区块链技术与应用

计算机科学与技术学院　李京

10章 区块链的治理和扩容

目 录

10.1 区块链监管与治理-区块链治理

- 区块链是一个分布式系统，它要求网络上的节点对存储在链上数据的内容达成一致，并且不可篡改。区块链一个不断发展的系统，应尝试调整以满足用户需求。因此，区块链如何适应不断变化的时代和需求并与之保持一致的机制称为区块链治理。
  - 链下治理：与传统治理结构相似，集中化程度高。通常由社区领导人达成共识，但产生硬分叉之后用户可自由选择是否更新。
  - 链上治理：治理过程在区块链协议上发生，任何提案或决策都必须嵌入智能合约中，用户、开发者、矿工等都可以通过（代币）投票决定区块链本身的发展方向。

区块链监管与治理-区块链监管

- 区块链因去中心化、不可篡改、自激励的特性，使其成为一个由技术驱动但深刻影响着经济、金融、社会、组织形态及治理的综合课题。区块链技术特点使得区块链的安全监管问题非常突出：
  - 去中心化的分布式共享账本带来了监管主体分散的问题
  - 自动执行的智能合约带来了其法律有效性的问题
  - 区块链难以篡改的特性带来的数据隐私和内容监管问题
  - 激励机制与数字资产特性带来的金融监管问题

10.2 区块链扩容

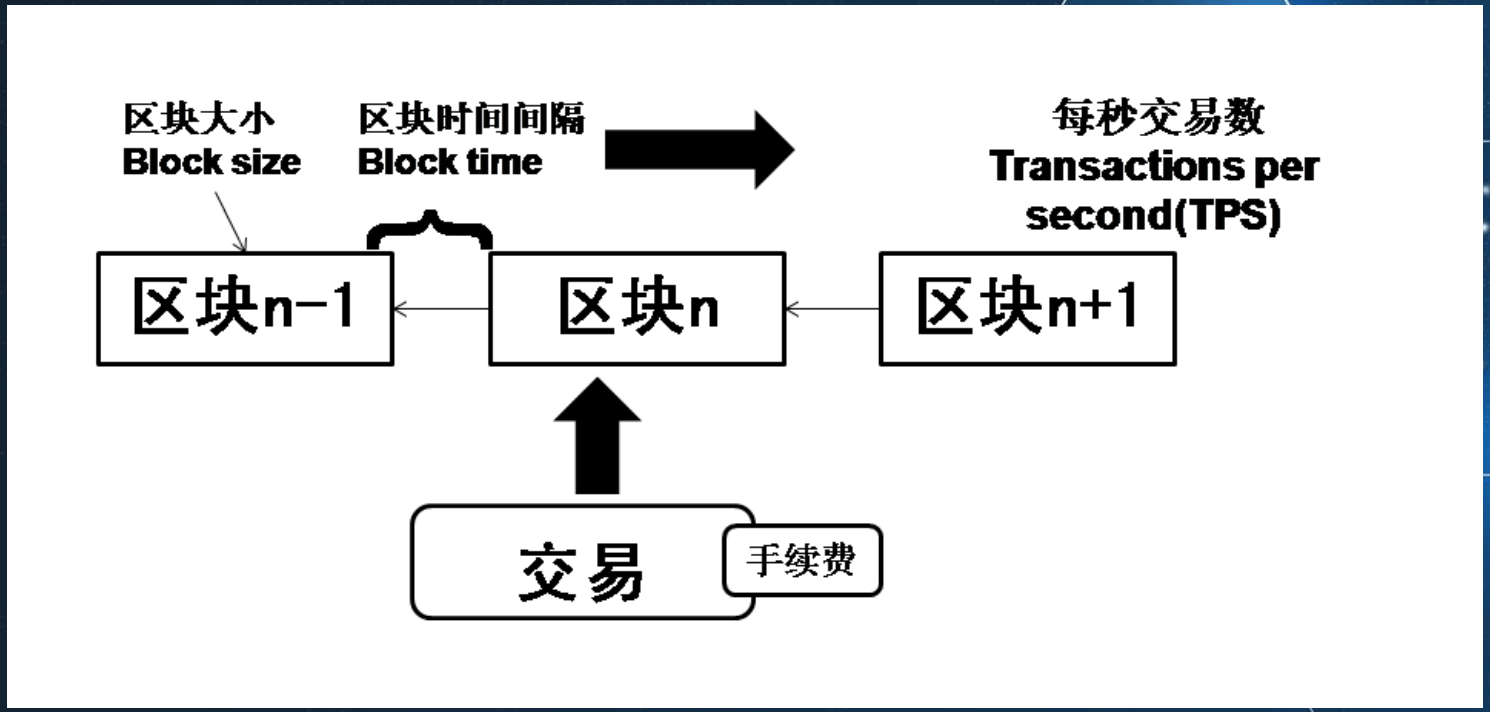
- 可扩展性是当今采用区块链技术的最大障碍。BTC虽然提供了安全性和去中心化，但其吞吐量与 Visa 的 1700 TPS 相比，比特币的 TPS 只有4-7。
- 以太坊作为支持智能合约和去中心化应用程序（DApps）的市场领导者，其平均的 TPS 约为 10 笔，最好的时候能达 20 笔。
- 对于依赖高性能传统交易处理系统的企业来说，区块链缓慢的交易速度是一个无法回避的严峻问题。

	Bitcoin	Ethereum	NEO	Bitshares	Waves	Qtum	PayPal	Visa	支付宝双十一
共识机制	PoW	PoW-PoS	DBFT	DPoS	PoS	PoS	-	-	-
实际TPS	3-4	25-30	1000	17	100	70	193	1667	256,000(2017) 491,000(2018)

