ArchData

技术峰会北京站

主办方：中生代技术 快CTO

2017年9月24日北京海淀区丹棱街5号微软亚太研发中心一号楼一层 故宫会议室

比特币与区块链原理解析

Inside Bitcoin and Block Chain

云时代架构技术社区发起人 李艳鹏

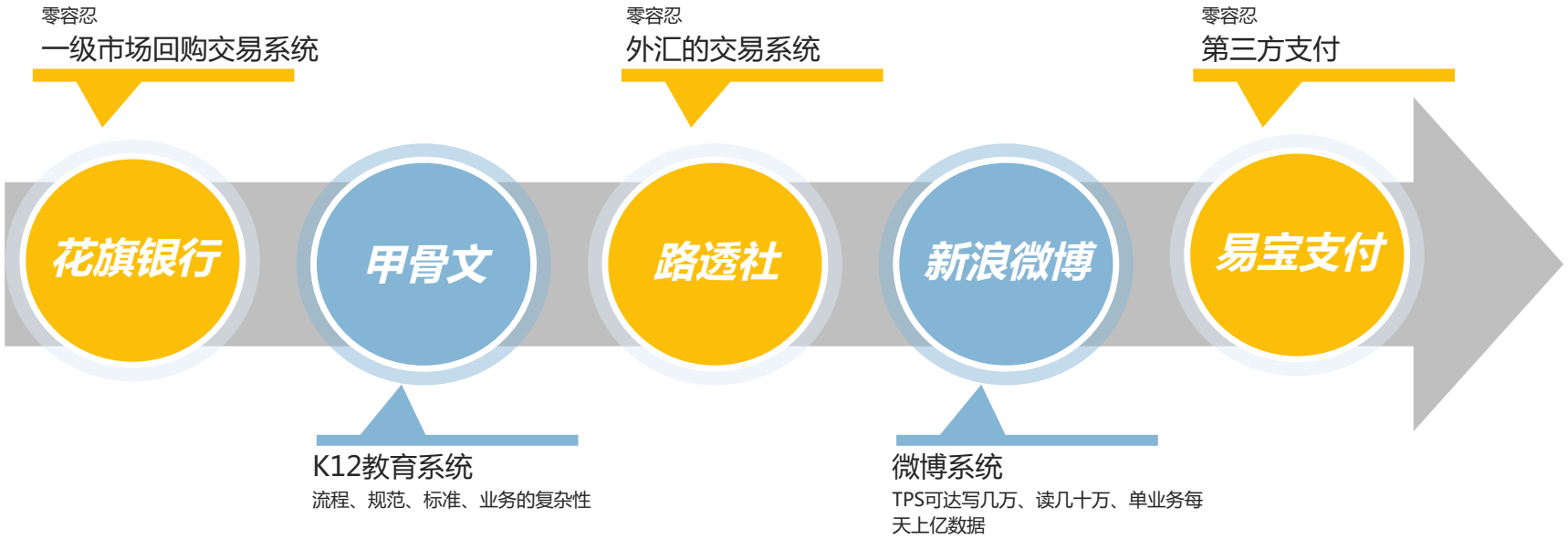
2017年9月

DIRECTORY
目录

01 云时代架构技术社区介绍

我的工作经历

My Experience



云时代架构技术社区的活动范围

The Area of Cloudate Club

云时代架构简书博客

6个月贡献11万字的博客，获得将近2000点赞，粉丝将近3000。

云时代架构分享

线上线下做了多场技术分享，即将与浪曦网共同举办线下分享大会，并录制培训视频。

云时代架构开源项目

拥有分库分表、缓存分片、消息队列处理器、发号器等众多轻量级开箱既用的开源项目。

做互联网时代最适合的架构，回归架构的简洁之美！

云时代架构公众号

3个月关注量超过5000。

云时代架构技术书籍

已经出版《分布式服务架构：原理、设计与实战》一书，即将出版《可伸缩服务架构：框架与中间件》，还有《Java核心要点和最佳实践》、《互联网研发最佳实践》、《支付平台架构》、《SSM源码解密》、《程序猿面试攻略：从技术到技巧》、《高可用架构》等6本书正在计划中。

云时代架构培训

提供微服务、一致性、高性能、高可用、Devops、支付业务架构设计、保险业务架构设计等主题培训。

最近出版的技术书籍

My Published Book


02
区块链

区块链总体结构

The Overview of Block Chain

区块结构

The Structure of Block

大小	字段	描述
4字节	区块大小	用字节表示的该字段之后的区块大小
80字节	区块头	组成区块头的几个字段
1-9 （可变整数）	交易计数器	交易的数量
可变的	交易	记录在区块里的交易信息

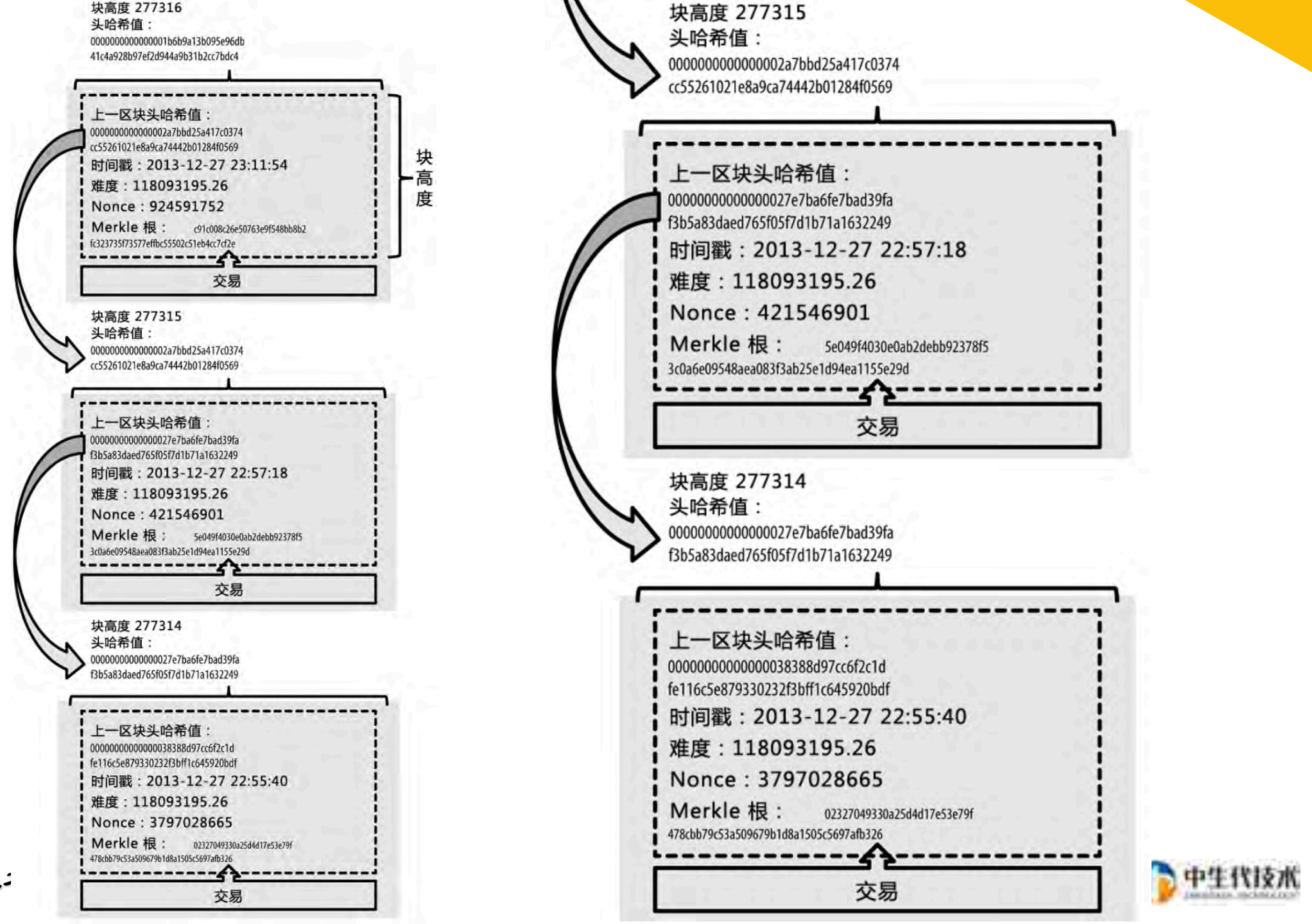
区块头结构

The Structure of Block Head

大小	字段	描述
4字节	版本	版本号，用于跟踪软件/协议的更新
32字节	父区块哈希值	引用区块链中父区块的哈希值
32字节	Merkle根	该区块中交易的merkle树根的哈希值
4字节	时间戳	该区块产生的近似时间（精确到秒的Unix时间戳）
4字节	难度目标	该区块工作量证明算法的难度目标
4字节	Nonce	用于工作量证明算法的计数器

