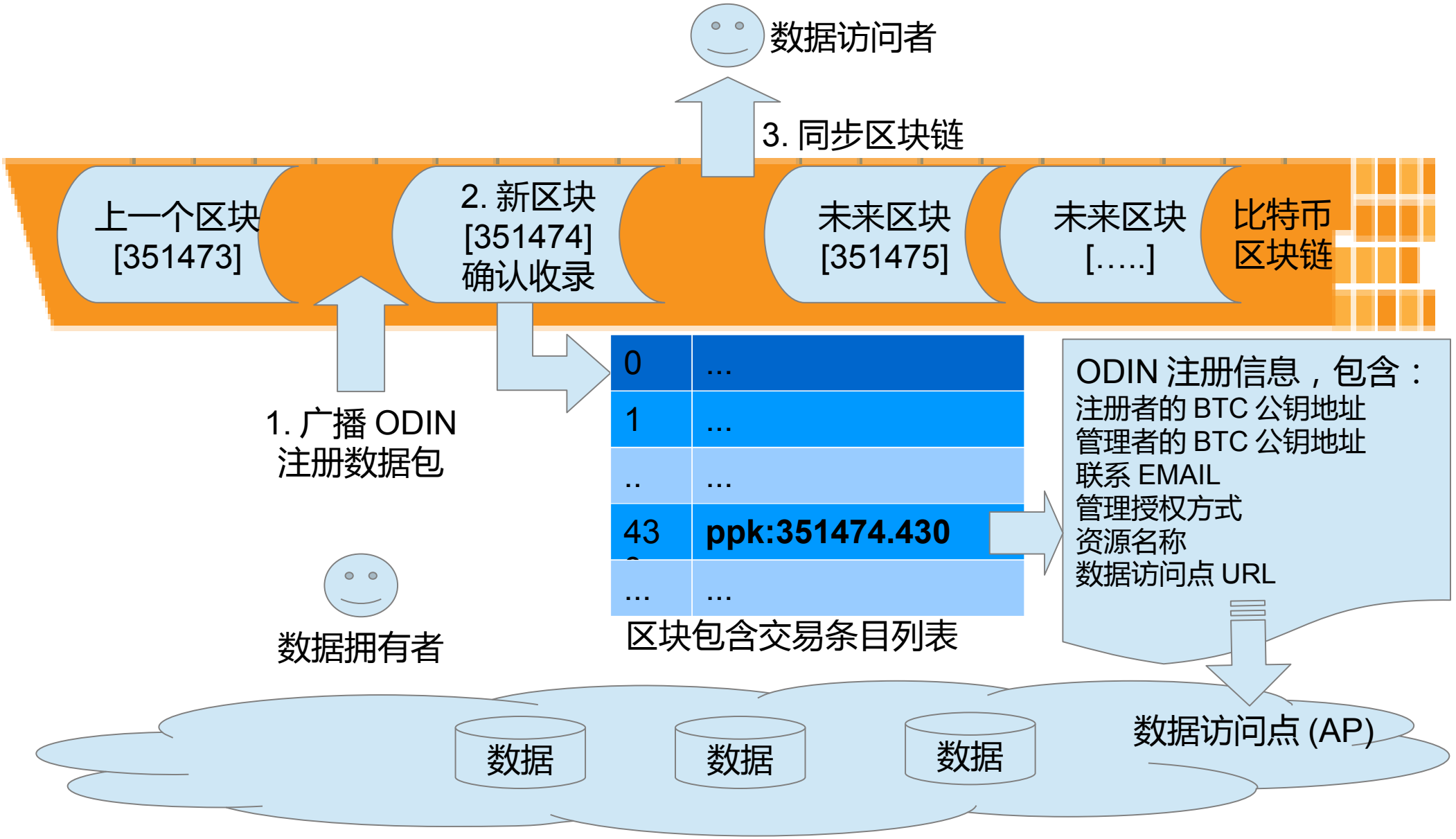
永　久

Permanent

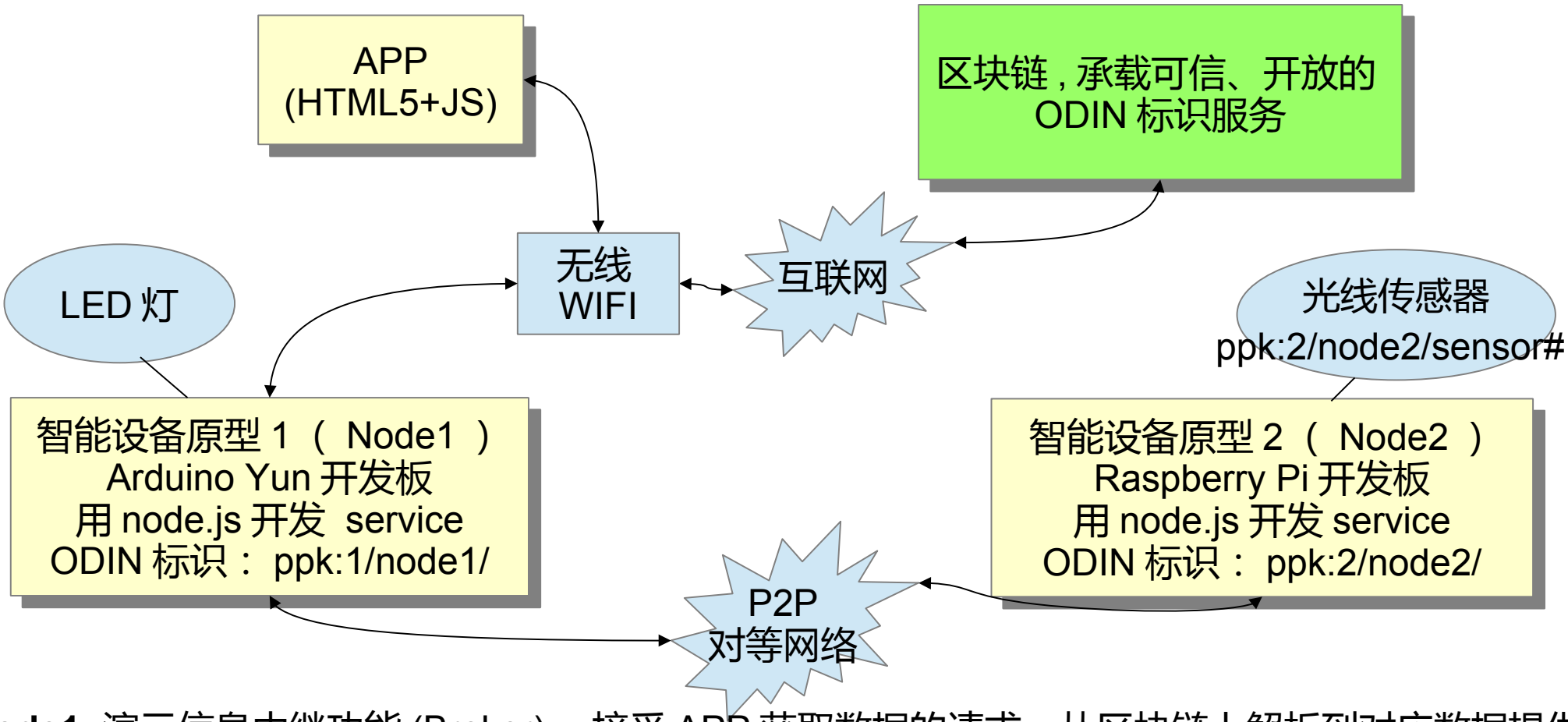
ODIN 与其它基于区块链的标识类解决方案的差异

	ODIN	Namecoin	Onename
基础区块链	Bitcoin	Namecoin	Namecoin → Blockstack based Bitcoin
多级扩展	支持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

运行机制


数据访问者
3. 同步区块链
上一个区块
[351473]
2. 新区块
[351474]
确认收录
未来区块
[351475]
未来区块
[.....]
比特币
区块链
1. 广播 ODIN
注册数据包
0 ...
1 ...
.. ...
43 ppk:351474.430
... ...
区块包含交易条目列表
ODIN 注册信息，包含：
注册者的 BTC 公钥地址
管理者的 BTC 公钥地址
联系 EMAIL
管理授权方式
资源名称
数据访问点 URL
数据拥有者
数据
数据
数据
数据访问点 (AP)

区块链应用于物联网的一个原型案例



Node1: 演示信息中继功能 (Broker) ，接受 APP 获取数据的请求，从区块链上解析到对应数据提供节点的访问配置参数后，从实际源数据节点获得数据块，并可以自主对数据块的签名合法性进行验证，验证通过的数据块会被返回给 APP, 同时可以缓存数据以备下次请求同样名称数据块时复用。

Node2: 提供源数据 (Publisher) ，按照登记在区块链上的配置信息对数据块进行私钥签名

APP: 与 Node2 没有直接数据通道，通过 Node1 和 Node2 构成的 P2P 网络间接获得 Node2 上光线传感器的环境亮度数值，再结合区块链验证获得传感器数据合法可信后动态调整 Node1 上的 LED 亮度

可预见的应用场景

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。

Welcome to **PPk** pub.

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

drive the future of P !

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