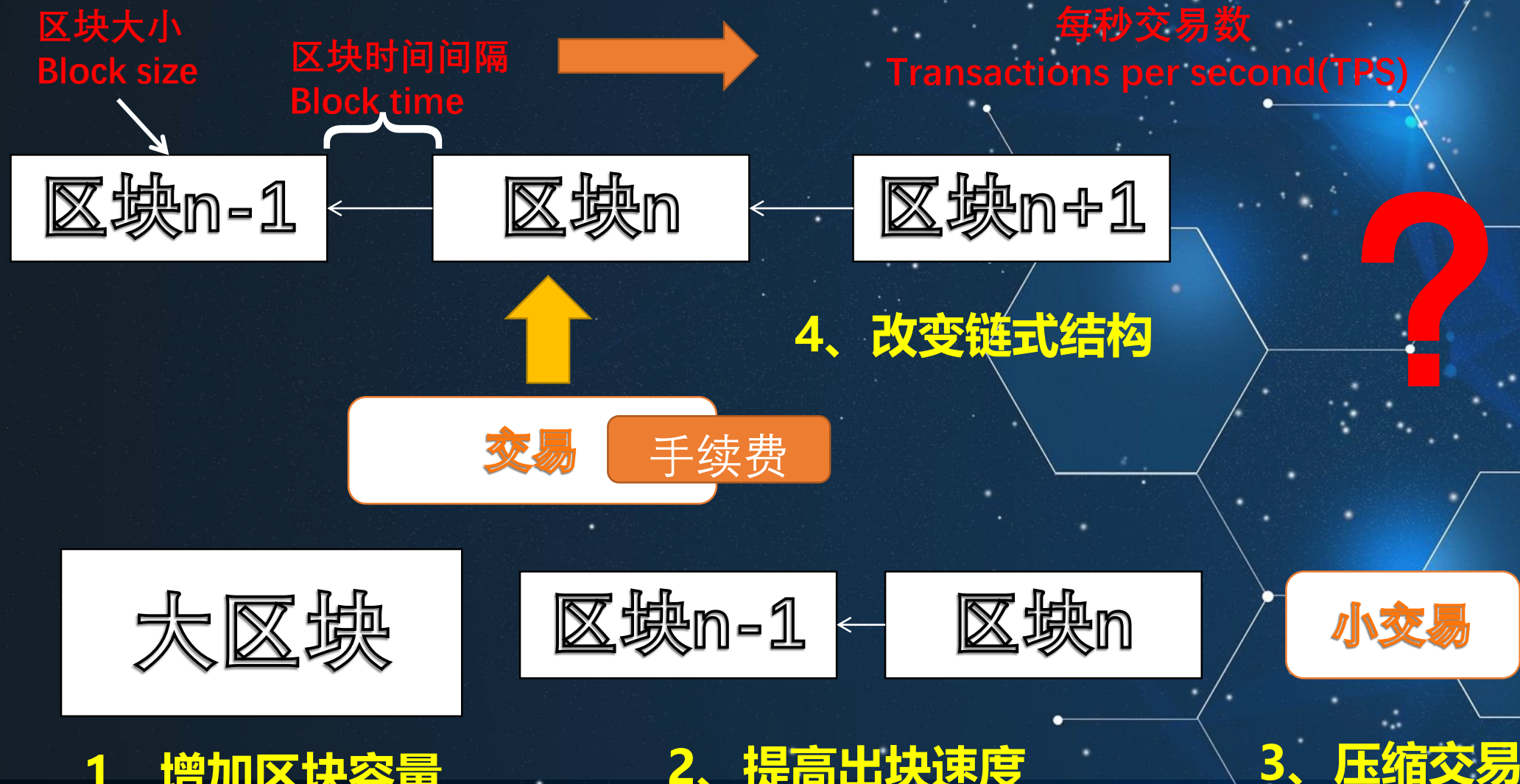
TPS（Transactions Per Second，平均每秒交易量）

原因分析：区块链结构和共识机制

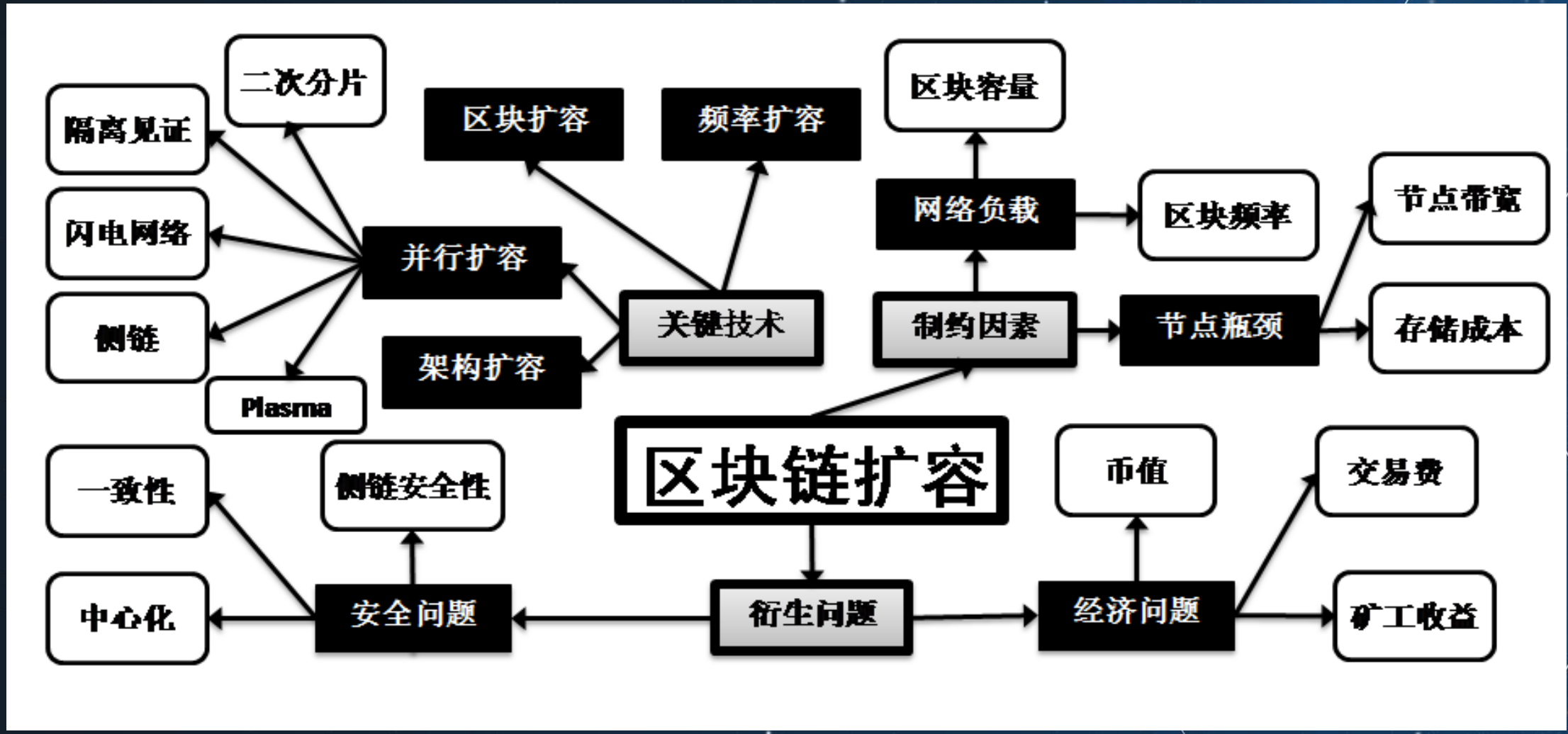
- 由区块链接而成的链式结构，每笔交易都被记录在一个区块上，矿工收入来自挖矿的系统奖励与交易手续费，受区块大小与区块时间间隔约束，可以“纳入”区块的交易数量有限，这硬性地限制了支付网络上的链上交易量。
- 节点数量多、分布广，网络负载大



扩容思路

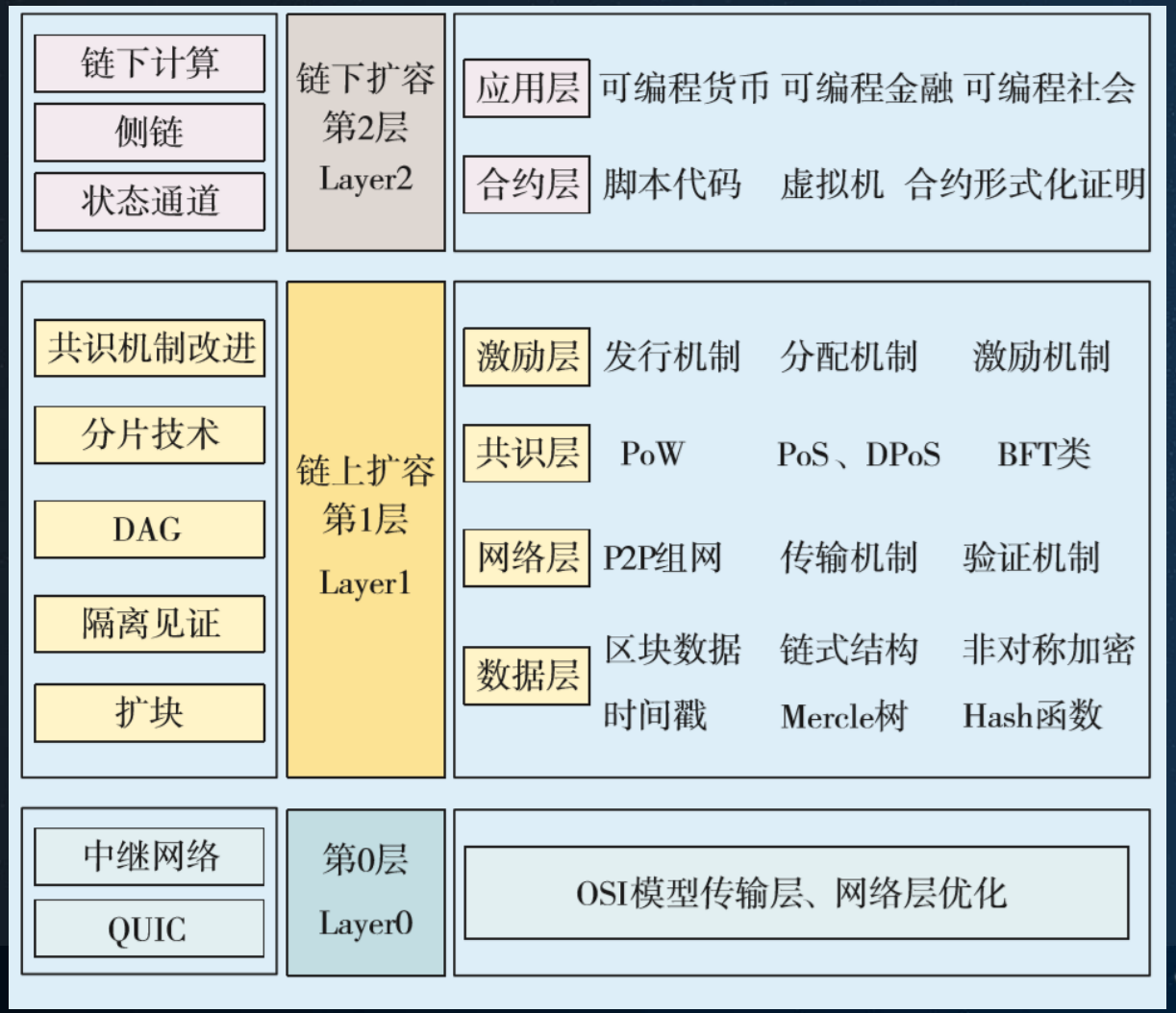

区块大小
Block size
区块时间间隔
Block time
每秒交易数
Transactions per second(TPS)
区块n-1
区块n
区块n+1
?
4、改变链式结构
交易
手续费
大区块
区块n-1
区块n
小交易
1、增加区块容量
2、提高出块速度
3、压缩交易大小

研究框架


区块链扩容
关键技术
并行扩容
二次分片
隔离见证
闪电网络
侧链
Plasma
区块扩容
频率扩容
架构扩容
制约因素
网络负载
区块容量
区块频率
节点瓶颈
节点带宽
存储成本
衍生问题
安全问题
一致性
中心化
侧链安全性
经济问题
币值
交易费
矿工收益

区块链扩容

- 区块链扩容方案

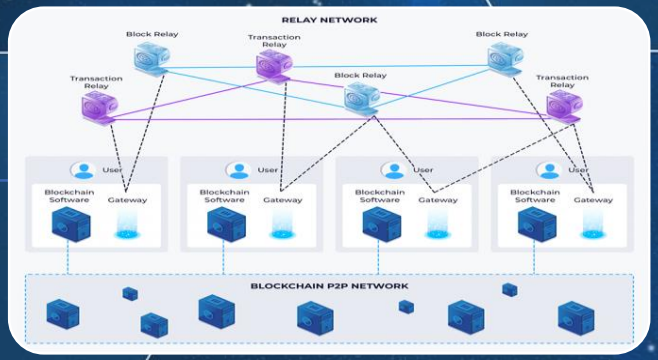


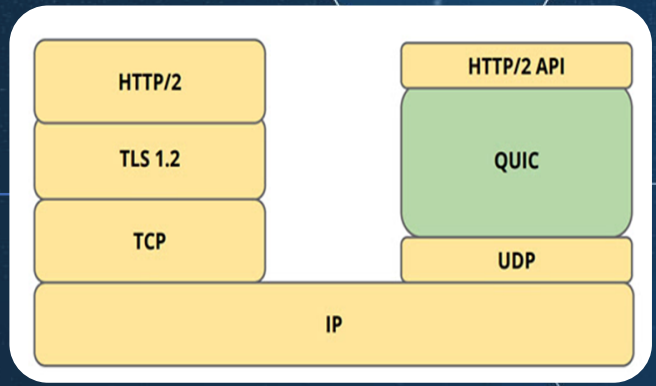
区块链的扩展性是阻碍区块链技术大规模应用的主要瓶颈，在维护区块链系统的去中心化、不可篡改和安全性等所有核心价值的前提下，通过提升联盟区块链架构的容量和扩展性，达到实体经济的产业级性能要求。目前学术界已经提出一些扩容方案：超级节点，链外扩展，链内扩展。超级节点将共识权利完全交给了具备超高性能的少数节点，从而提升了交易速度和总吞吐量。链外扩展主要包含侧链和状态通道两种伸缩方案，都是将大多数事务在主链以外进行处理，从而绕过主链系统的性能瓶颈。链上扩展以分片技术（Sharding）和有向无环图（DAG）为主，希望通过改变网络中节点的结构来实现区块链的可扩展性。提出一种链上+链下联合扩容方案，提升链上数据处理能力，并将部分事实移至链下处理，有效提升区块链容量和可扩展性。