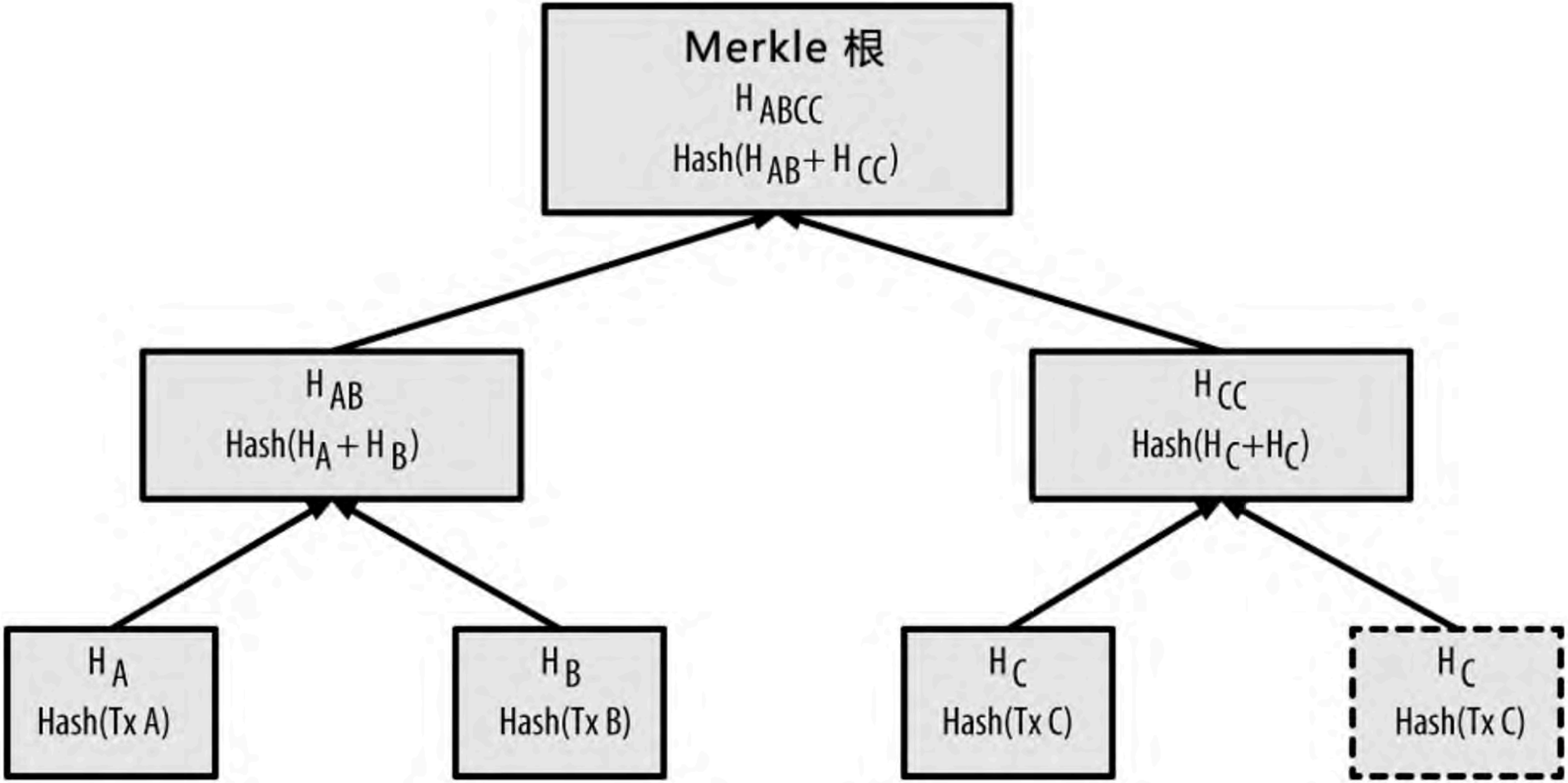
区块的链接

The Link of Block



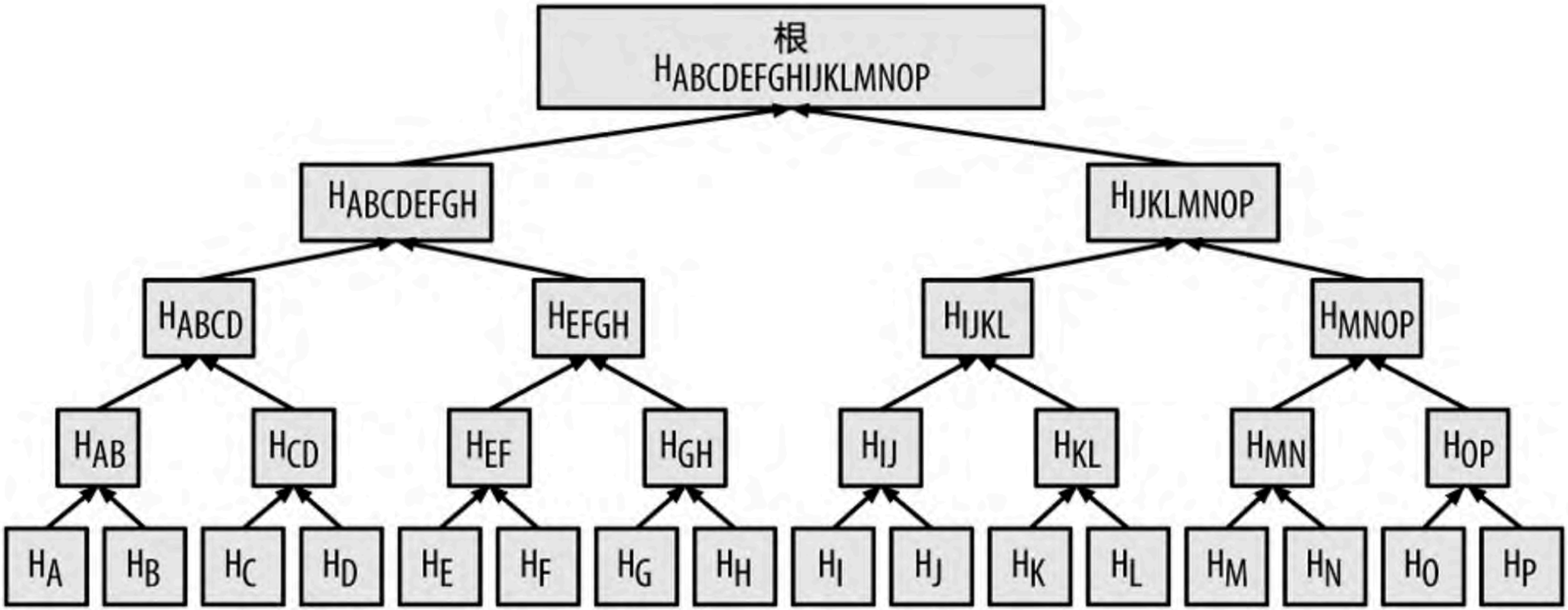
交易存储方式

The Storage of Transactions



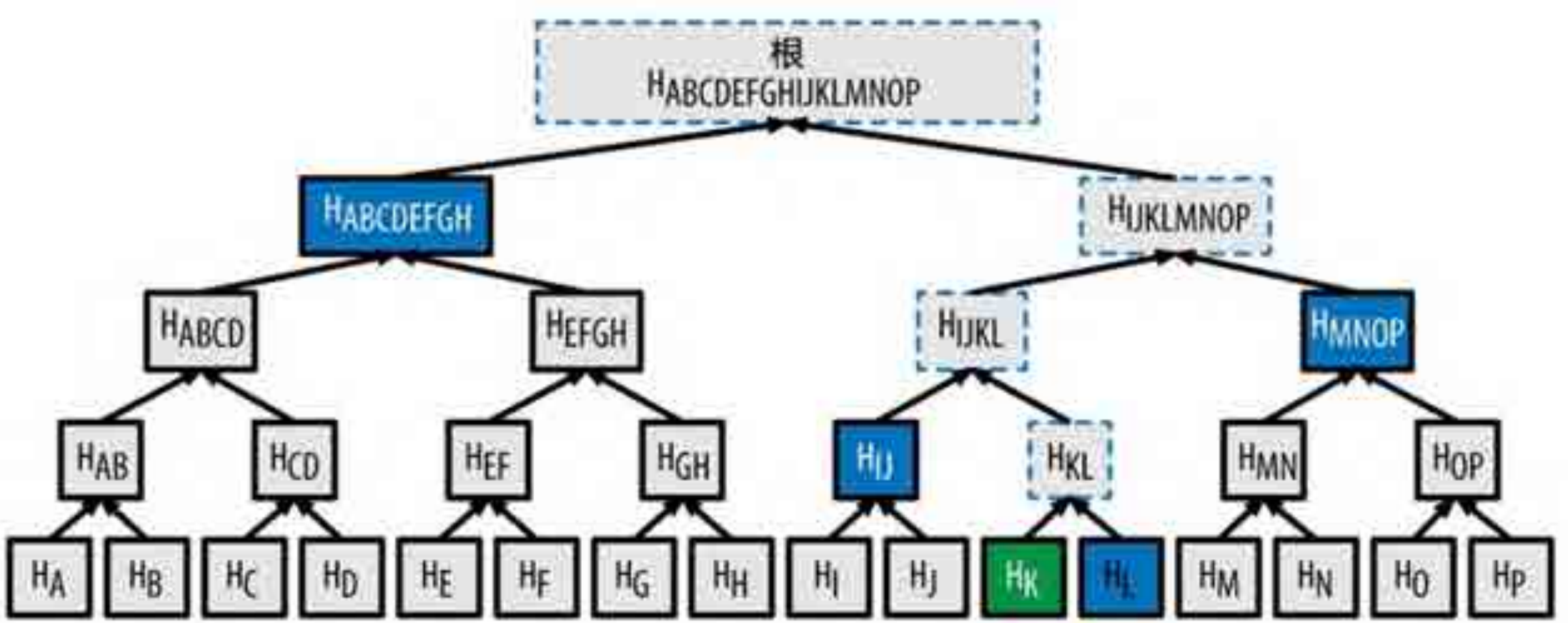
交易存储示例

The sample of the Storage of Transactions



验证交易路径

The Path of Verifying Transaction



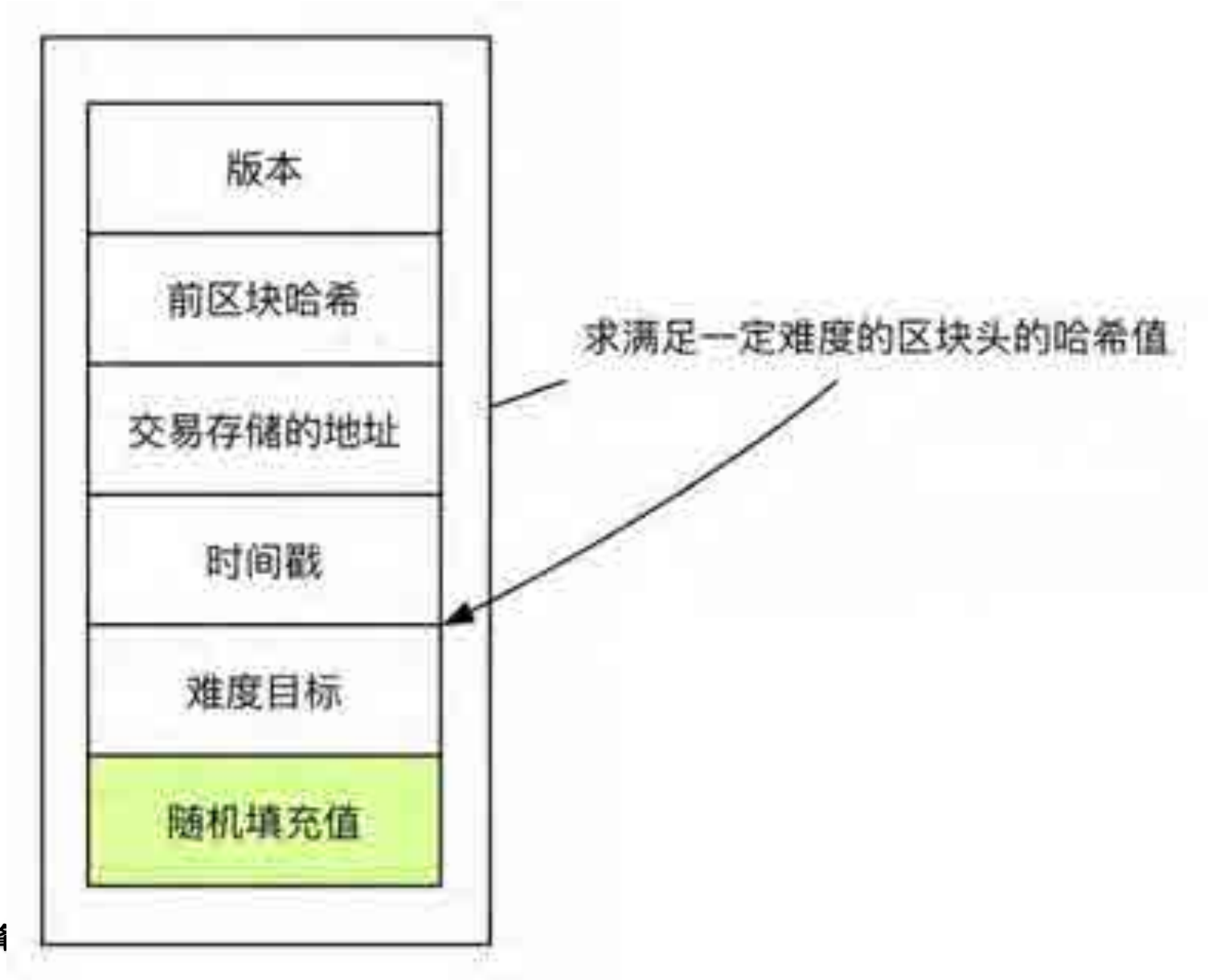
03 挖矿与共识

比特币供应量

The Amount of Bitcoin

挖矿在做什么

What is the Digging doing?



普通交易和挖矿交易的输入结构

The Structure of the Normal and Bonus Transaction

长度	字段	描述
32 字节	交易哈希	指向包含有将要被花费UTXO的交易
4 字节	交易输出索引	UTXO在交易中的索引，0 从0开始计数
1-9 字节	解锁脚本长度	解锁脚本的长度
