北京大学
PEKING UNIVERSITY

《区块链》课程

孙惠平
sunhp@ss.pku.edu.cn

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

北京大学
PEKING UNIVERSITY

PART 第八章

区块链性能

目 录

CONTENTS

第一节

性能问题分析

01 性能问题

02 系统模型

03 性能问题的产生原因

1.1性能问题

近年来，区块链技术得到了越越来越多的应用，主要表现在两个方面：

一是区块链技术逐渐涉及到了各行各业，其应用领域不断扩展。

二则是一些区块链应用的用户不断增长，单位时间内产生了更多的交易。

交易规模的增大可能导致各种挑战，而要保证区块链系统的可靠运行，就要求区块链系统具有足够的性能以应对这样大规模的交易处理。

1.1性能问题

在区块链领域，往往使用可扩展性（scalability）来概括一个系统的整体性能。
具体而言，可扩展性包括吞吐量、存储、交易时延、网络、甚至用户进行交易的费用等指标。

吞吐量

代表系统在单位时间内可处理的交易数目，直接反映了系统所支持的服务规模，决定了区块链系统在用户数量多、交易频繁状况下的表现好坏。

时延

反映用户交易从发布到确认的延迟，影响系统服务质量。当用户更多，发布的交易量更大时，平均的验证时延也会更长。

存储

及到系统节点对区块链数据和交易的存储开销，同时也影响了节点初始化加入系统的门槛。如果所有交易和区块都记录在链上，随着系统不断运行，区块链的存储开销会不断增大。

1.1性能问题

伴随区块链系统的应用，参与到系统中的节点数量上升，系统的规模也越发庞大。

当前比特币和以太坊等公链的记账节点规模都不高于1万，联盟链一般因为共识算法的影响记账节点规模一般不高于100。而现有的区块链性能指标逐渐显得不足：