区块链扩容-第0层扩容方案

第0层扩容方案

- 覆盖网络
  - 比特币中继网络
  - 区块链分发网络
- QUIC优化协议

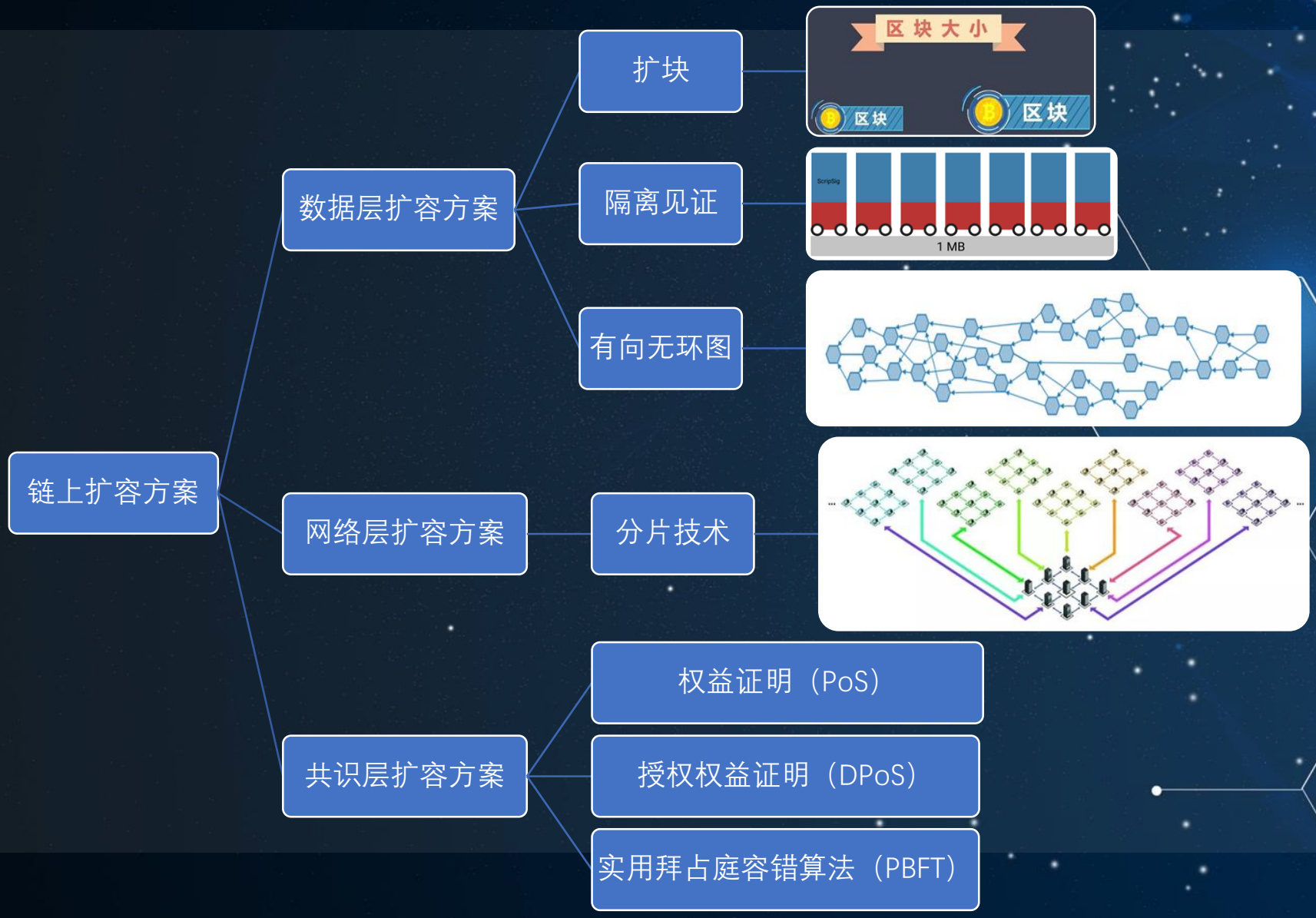




覆盖网络：覆盖网络能够快速传播区块，减少区块在网络间传播时延。

QUIC优化协议：优化OSI传输层协议，加快区块传播速度，减少网络时延。

区块链扩容-链上扩容方案



扩块：通过扩大区块容量，增加数据区块能够打包的交易数，间接提升系统吞吐量。

隔离见证：将数字签名信息移出区块，增加区块容纳交易数量，提升系统吞吐量。

有向无环图：块链式结构改为DAG网状并发式结构， 实时验证交易。

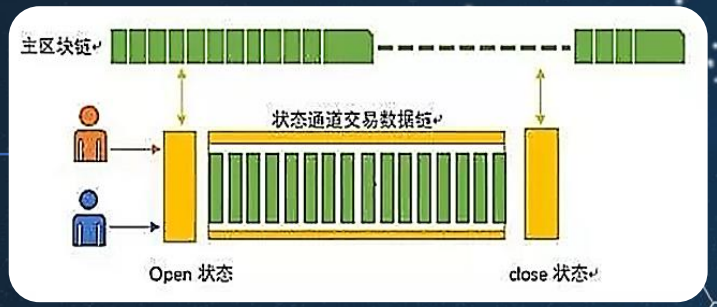
分片技术：将网络分片，每个分片独立并发处理全网交易。

共识机制改进：PoS、DPoS、PBFT 等改进算法、混合共识算法。

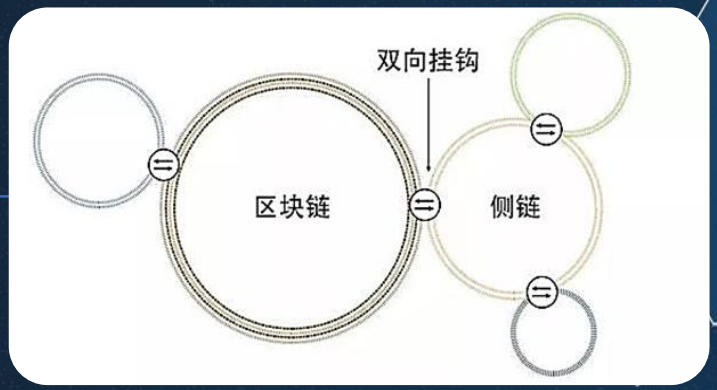
区块链扩容-链下扩容方案

链下扩容方案

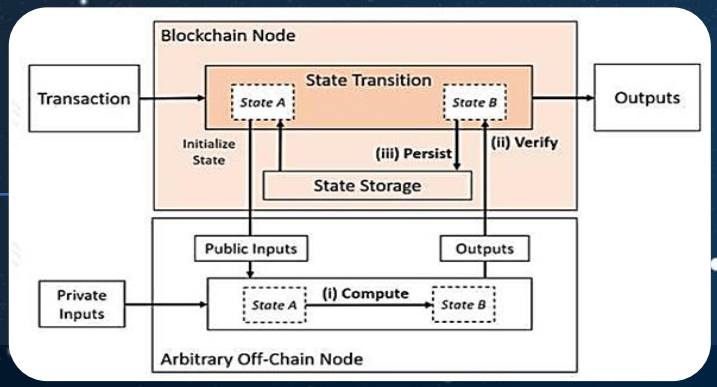
- 状态通道
- 侧链
- 链下计算



状态通道：建立通信双方间的私密双向通道，将计算下放到通道进行，将最终结果上链。



侧链：将不同的区块链互相连接在一起，以实现区块链的扩展。



链下计算：将原本置于链上处理的各类事务，移至链下处理，而链上仅保留验证的部分，以此间接提升链上的数据处理能力。

区块链扩容-区块链存储扩容

比特币的扩容方案

- 侧链：BTC-Relay是一种让比特币可以在其他系统（至少是以太坊）能够流通的一个跨链技术方案，它也是区块链生态系统中公认的第一条侧链。
- 状态通道：闪电网络(Lightning Network)将大量交易放到比特币区块链之外进行。
- 覆盖网络：比特币中继网络(BRN)和快速互联网BTC中继引擎(Fast Internet Bitcoin Relay Engine，FIBRE)。比特币中继网络(BRN)，选取多个服务器作为枢纽，以便能够将区块数据快速分发到世界各地，减少区块链网络共识传播的延迟.快速互联网BTC中继引擎(FIBRE)是中继网络的升级版。

以太坊的扩容方案

- 子链：Plasma在以太坊主链上创建“子链”，处理链下交易的技术，需要依赖以太坊底层技术去对其安全性进行保障。
- 状态通道：雷电网络(Raiden Network)是状态通道技术在以太坊上的实现。利用链下（off-chain）状态网络对以太坊交易处理能力进行扩展。
- 分片+PoS：以太坊2.0