(Varint) 可变长度	Unlocking-Script	一段脚本，用来解锁UTXO锁定脚本中的条件
4 bytes	顺序号	当前未启用的TX替换功能，设置为0xFFFFFFFF

长度	字段	描述
32 字节	交易哈希	不引用任何一个交易，值全部为0
4 字节	交易输出索引	值全部为1
1-9 字节	Coinbase数据长度	coinbase数据长度
(Varint) 可变长度	Coinbase数据	在v2版本的区块中，除了需要以区块高度开始外，其他数据可以任意填写，用于extra nonce和挖矿标签
4 bytes	顺序号	值全部为1，0xFFFFFFFF

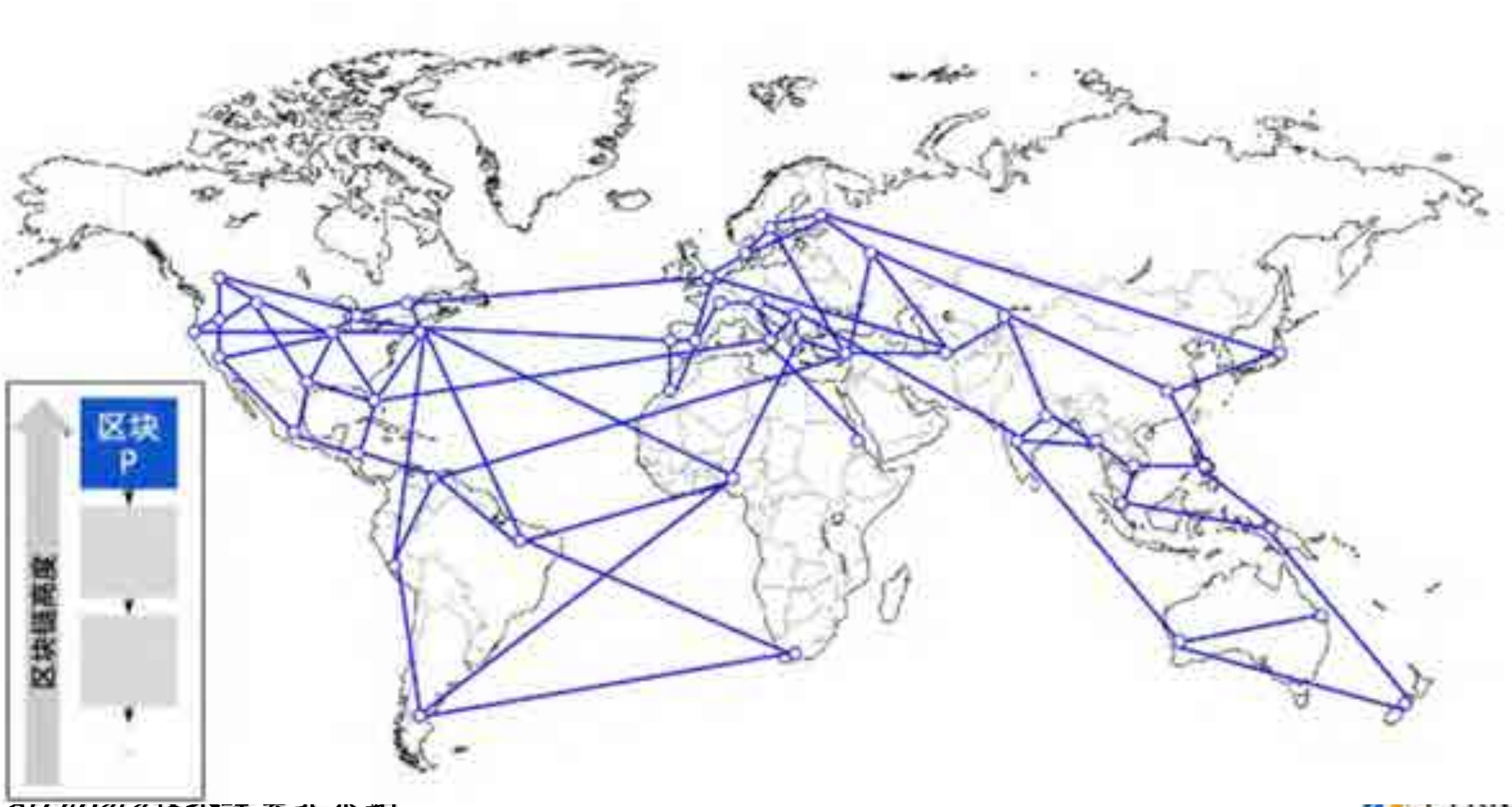
构造区块头

Construct the Block Head

长度	字段	描述
4 字节	版本	版本号，用来跟踪软件或协议的升级
32 字节	前区块哈希	链中前一个区块（父区块）的哈希值
32 字节	Merkle根	一个哈希值，表示这个区块中全部交易构成的merkle树的根
4 字节	时间戳	以Unix纪元开始到当下秒数记录的区块生成的时刻
4 bytes	难度目标	该区块的工作量证明算法难度目标
4 bytes	Nonce	一个用于工作量证明算法的计数器

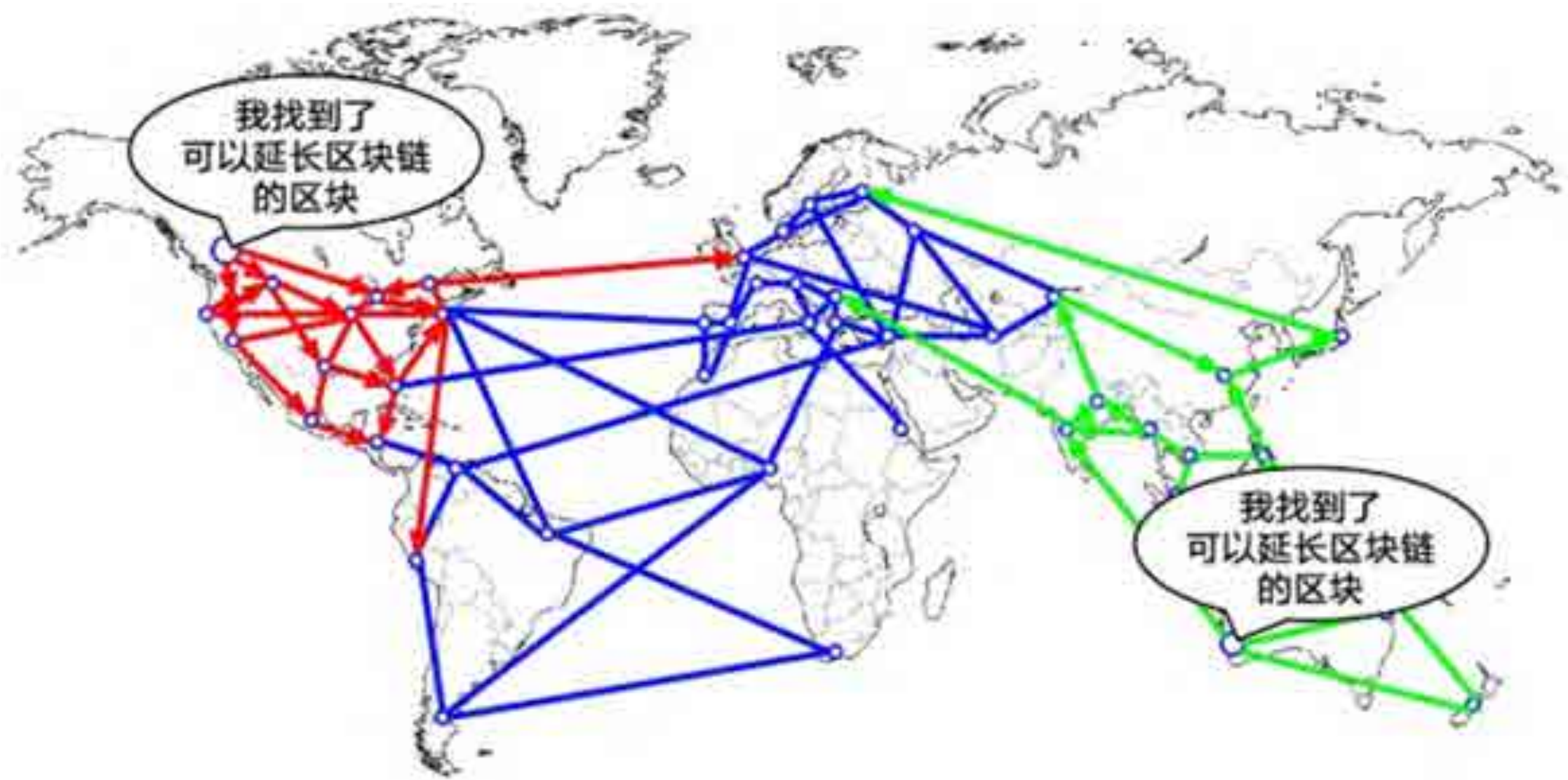
正常的区块链

Normal Block Chain



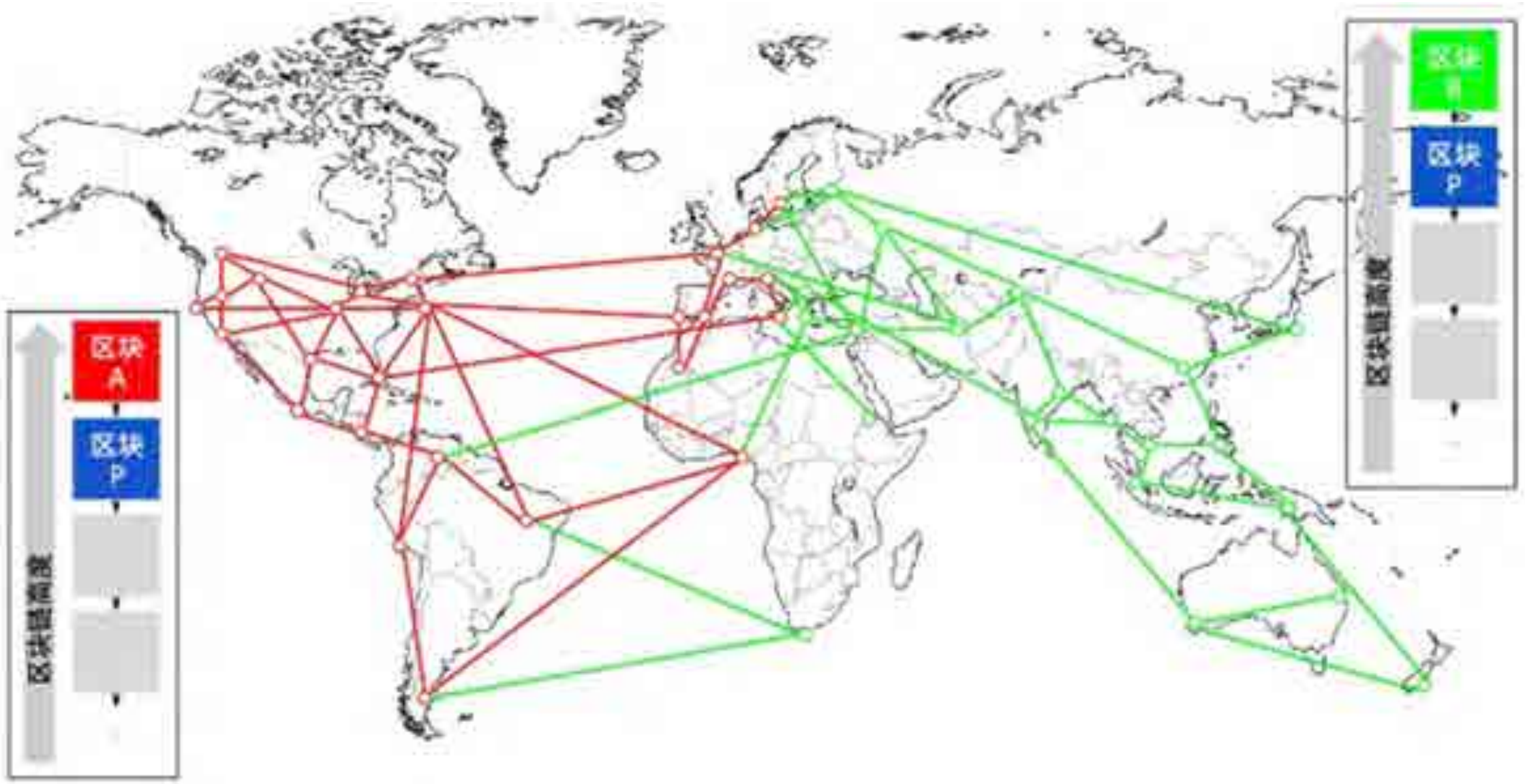
区块链分叉

Forked Block Chain



网络分区

Network Partition



网络分区

Network Partition

达成共识

Final Consensus

04 交易

交易验证方式

The Way of Verification

交易结构

The structure of a Transaction

大小	字段	描述
4字节	版本	明确这笔交易参照的规则
1-9字节	输入计数器	被包含的输入的数量
不定	输入	一个或多个交易输入
1-9字节	输出计数器	被包含的输入的数量
不定	输出	一个或多个交易输出
4字节	时钟时间	一个UNIX时间戳或区块号

交易的输入和输出

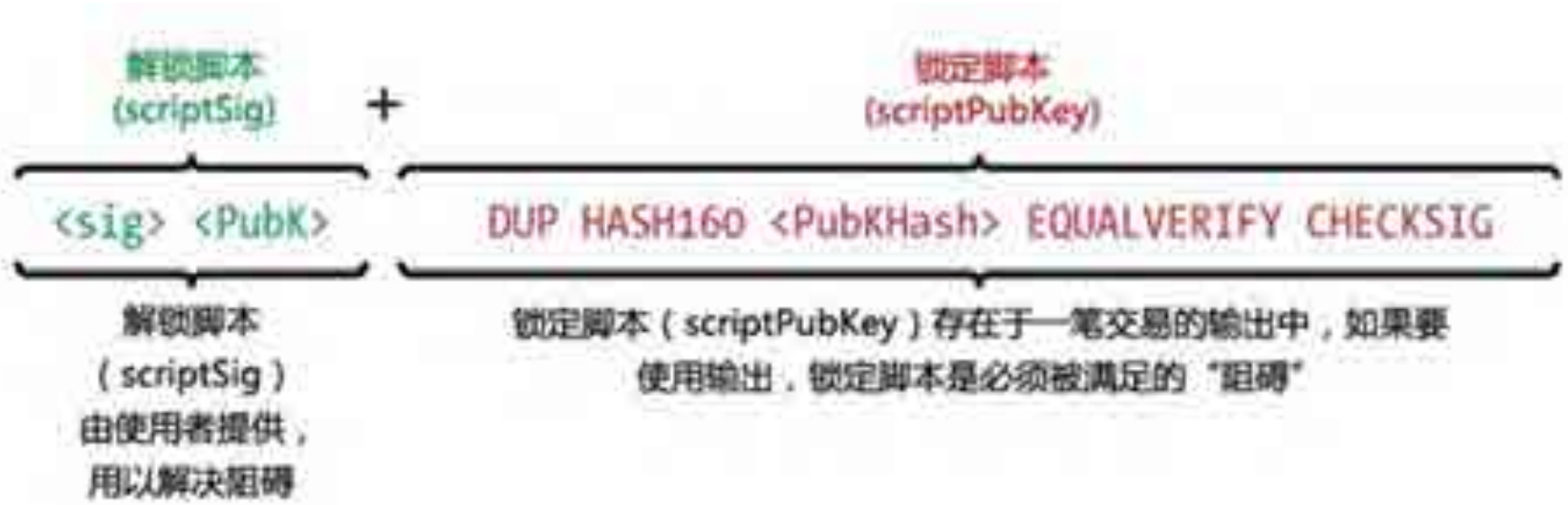
The Input and Output of a Transaciton

尺寸	字段	说明
32个字节	交易	指向交易包含的被花费的UTXO的哈希指针
4个字节	输出索引	被花费的UTXO的索引号，第一个是0
1-9个字节（可变整数）	解锁脚本尺寸	用字节表示的后面的解锁脚本长度
变长	解锁脚本	一个达到UTXO锁定脚本中的条件的脚本
4个字节	序列号	目前未被使用的交易替换功能，设成0xFFFFFFFF

尺寸	字段	说明
8个字节	总量	用聪表示的比特币值（10-8比特币）
1-9个字节（可变整数）	锁定脚本尺寸	用字节表示的后面的锁定脚本长度
变长	锁定脚本	一个定义了支付输出所需条件的脚本