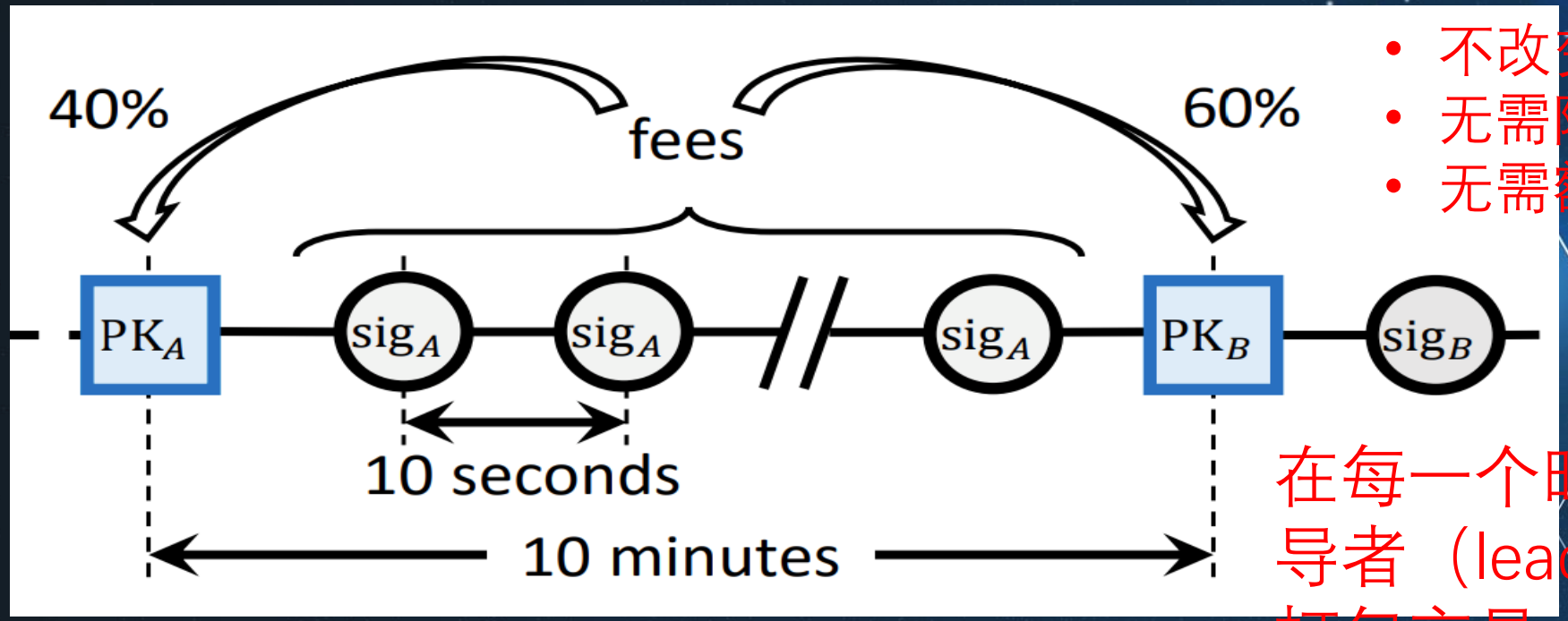
区块链扩容-区块扩容

- BIP100提议将区块容量控制权交给矿工，曾得到占据全网算力25%的三家矿池（f2pool、Kano pool以及 Bitclub）的支持，但同时也引发了许多争议；
- BIP101曾获得业内多家公司支持，曾一度被加入BitcoinXT代码库，但BitcoinXT后来转而支持Classic的2MB区块方案；
- 2016年2月份，Gavin Andreesen基于BIP109创立了Bitcoin Classic。Bitcoin Classic得到了一些比特币公司、开发商、投资者和矿商的支持。2017年11月10日，在通过硬分叉将比特币区块容量扩大到2MB的计划失败后，Bitcoin Classic宣布停止运营，并称比特币现金是扩展比特币的唯一希望；
- 经过香港共识、纽约共识的失败，于2017年8月1号，在ViaBTC等大矿池的推动下，比特币通过硬分叉产生了一条新的区块链，被称为“比特币现金(bitcoin cash)”。比特币现金支持8MB的大区块，获得了Bitcoin ABC、Bitcoin XT、Bitcoin Unlimited、Bitcoin Classic等力推链上扩容的主要开发团队的支持。
- 2018年5月15日，比特币现金通过第二次硬分叉升级为支持32MB（第一次是2017年11月13日）；同年11月10日，比特币现金创建了历史上第一个接近32MB的大区块，该区块高度为556034，它的大小约为31997,634 kB（31,99 MB）。
- 11月15日，比特币现金再一次硬分叉为Bitcoin ABC和Bitcoin SV（Satoshi's Vision），后者进一步将区块大小限制提高到128MB

区块链扩容-出块时间-比特币及其衍生币

- 比特币的难度机制
  - 比特币通过调整难度（difficulty），控制区块生成间隔在10分钟左右
  - 比特币衍生币也采用类似机制
- 比特币现金：紧急难度调整（Emergency Difficulty Adjustment，EDA）机制
  - 若12小时内生成区块的数量小于6，就将难度下调20%
  - 算力的剧烈波动对比特币和比特币现金都造成了冲击
- 2017年11月13日，比特币现金进行了第一次硬分叉，原链称为Bitcoin clashic（BCL），新的比特币现金对EDA机制进行了修改，以保证出块速度仍然维持在10分钟左右，但“被分出去”的BCL目前仍在运转中

区块链扩容-出块时间-Bitcoin-NG



- 不改变区块容量
- 无需降低难度
- 无需额外增加矿工的工作量

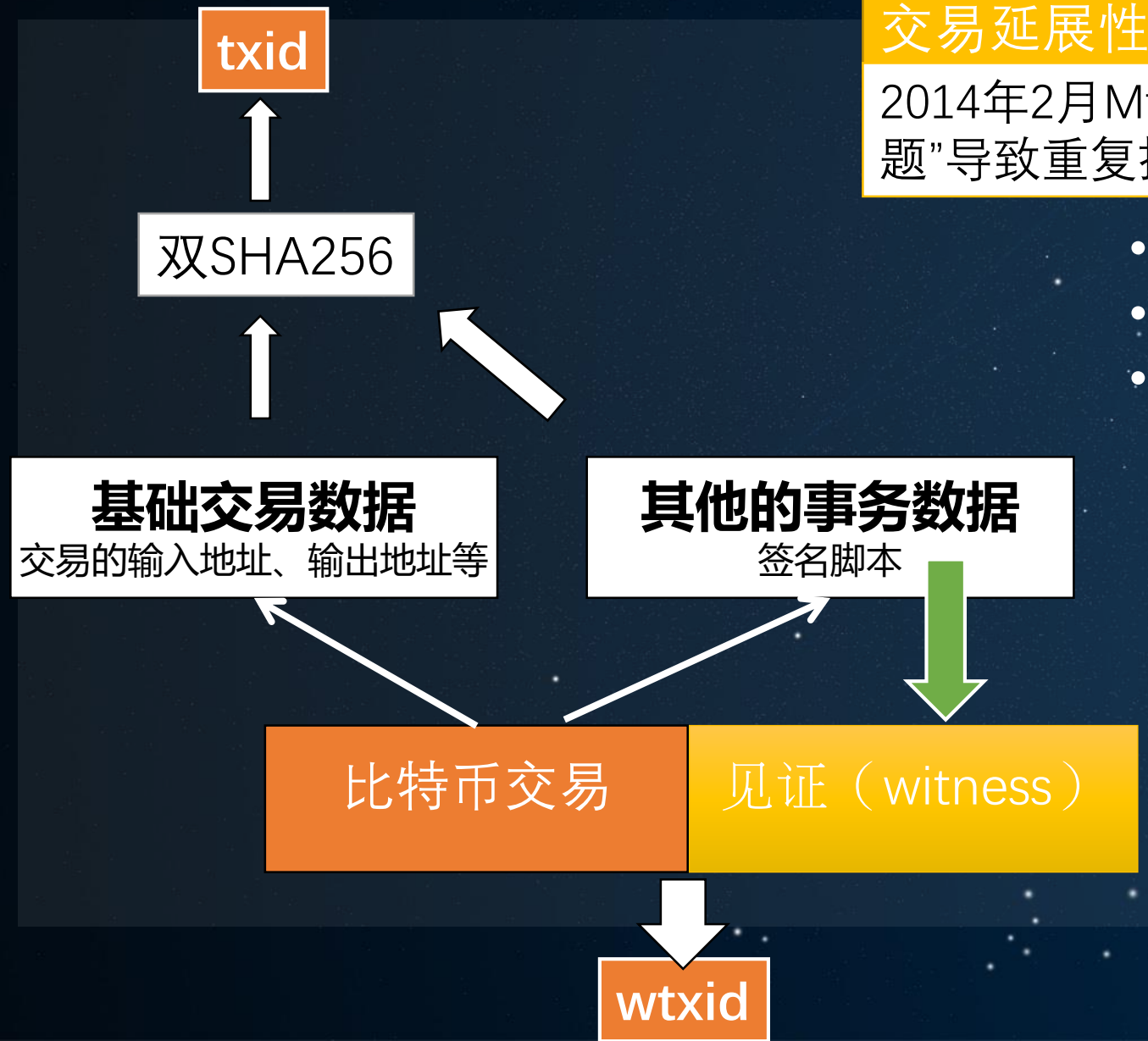
在每一个时间段上，由一个领导者（leader）负责生成区块，打包交易。

用于选举领导的关键区块(key blocks)

包含交易数据的微区块(micro blocks)

（康奈尔大学，Ittay Eyal等）

区块链扩容-架构扩容-隔离见证



交易延展性（transaction malleability）

2014年2月Mt.Gox交易所声称由于“交易延展性问题”导致重复提现，造成部分比特币的丢失。

- secp256k1的椭圆曲线加密签名
- 攻击者可以进行非功能的修改
- 当交易所或用户基于txid查询交易时，会无法确认交易完成，发送大量交易请求

区块中的所有wtxid被存储在一棵梅克尔树的叶子结点上，这棵树的根节点HASH记录在coinbase交易的scriptPubKey中。

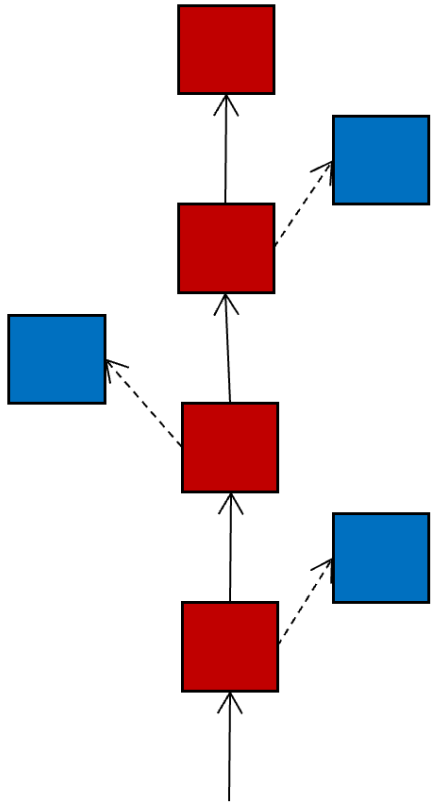
2015年12月香港比特币扩容会议中由Bitcoin Core开发团队的Pieter Wuillle提出

区块链扩容-架构扩容-隔离见证

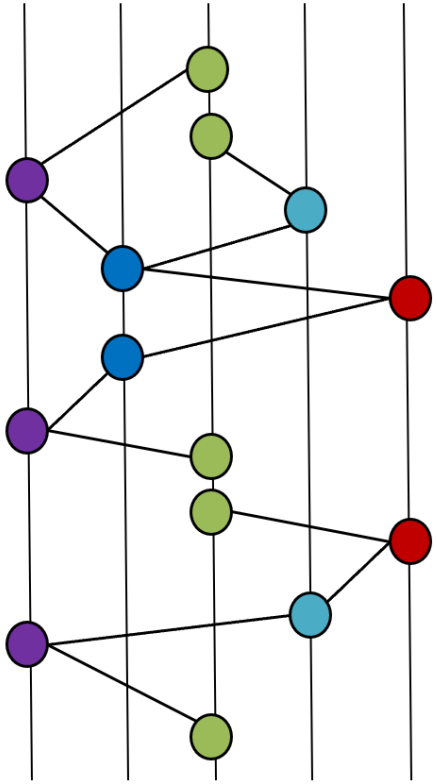
2017.5.11，莱特币正式激活隔离见证;

2017.8.24，当区块高度达到481,824，比特币正式激活隔离见证，第一个Segwit交易被写进比特币中;