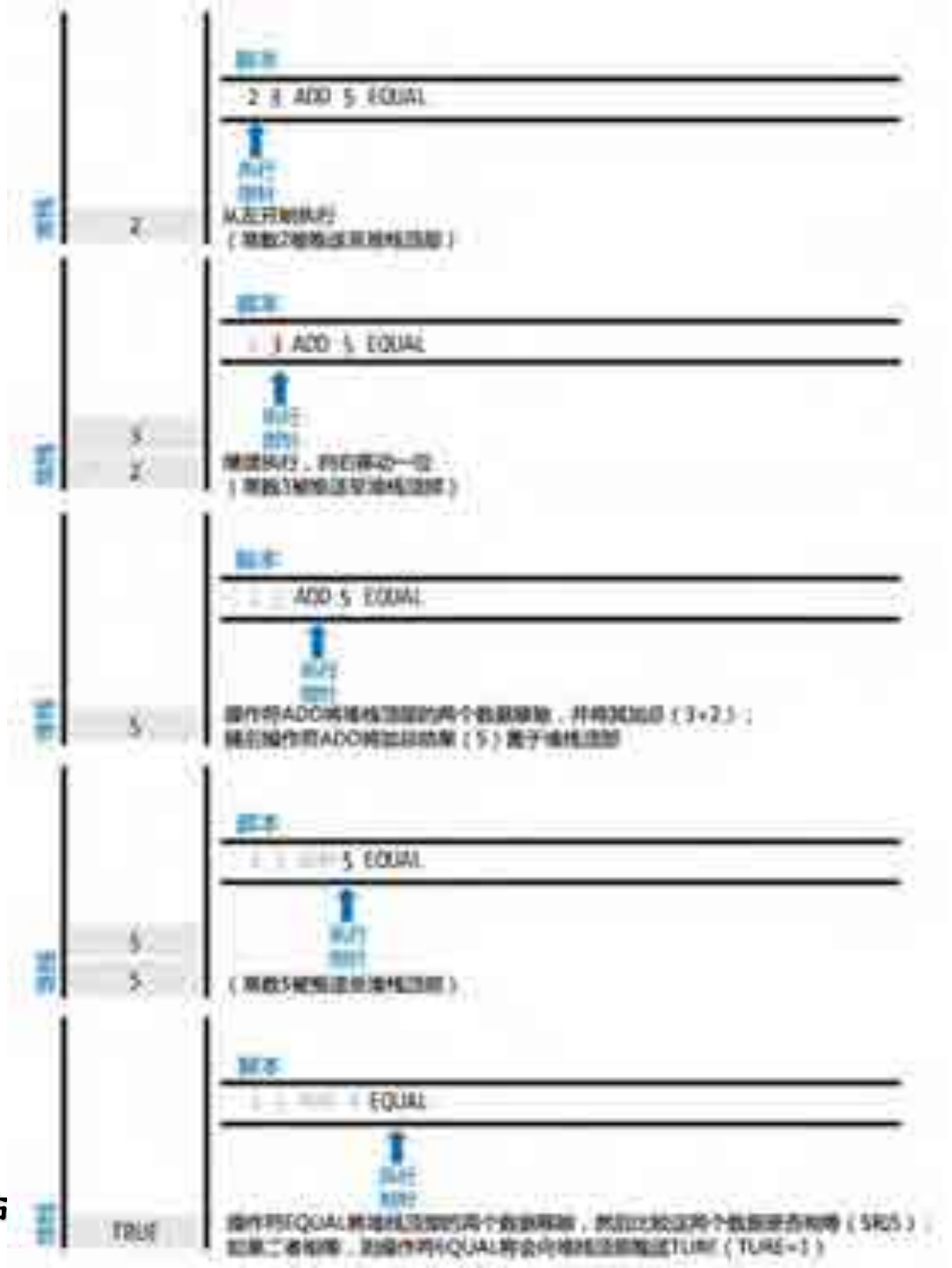
锁定和解锁脚本

The Lock and Unlock Script



逆波兰表示法

Reversed Polish Notation



交易过程(P2PKH)

Pay to Public Key Hash

交易过程(P2PKH)

Pay to Public Key Hash

五大标准脚本

The 5 Standard Types of Scripts

P2PKH

PaytoPublicKeyHash，标准脚本。

P2PK

PaytoPublicKey，更简单的脚本。

MS

Multiple Signature 多重签名，锁定脚本中有N个公匙，至少提供M个签名才能解锁。

P2SH

PaytoScriptHash，把脚本从锁定脚本中移动到解锁脚本中。

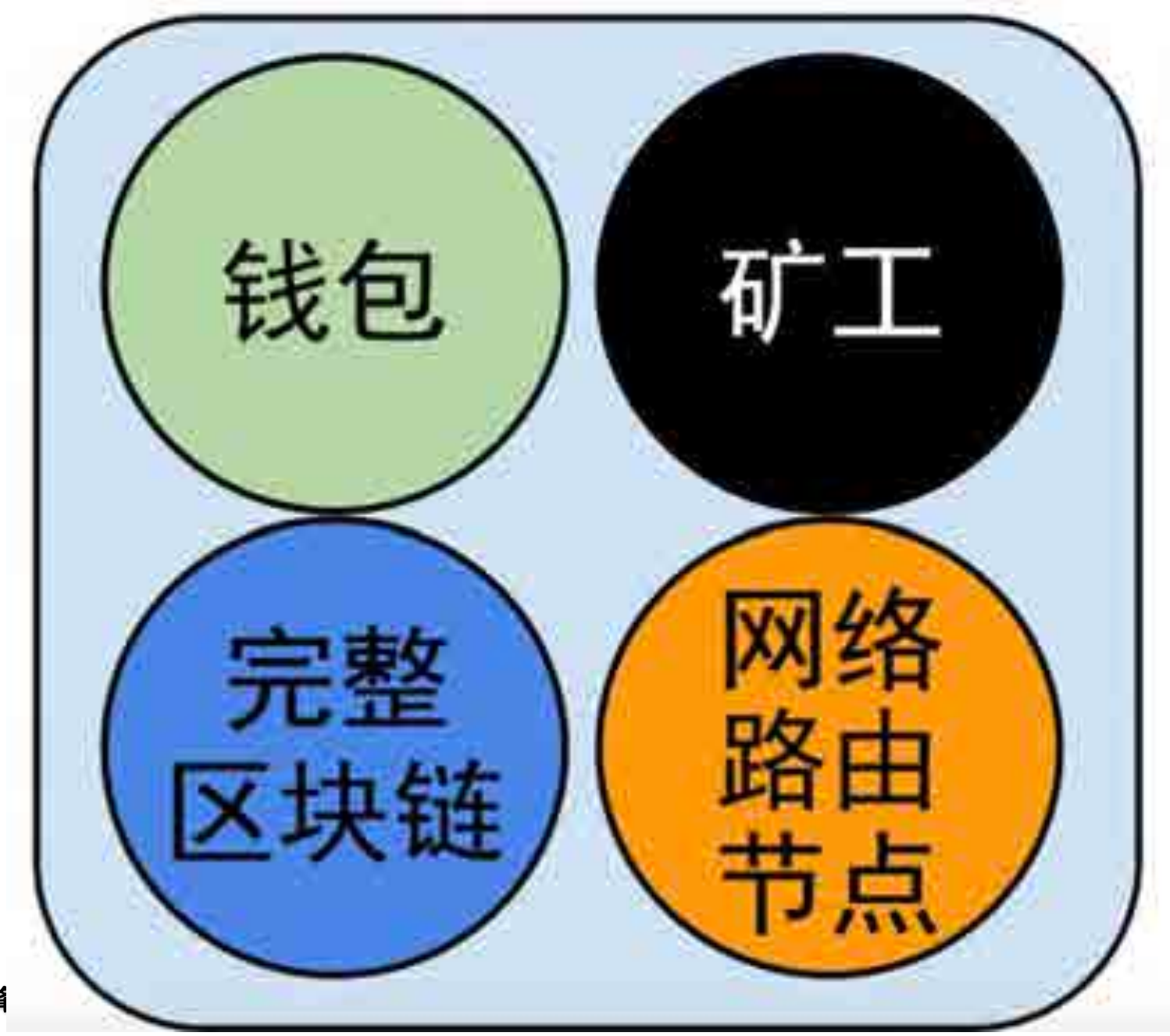
OP_RETURN

非交易类数据，只是为了增加附加信息。

05 P2P网络

节点功能

Functionalities of Nodes



节点类型

Types of Nodes

核心客户端 (Bitcoin Core)