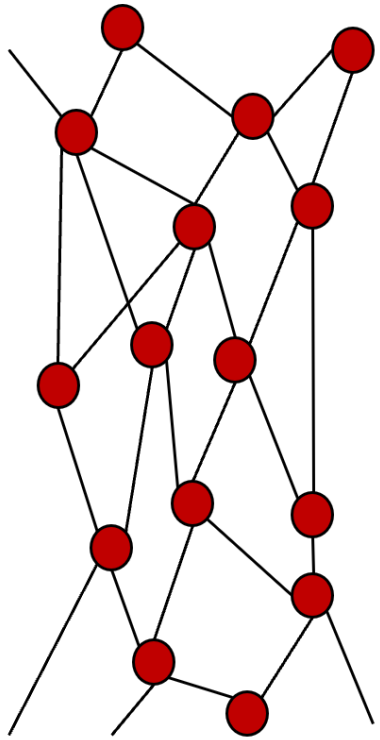
区块链扩容-架构扩容-基于DAG的新型区块链架构



链式结构



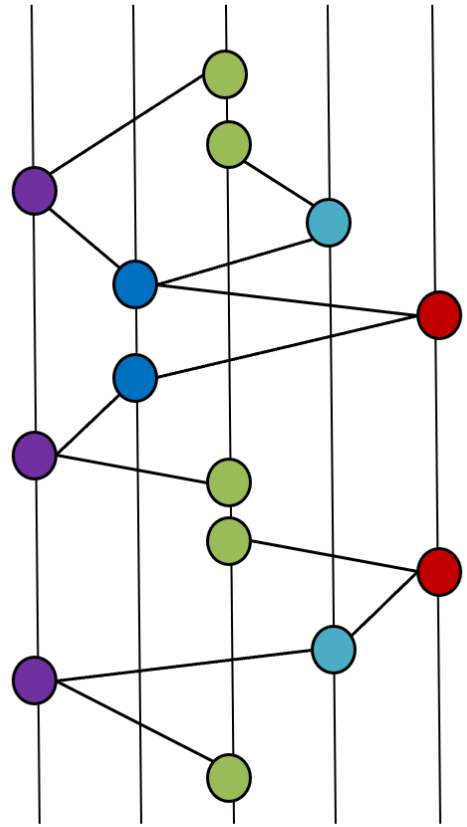
哈希图（Hash Graph）



缠结（Tangle）

区块链扩容-架构扩容-HashGraph

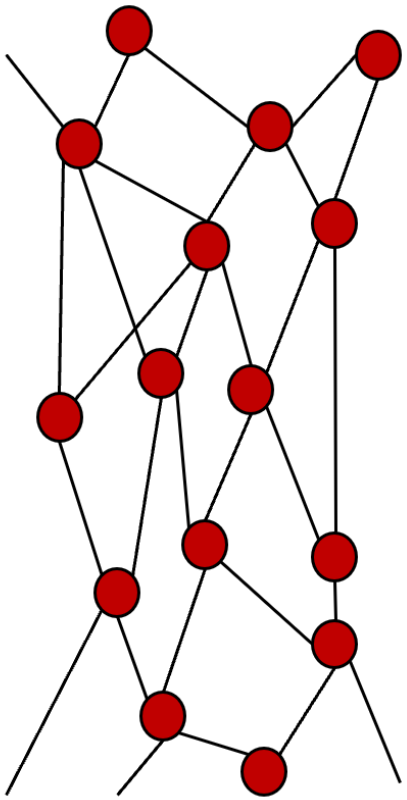
- Hedara Hashgraph: building a fast and secure blockchain alternative
- 共识：aBFT（Asynchronous Byzantine Fault Tolerant异步拜占庭容错算法）
- 见证即投票
  - 每个参与者维护单独的链条，该链条上都是自己生成的区块
  - 每个区块需引用两个区块，一个是自己上一个生成的区块，另一个是收到的最新区块
  - 类比“八卦网络”中的话题传播



哈希图（Hash Graph）

区块链扩容-架构扩容-IOTA

- 基于名为Tangle（缠结）的有向无环图而建立交易之间的联系
- 无需矿工挖矿来记录交易
- 每个参与者都有相同的激励和奖励，而无需建立角色和职责的层次结构
- “付费转发”的交易验证系统
- 适合物联网场景



缠结（Tangle）

区块链扩容-并行扩容

闪电网络(Lightning Network)

雷电网络(Raiden Network)

Plasma

分片(Sharding)

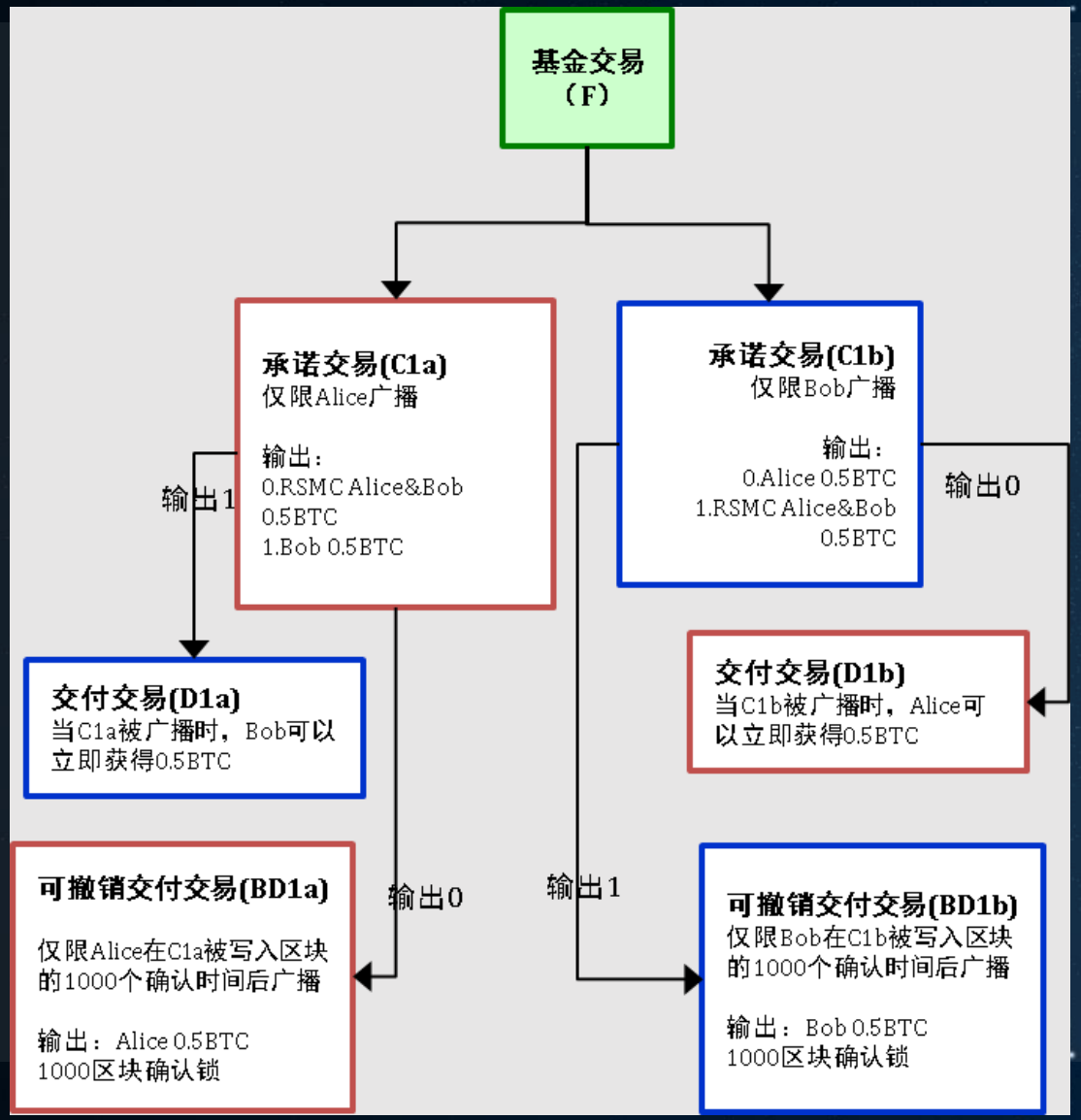
楔入式侧链技术(Pegged Sidechains)

闪电网络

- 通过建立交易方的微支付渠道（Micropayment Channels）网络，将小额交易带离比特币，从而促进比特币的交易吞吐量达到每秒百万笔。
  - 双向支付通道(Bidirectional Payment Channels)
  - 序列到期可撤销合约（Revocable Sequence Maturity Contract，RSMC)
  - 哈希时锁合约(Hashed Timelock Contract，HTLC)

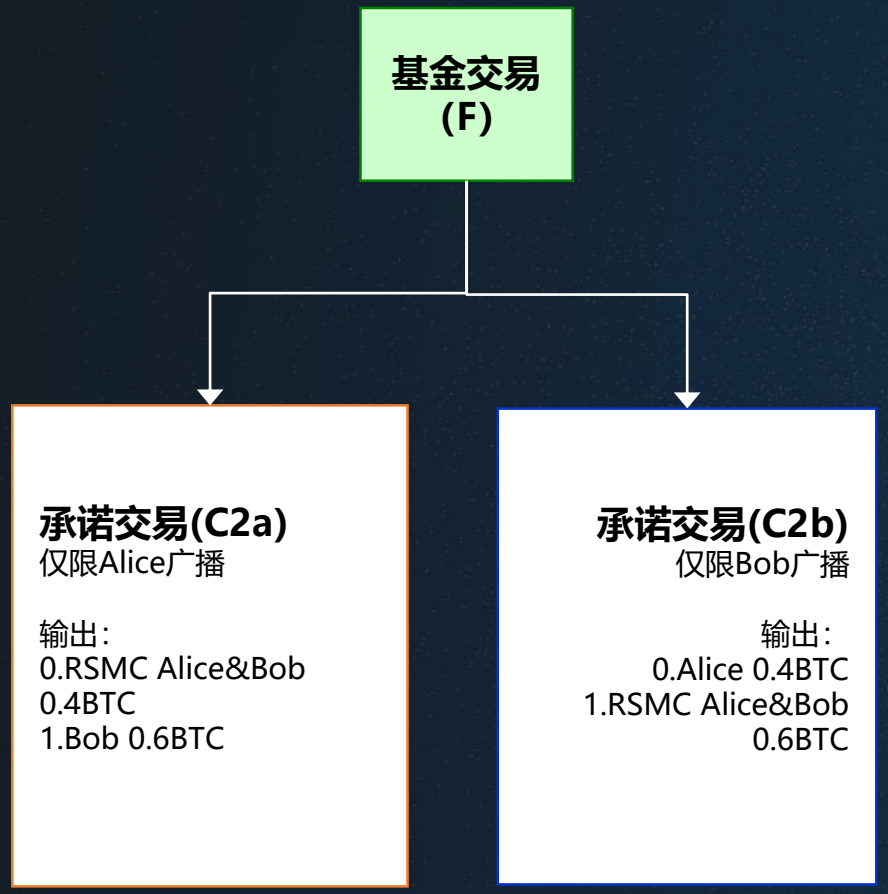
The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments (Joseph Poon and Tadge Dryja, 2015)

创建通道

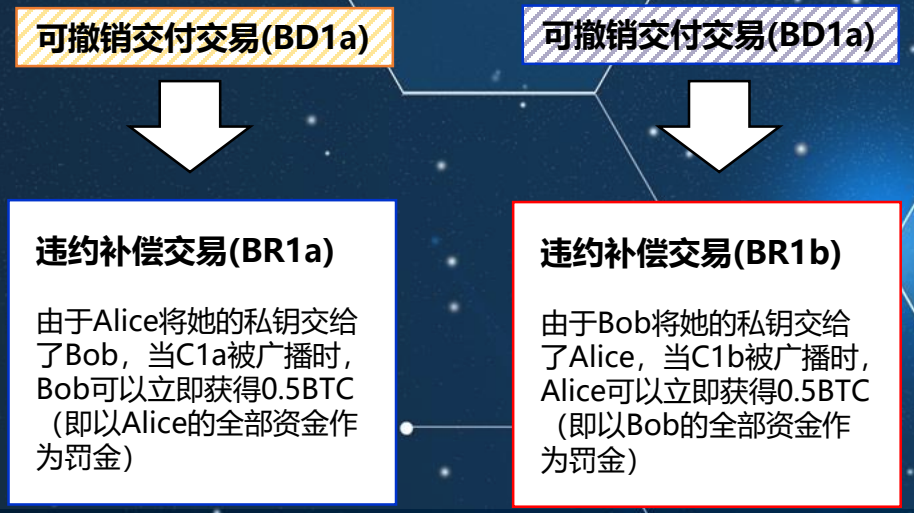


- Alice和Bob同意建立支付通道，双方各拿出0.5BTC用于创建基金交易(未签名)；
- Alice创建一笔初始的承诺交易C1b，该交易的输出为Alice:0.5BTC,Bob:0.5BTC，Alice对C1b签名后将该笔交易发送给Bob；
- Bob以同样的方式创建并签署C1a，并发送给Alice；
- 双方交换完毕后，就可以对基金交易进行签名，并在比特币系统中广播。

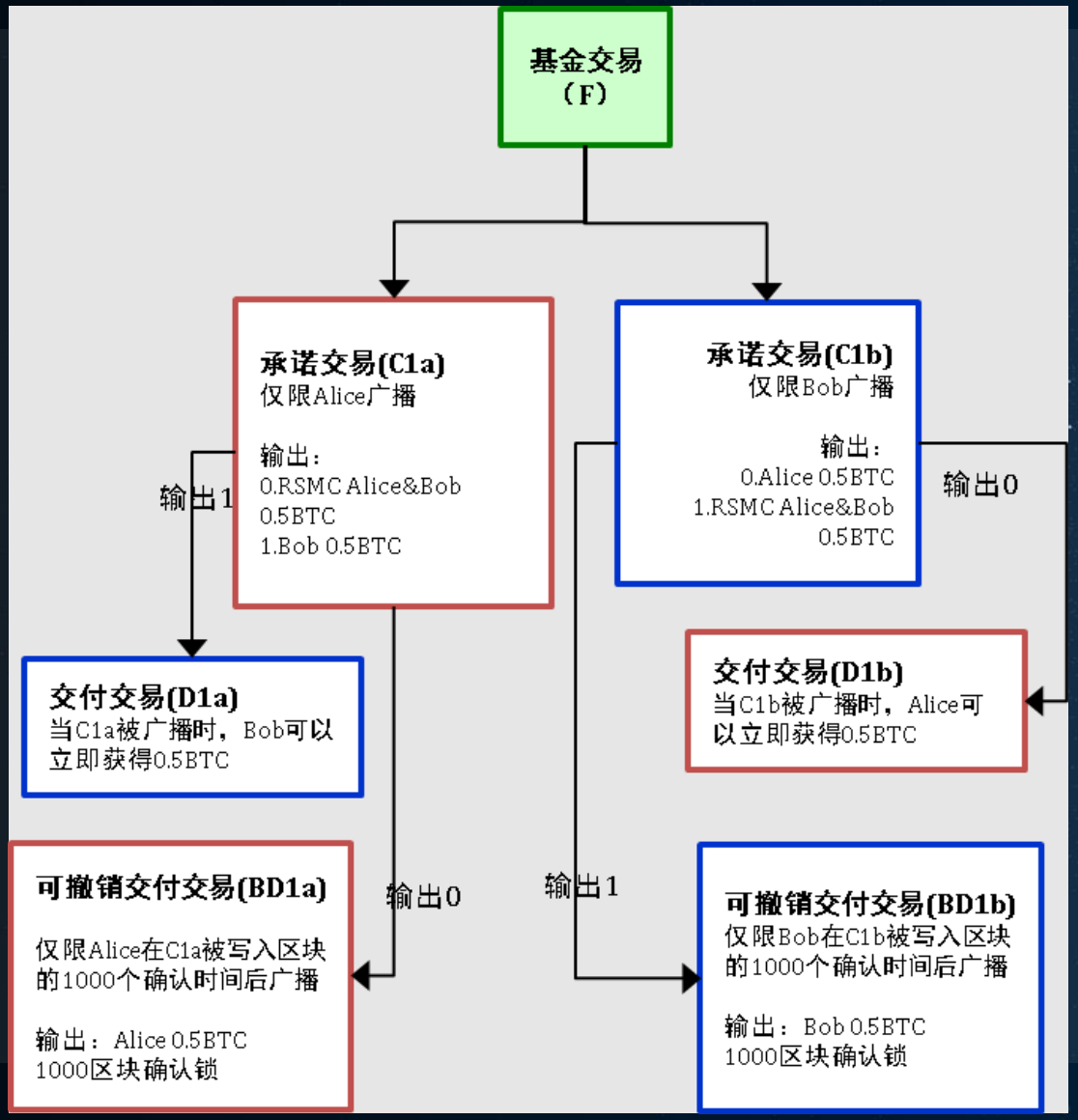
交易方式



- 双方可以通过生成新的承诺交易，并将旧的承诺交易作废，以达到资金重新分配的目的
- 为了让C1a和C1b失效，双方可以交换用于C1a和C1b签名的私钥，或者创建并交换违约补偿交易（Breach Remedy Transaction）BR1a/BR1b



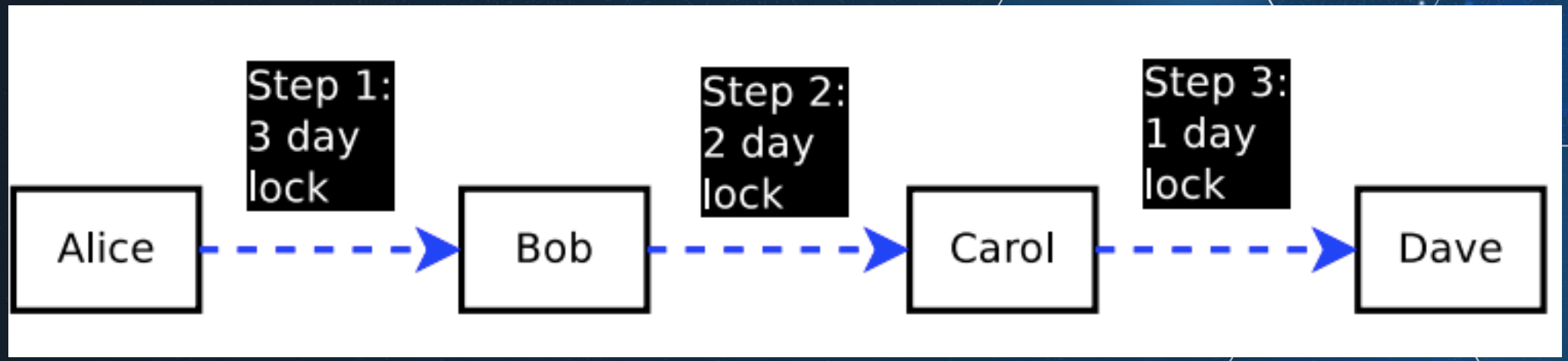
关闭通道



- 任意一方广播承诺交易，即可关闭支付通道；
- 序列到期可撤销合约（Revocable Sequence Maturity Contract，RSMC）：率先广播承诺交易的一方，需要等待一段时间才能拿到资金，而另一方则可以立即获得资金；
- 如果双方都同意关闭通道，可以创建一个结算交易（Exercise Settlement Transaction），经双方签名并广播后，双方都可以立即获得结算资金；
- 如果有一方广播的承诺交易不是最新版本，那么将受到惩罚，失去所拥有的资金，通道中的全部资金都将属于另一方

哈希时锁合约
(Hashed Timelock Contract，HTLC)

基于RSMC，闪电网络实现了节点之间的直接支付通道
基于HTLC，闪电网络实现了节点之间的间接支付通道。HTLC的目的是通过哈希运算允许跨多个节点的全局状态。具体而言，它可以锁定一项交易，并以一个约定的时间（未来某个区块的高度）和承诺披露的知识作为解锁条件。



并行扩容

闪电网络(Lightning Network)

雷电网络(Raiden Network)

Plasma

分片(Sharding)

楔入式侧链技术(Pegged Sidechains)

雷电网络

Update Transaction:

Sequence Number: This number is incremented with each new Update Transaction.

Net Transfer Amount: The amount of money to transfer from Party 1 to Party 2 (can be negative).

Hold Period: An amount of time (or number of blocks) to wait before closing the channel and transferring funds, after an Update Transaction has been posted.

Conditions:

1: Function(argument): Takes an argument and returns a number between 1 and 0.

Conditional Transfer Amount: Multiply this by the number returned by the Function and add it to the channel's Net Transfer Amount.

2: . . .