在比特币P2P网络中，包含钱包、矿工、完整区块链数据库、网络路由节点。

完整区块链节点

在比特币P2P网络中，包含完整区块链以及网络路由节点。

独立矿工

包含具有完整区块链副本的挖矿功能，以及比特币P2P网络路由节点。

轻量(SPV)钱包

包含不具有区块链的钱包以及比特币P2P网络节点。

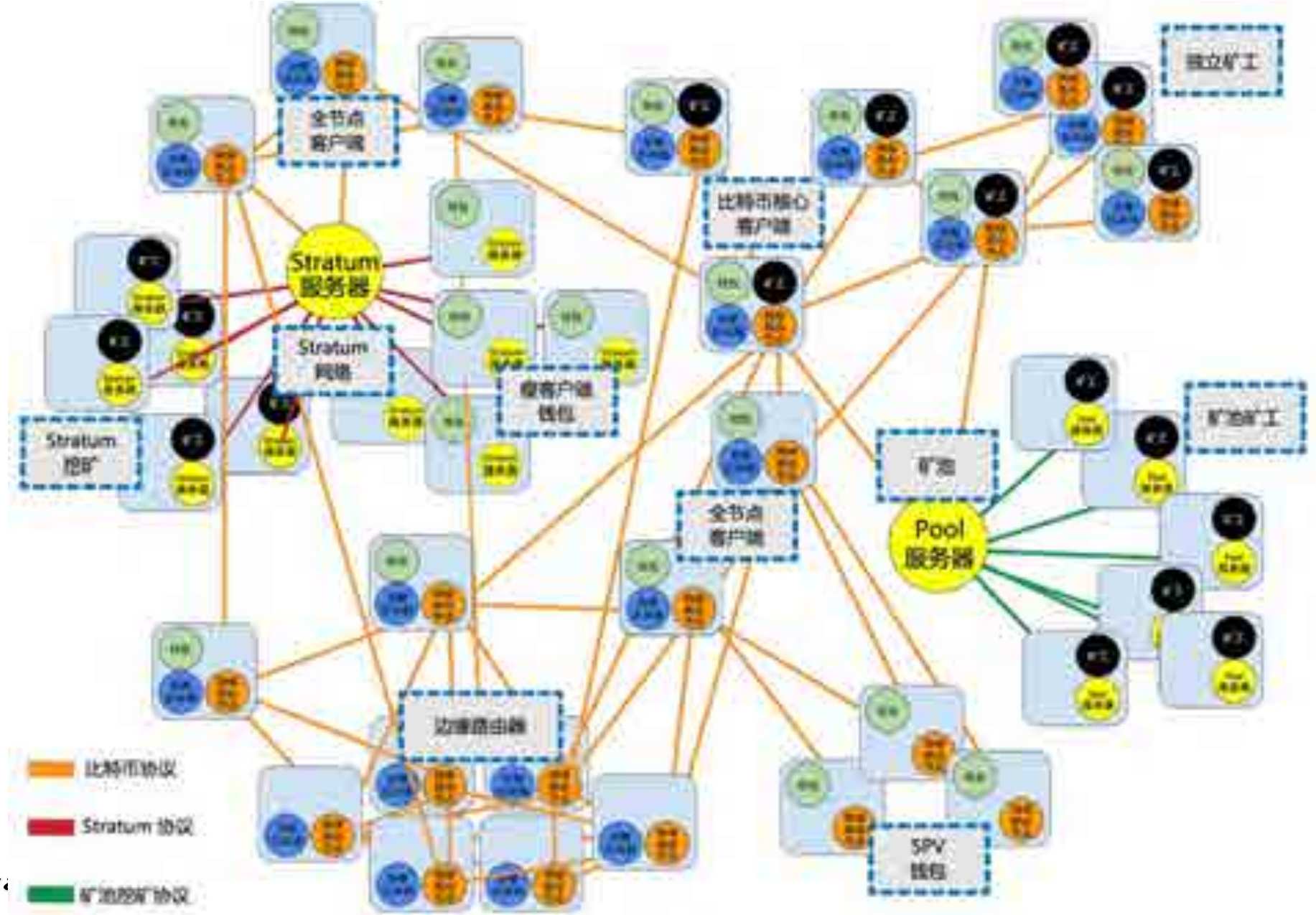
矿池协议服务器

挖矿节点

轻量(SPV) Stratum 钱包

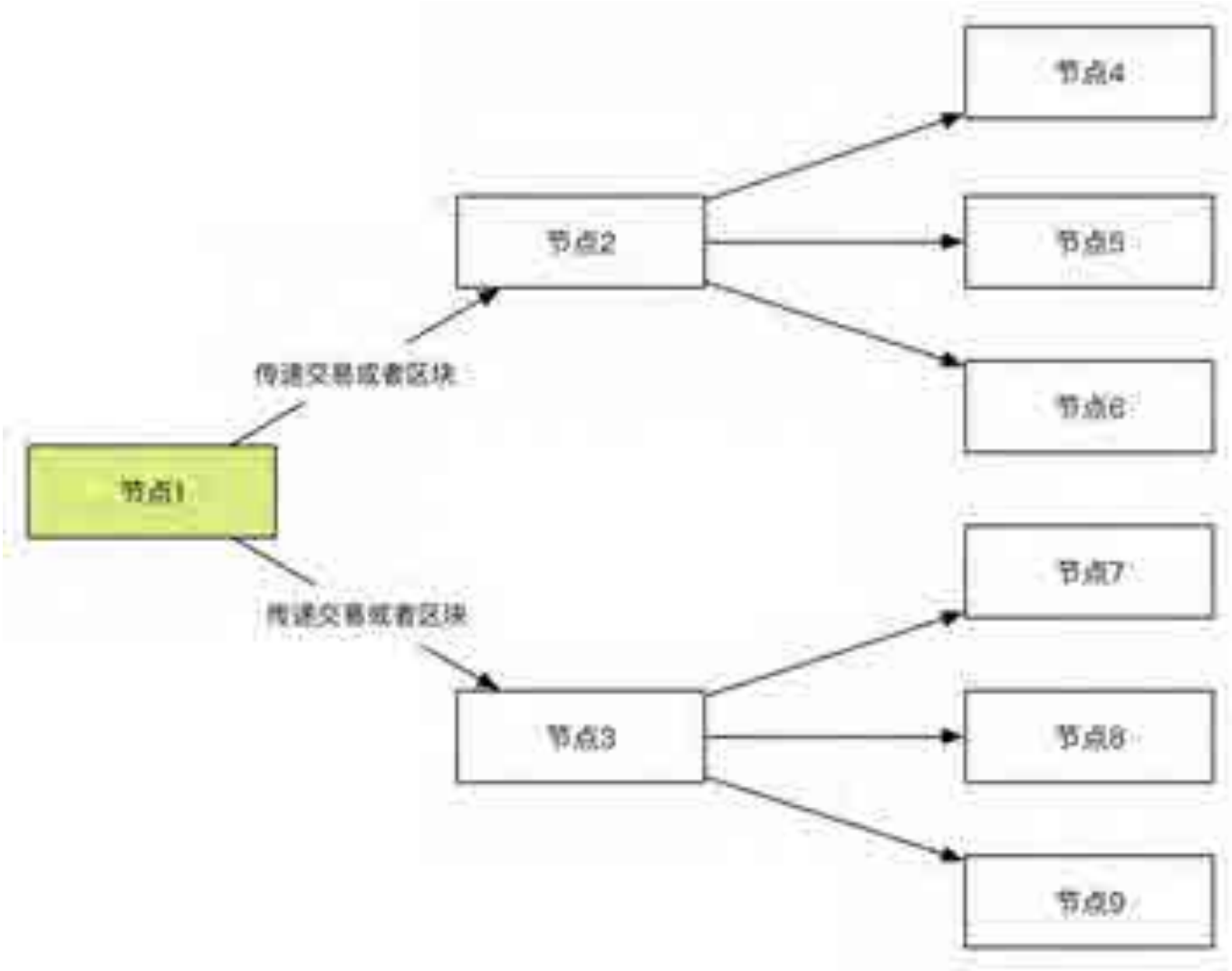
比特币网络示例

Sample of Bitcoin Network



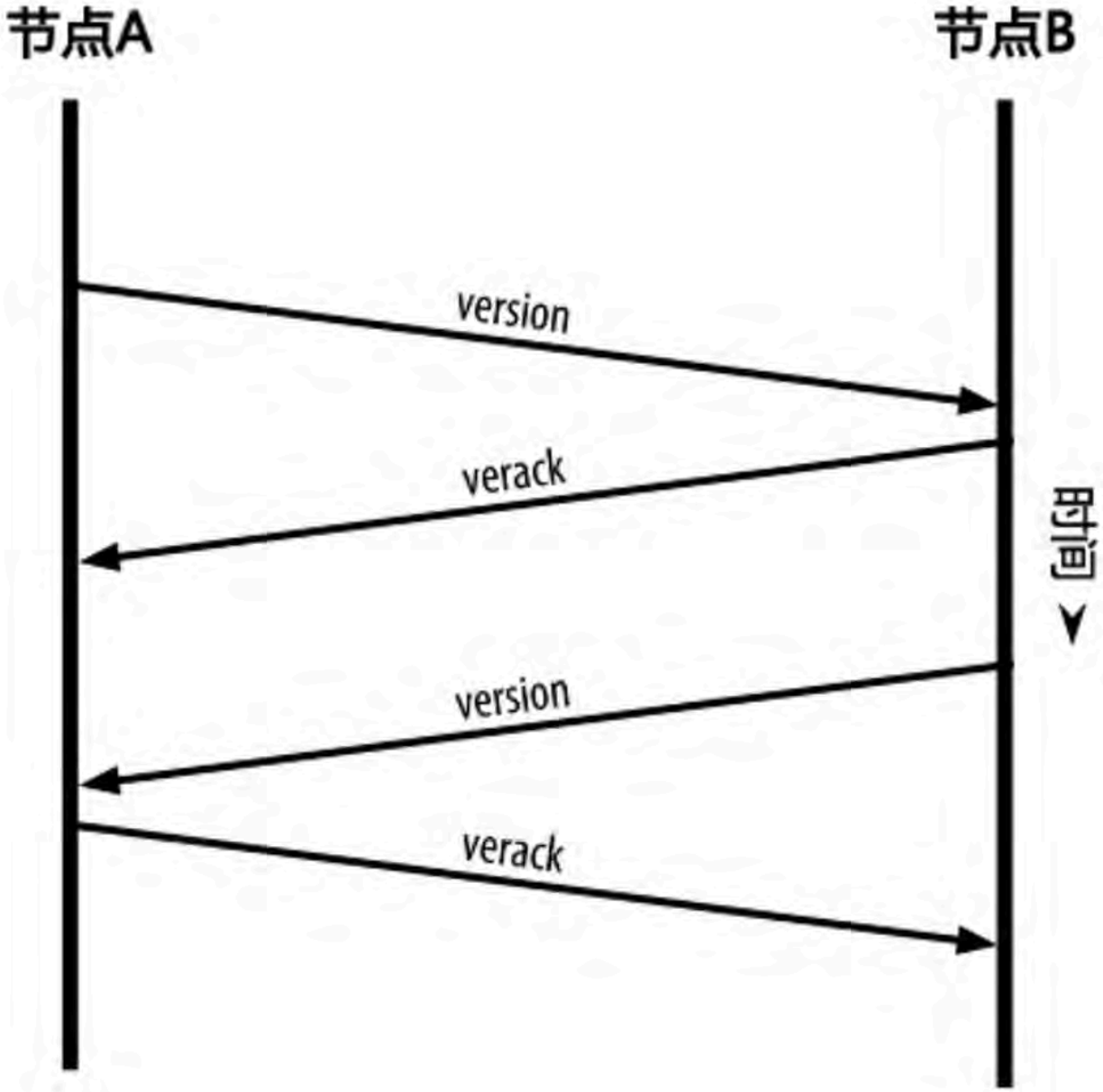
P2P网络示意图

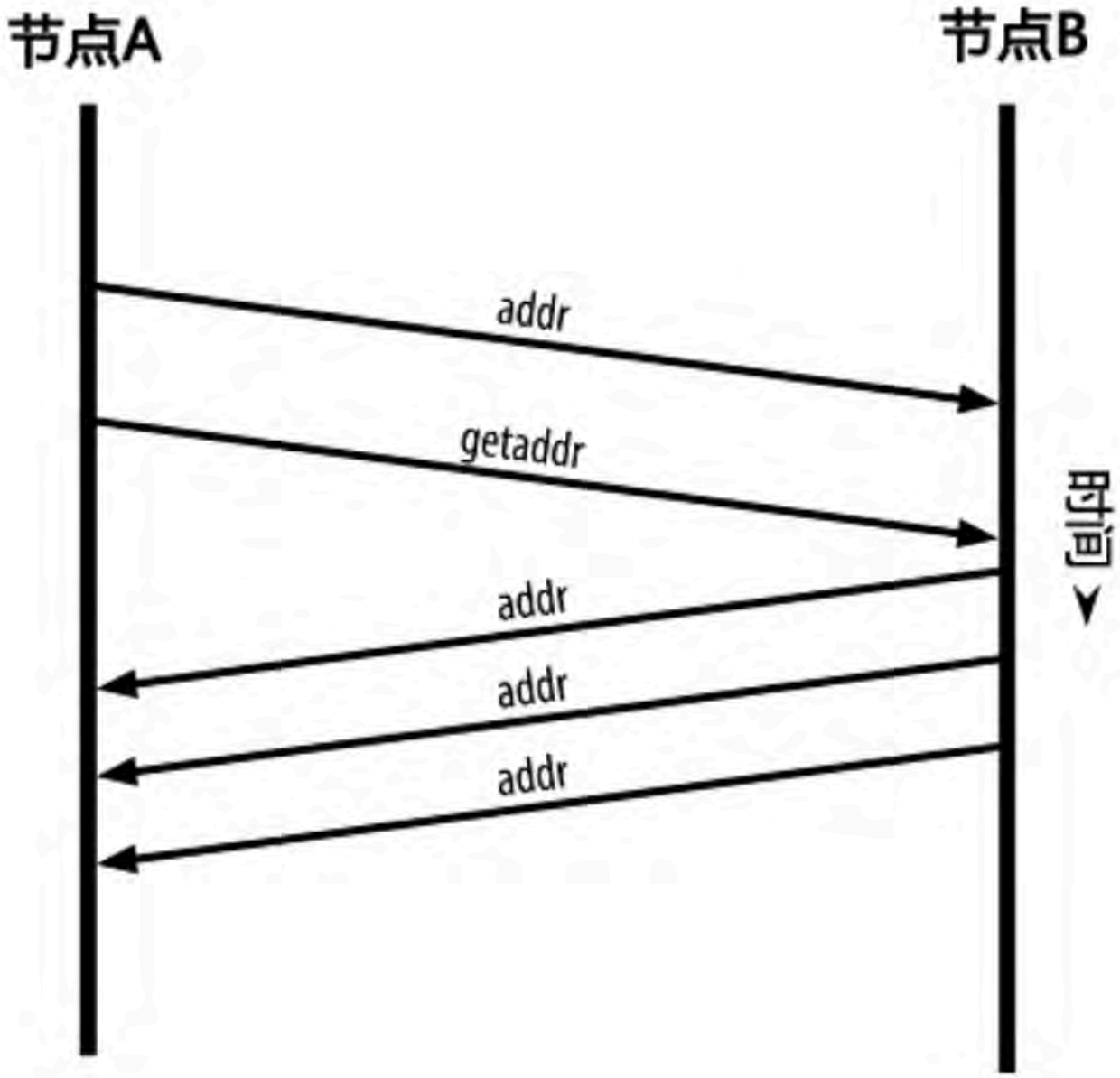
P2P Network



握手和发现

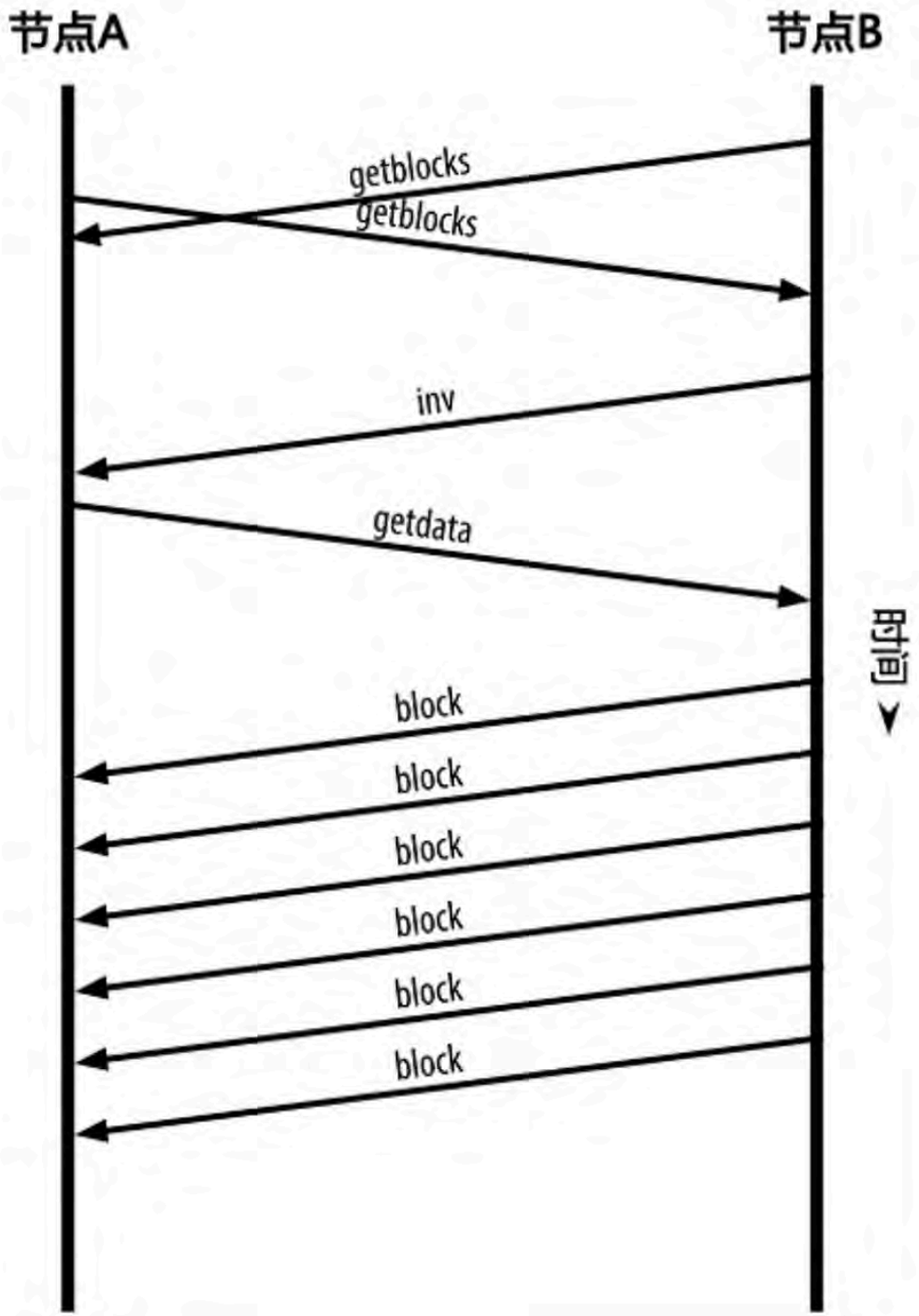
Handshake and Discovery





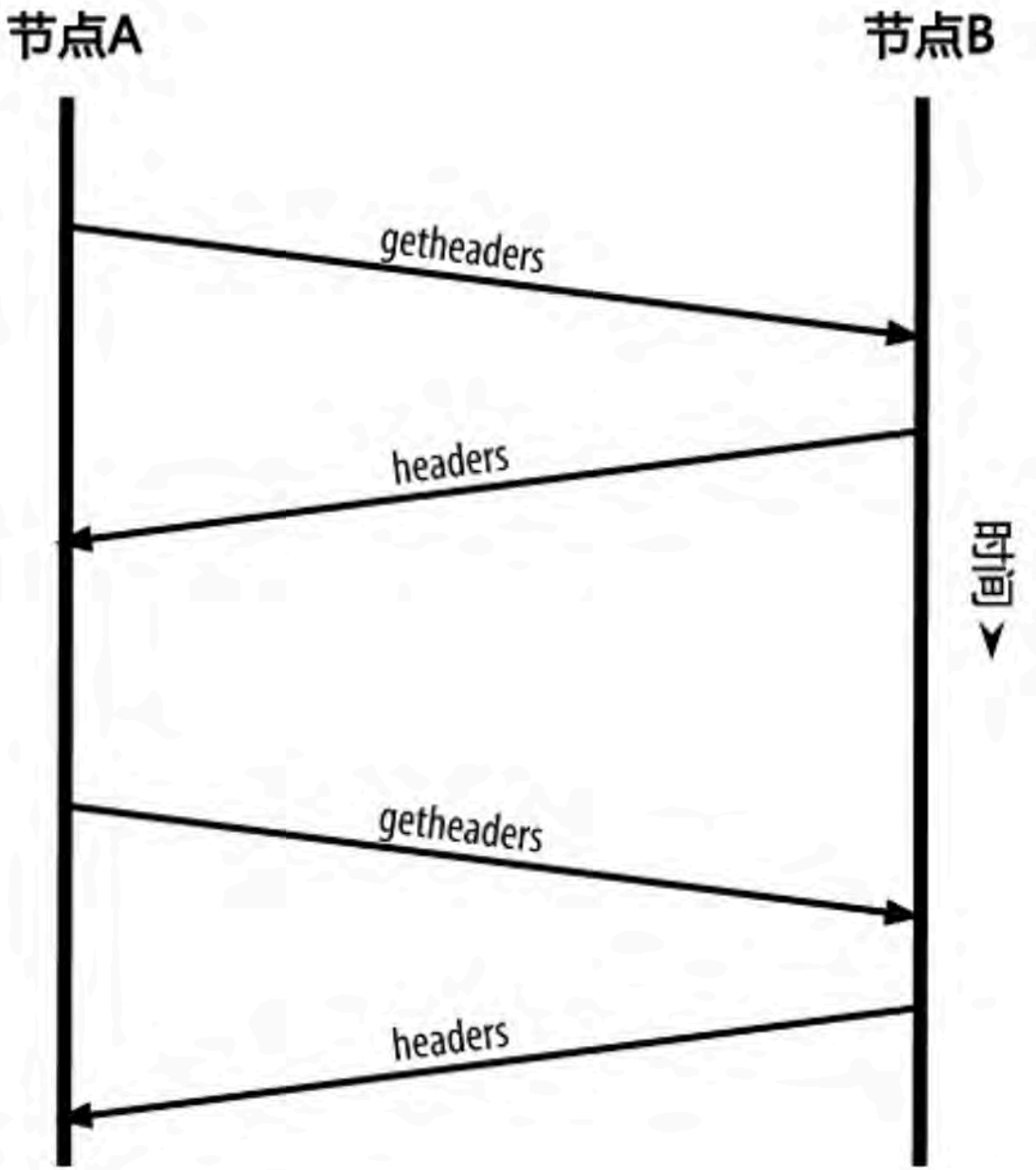
同步区块

Synchronization of Blocks



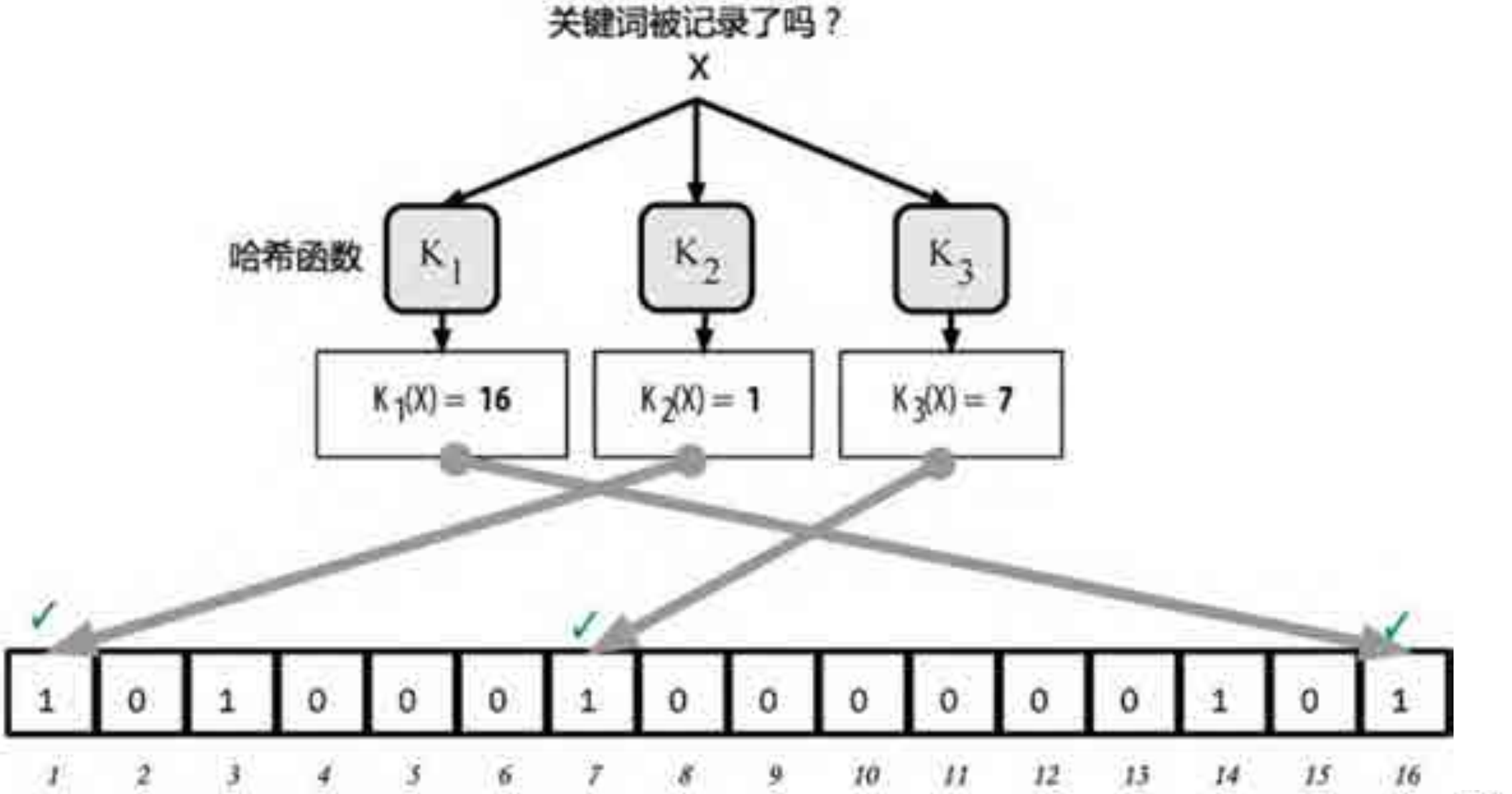
简单支付验证节点

SPV



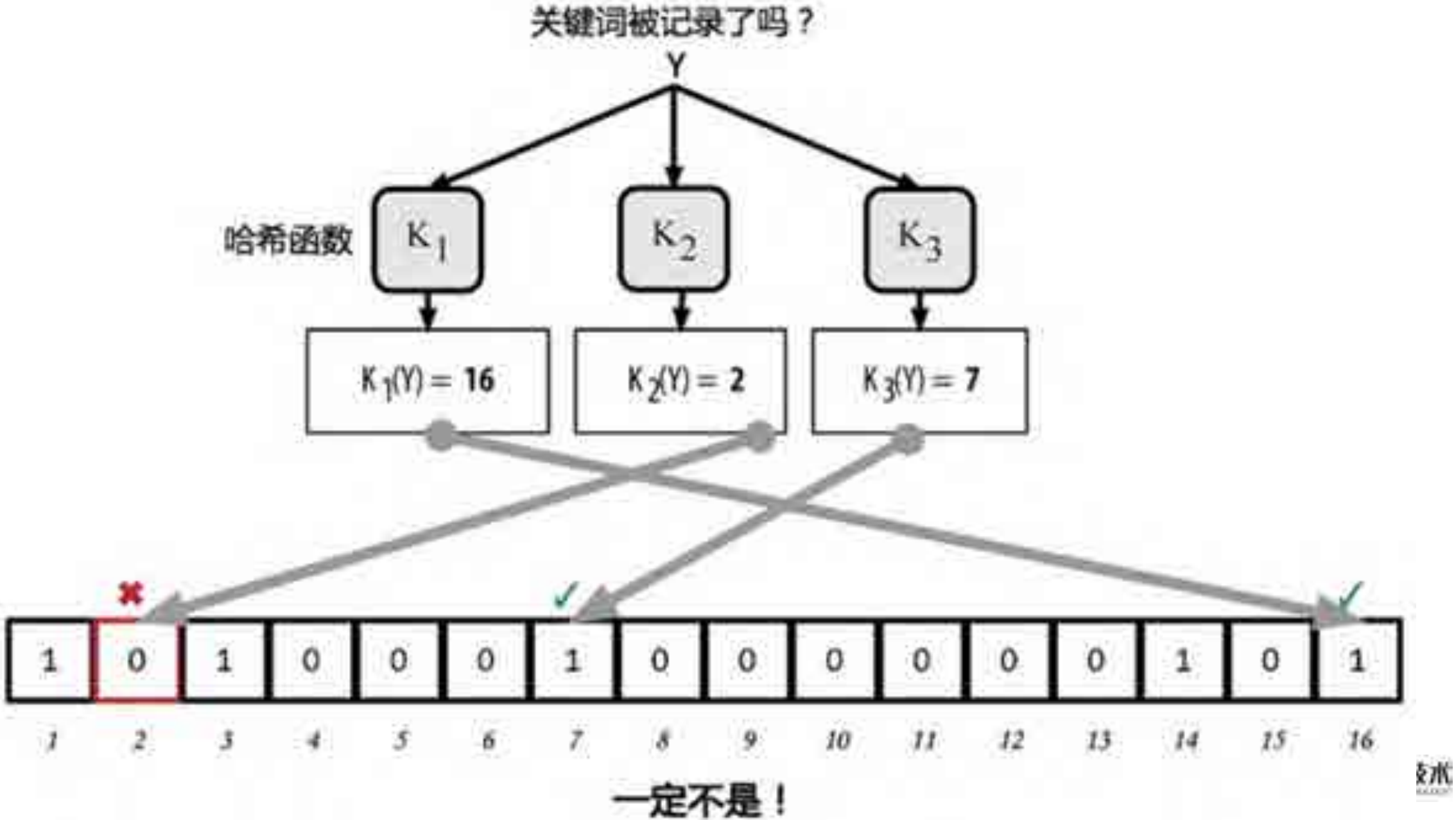