- 雷电网络（Raiden Network）是状态通道技术在以太坊上的实现。
- 当前版本：0.3.0
- Universal Payment Channels (Jehan Tremback and Zack Hess, 2015)

并行扩容

闪电网络(Lightning Network)

雷电网络(Raiden Network)

Plasma

分片(Sharding)

楔入式侧链技术(Pegged Sidechains)

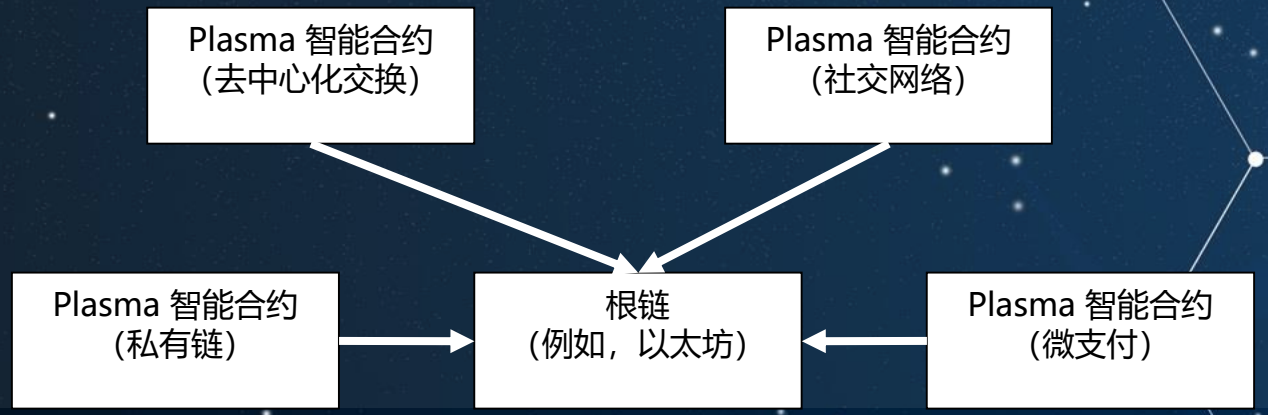
Plasma：可扩展的自主智能合约

- 一个可扩容的自主智能合约框架，能够将区块链的交易量提高至每秒十亿次左右；
- Plasma 可以扩展到更加复杂的计算（比如以太坊智能合约）之中，而不仅仅是闪电网络所能实现的链下支付；
- 创建依附于“主”（以太坊）区块链的“子”区块链；

Plasma: Scalable Autonomous Smart Contracts
(Joseph Poon and Vitalik Buterin, 2017)

基于Plasma智能合约的树状区块链

- 通过Plasma智能合约，区块链将被组织为树状层次结构，每个节点都是一个独立的区块链系统，拥有完整的区块链历史。
- 任何人都可以通过调用发布在根链上Plasma智能合约，来创建自定义的Plasma链，以实现多种用途，如去中心化交易、社交网络、私链、微支付等。其中，根链强制（enforce）Plasma链中的状态，同时它也是全局范围内所有计算的执行者，但实际上只有在收到欺诈证明的情况下才执行计算和处罚。Plasma链可以执行独立的计算，拥有独立的商业逻辑和智能合约条款



并行扩容

闪电网络(Lightning Network)

雷电网络(Raiden Network)

Plasma

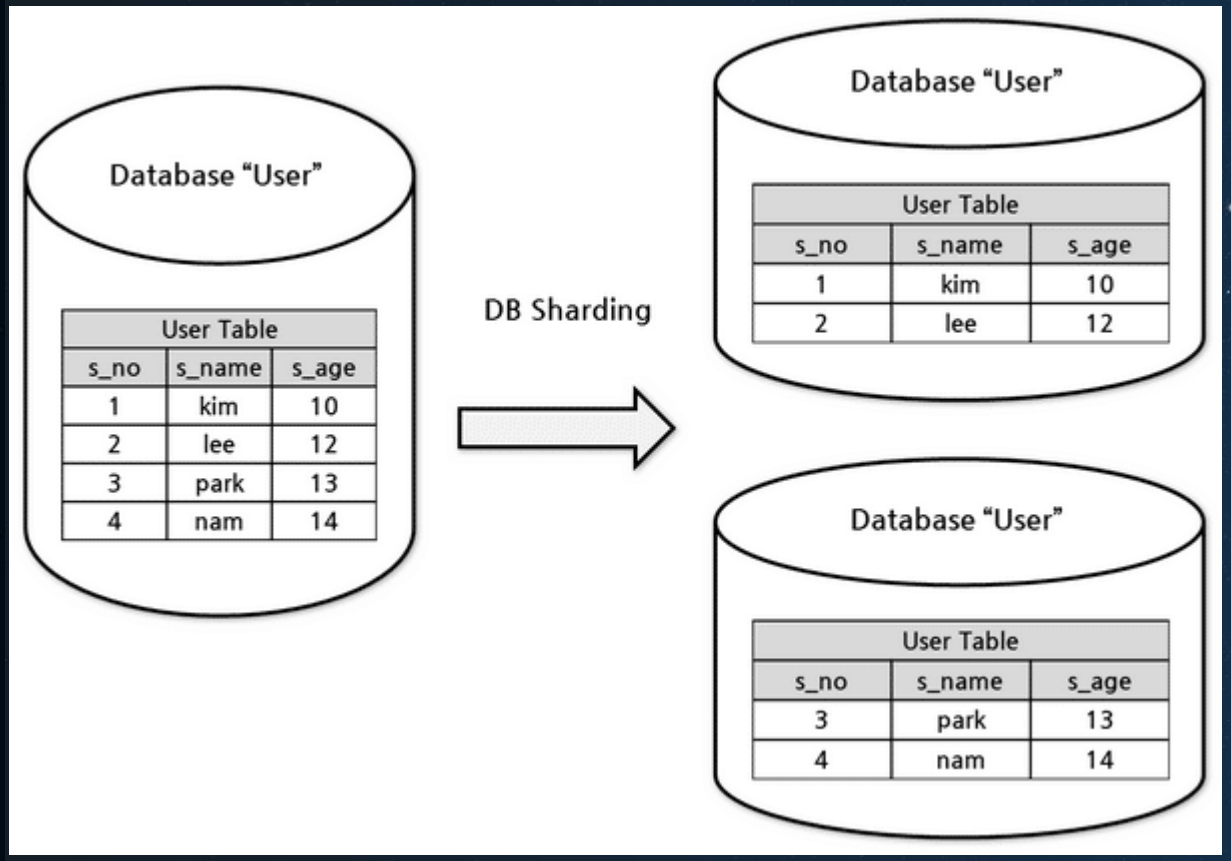
分片(Sharding)

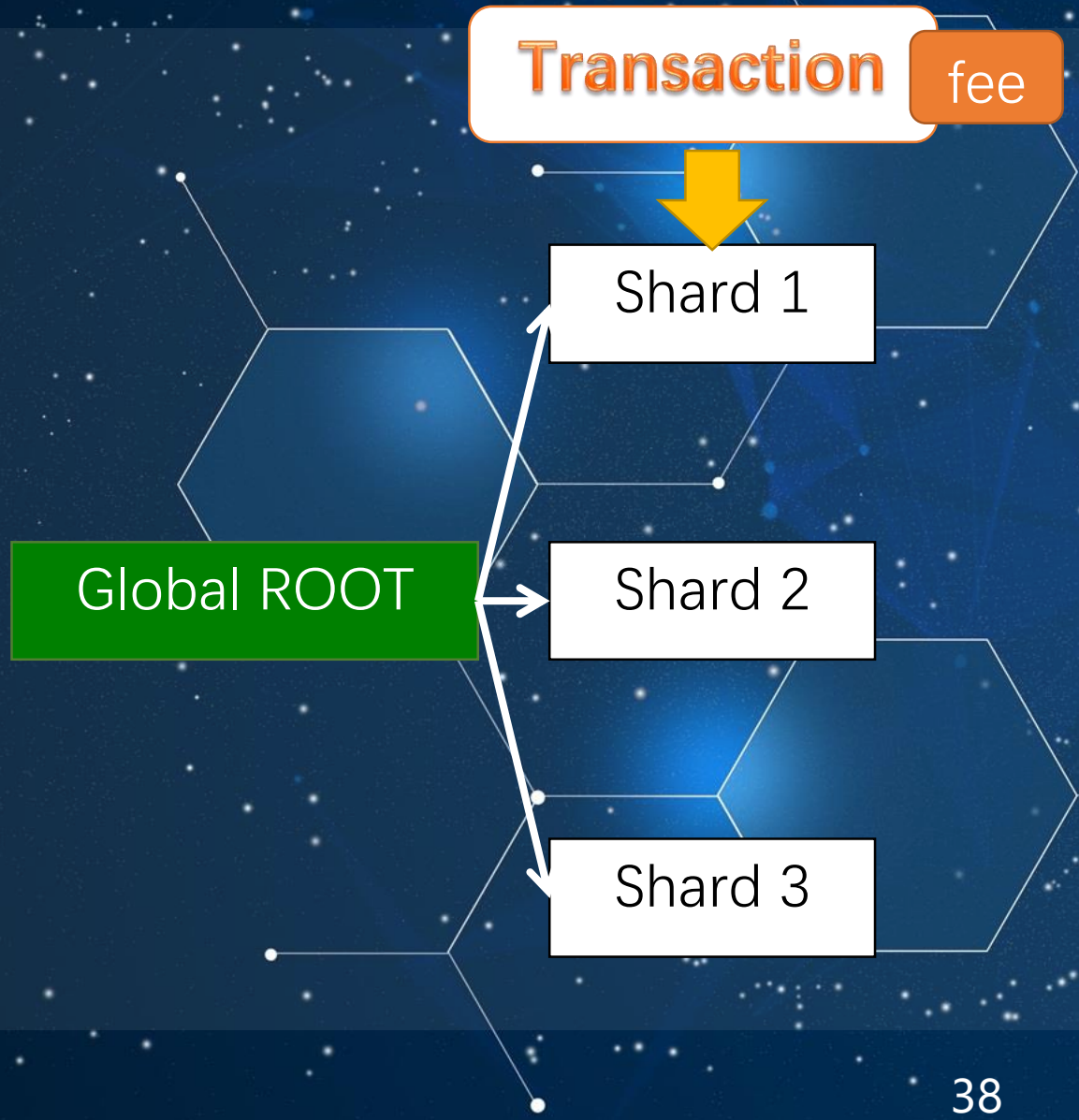
楔入式侧链技术(Pegged Sidechains)