简单支付验证节点-布隆过滤器

SPV-Bloom Filter



简单支付验证节点-布隆过滤器

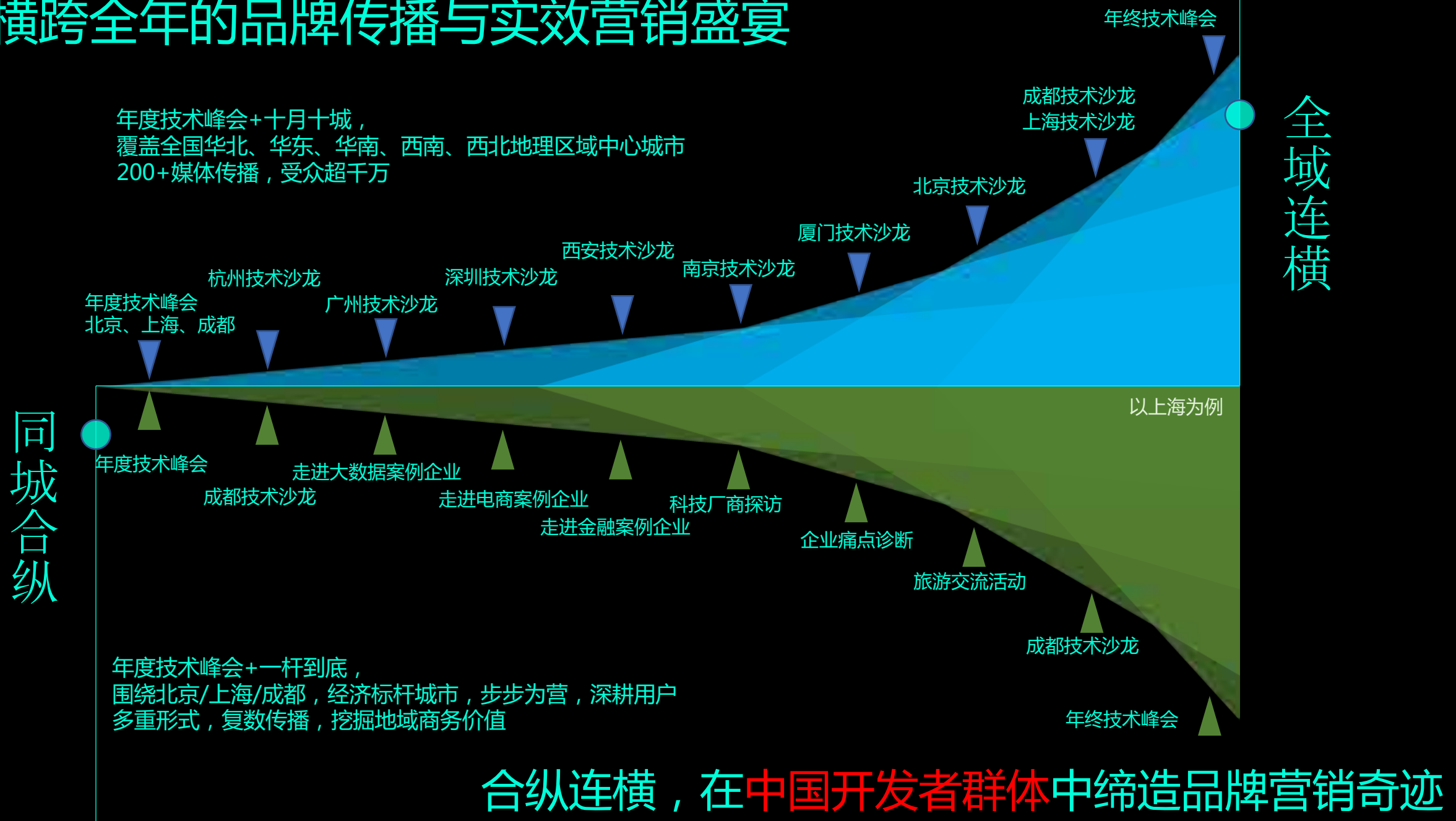
SPV-Bloom Filter



谢谢您的关注

Thank you for your subscribing……

横跨全年的品牌传播与实效营销盛宴



合纵连横，在中国开发者群体中缔造品牌营销奇迹

中生代技术
FRESHMAN TECHNOLOGY

ArchData技术峰会全国巡回
上海9月，北京9月，成都10月，南京10月，
长沙11月，广州11月
中生代咨询内训
技术架构，研发管理，敏捷开发，大数据
微服务，AI，机器学习
中生代人才内推
对接研发主管，内推精准人才