分片/二次分片”（ Sharding/ Quadratic Sharding)

- 分片/二次分片(Sharding/ Quadratic Sharding)是以太坊创始人维塔利克·布特林(Vitali Buterin)为了解决以太坊网络扩容问题而设计的一种技术方案。
- 分片原本指种数据库扩展方案，它把数据库横向扩展到多个物理节点上，其目的是为了突破单节点数据库服务的I/O能力限制；而区块链的分片方案是将原来的单条区块链进行二次扩展，以突破单个节点的计算能力限制。

二次分片（quadratic sharding）





并行扩容

闪电网络(Lightning Network)

雷电网络(Raiden Network)

Plasma

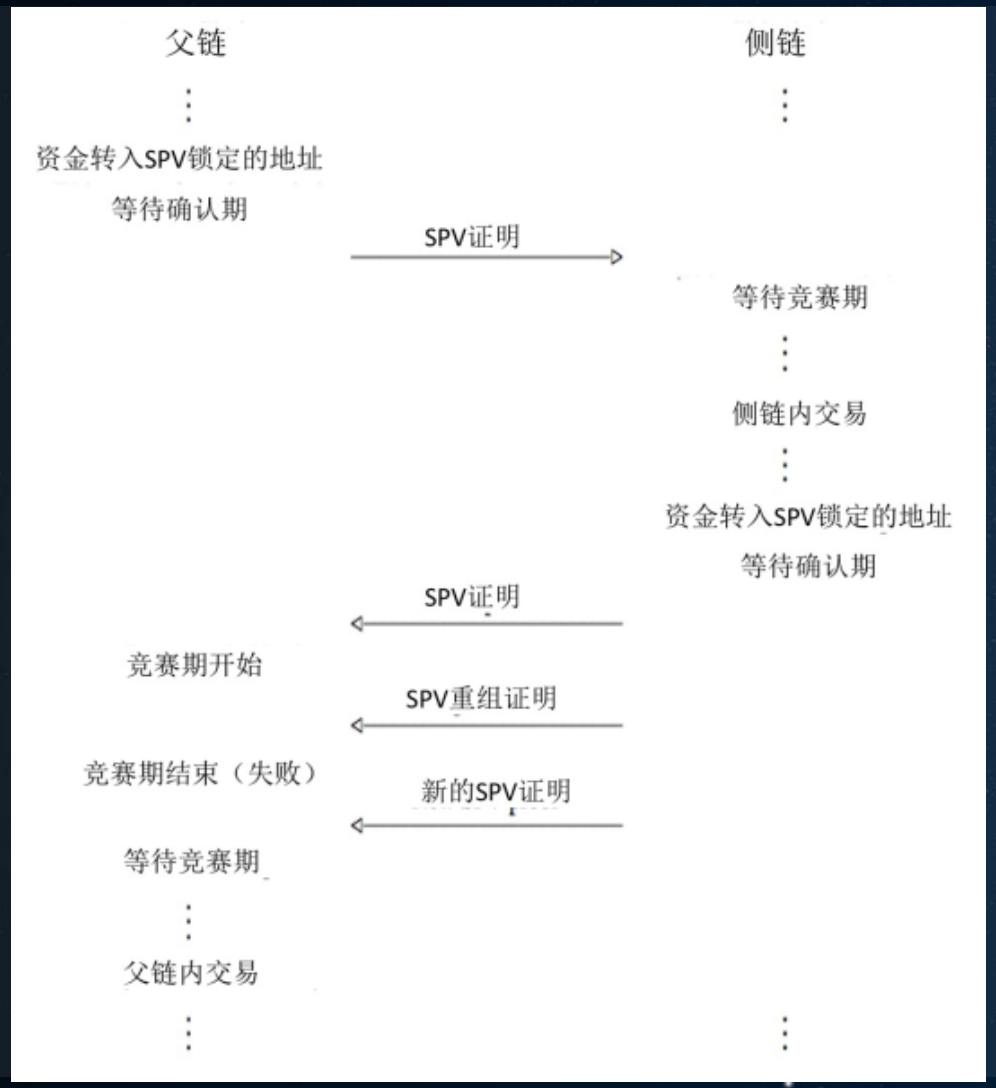
分片(Sharding)

楔入式侧链技术(Pegged Sidechains)

楔入式侧链技术(pegged sidechains)

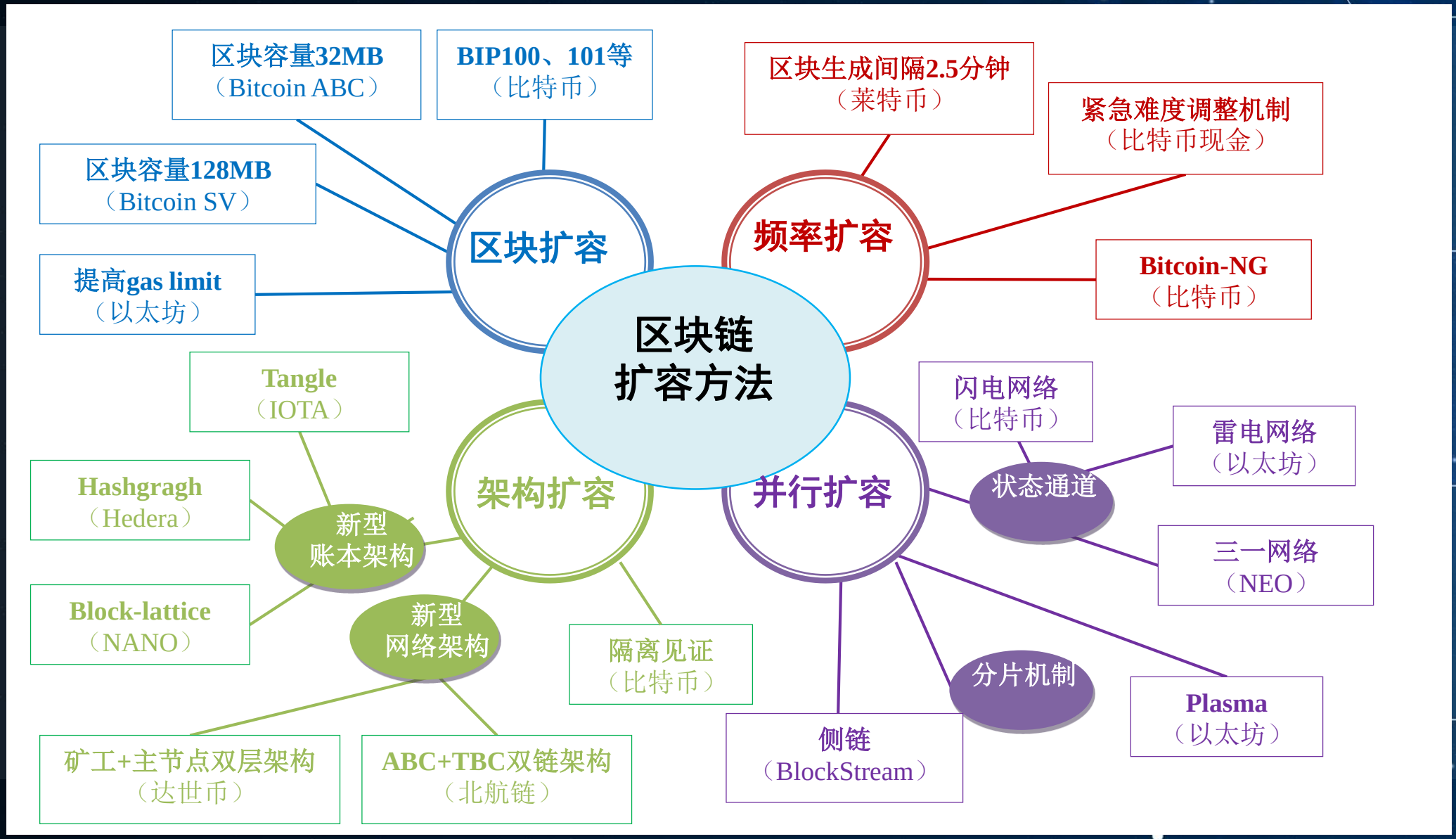
- 侧链是可以验证来自其他区块链数据（父链）的区块链；
- 侧链技术允许用户在父链之外的其他区块链上使用他们的资产；侧链虽然依赖于父链，然而侧链上的事务处理与父链完全独立；
- 其工作基础为简单支付验证（Simplified Payment Verification，SPV）证明，它是一种动态成员多方签名（Dynamic Membership Multi-party Signature，DMMS），用在基于工作量证明（Proof-Of-Work，POW）的区块链中（如比特币系统）。一个SPV证明包含：
  - （a）一个展示工作量证明的区块头(block headers)列表
  - （b）一个表明列表中的某一区块中存在某项输出的密码学证明。
- 基于SPV证明，无需运行全节点即可验证支付信息。

（BlockStream）



- 用户将这笔资金转到父链上的一个特殊输出，该输出只能由侧链上的SPV证明来解锁。
- 用户等待一个确认期后，在子链上创建一个引用该输出的交易，并提供该输出已被父链上足够工作量证明覆盖的SPV证明。
- 用户继续等待一个竞赛期，在此期间如果收到新的SPV证明，且比之前的SPV证明有更多工作量证明，那么将替代原来的SPV证明。
- 竞赛期结束后，用户就可以在侧链上自由使用这笔资金了。资金在侧链上依然保持自己“父链币”的身份，只能转回到相应的父链，并且侧链不允许来自不同父链的币之间进行交易或兑换。
- 当用户想把币从侧链上转回父链时，需要经历相同的过程：在子链上将这笔资金发送到一个特殊输出，产生一个SPV证明给父链，用于解锁父链上的等额资金

区块链扩容方法总结


区块链
扩容方法
区块扩容
区块容量32MB
（Bitcoin ABC）
BIP100、101等
（比特币）
区块容量128MB
（Bitcoin SV）
提高gas limit
（以太坊）
频率扩容
区块生成间隔2.5分钟
（莱特币）
紧急难度调整机制
（比特币现金）
Bitcoin-NG
（比特币）
架构扩容
Tangle
（IOTA）
Hashgragh
（Hedera）
新型
账本架构
Block-lattice
（NANO）
新型
网络架构
矿工+主节点双层架构
（达世币）
ABC+TBC双链架构
（北航链）
隔离见证
（比特币）
并行扩容
闪电网络
（比特币）
状态通道
雷电网络
（以太坊）
三一网络
（NEO）
分片机制
侧链
（BlockStream）
Plasma
（以太坊）

本章参考书

谢谢！