吞吐量：比特币7tx/s，以太坊15tx/s

时延：比特币6*10=60分钟

存储：比特币超过300G

区块链系统现有性能的不足逐渐成为阻碍其进一步应用的障碍，这便是区块链系统的性能问题。

1.1性能问题

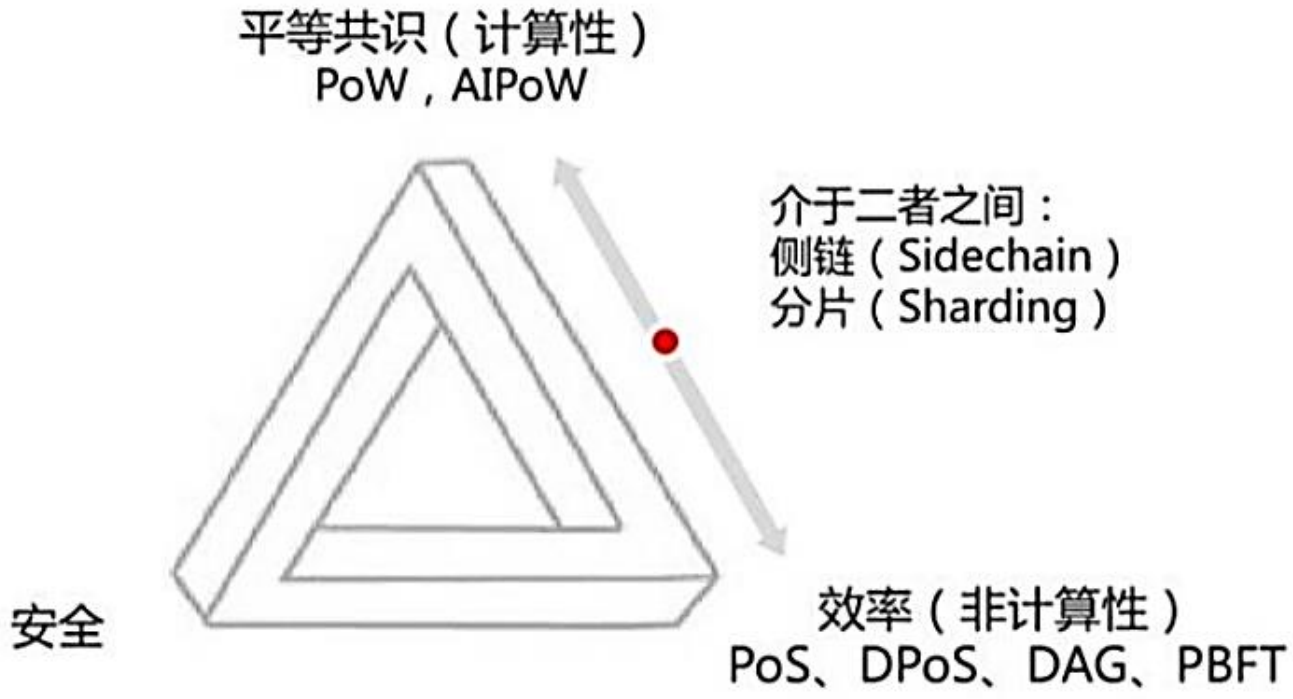
区块链扩容的不可能三角：

认为区块链不能同时在以下三个方面做到最好，满足其中两项往往意味着牺牲剩下的一项。

1、去中心化：共识的平等参与，无中心节点。

2、高效率：高吞吐量、低延迟等，是区块链性能扩展的目的。

3、安全：系统节点在运行中最终能对区块链状态保持一致。

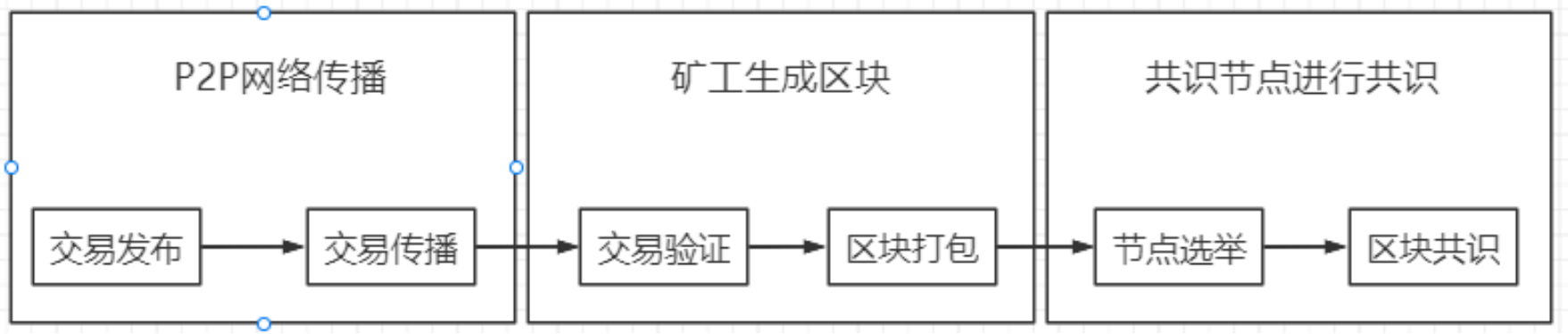


1.2系统模型

- **为了解释区块链系统的性能限制从何而来，我们简单建立区块链处理交易的系统模型，并回顾处理交易和生成区块的过程**

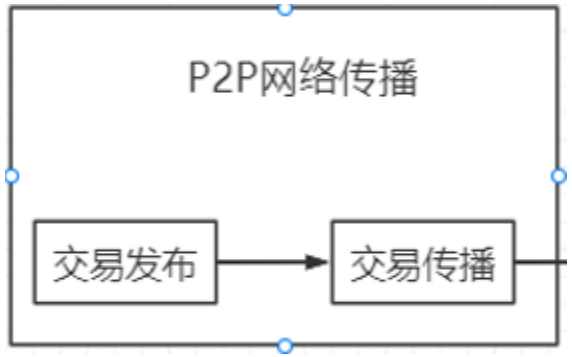
交易处理系统模型

当一个交易被发布到区块链网络，包括交易发布、传播、验证、区块打包和区块共识等过程将依次发生。



上述环节，又可以分为P2P网络传播，
矿工生成区块，以及公式节点进行共识
三个大步骤

1.3性能问题的产生原因

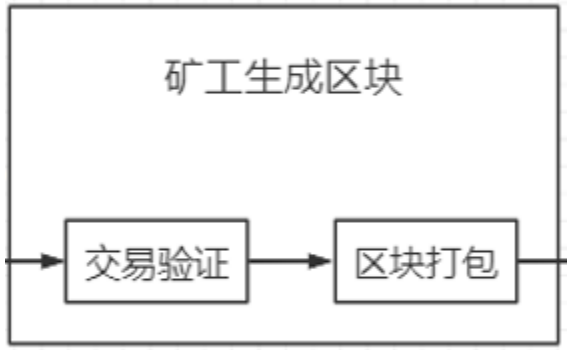


在交易传播的过程中，网络规模和采用的传播模型影响了消息传播的速度与网络开销的大小。

网络规模决定传播范围，大的传播范围使得传播过程更长。而传播模型决定了网络中消息传播的复杂度，消息太多（比如使用泛洪）则会增大网络传输压力。

一般来说，设计合适的子网络规模和传播模型可以有效降低交易传播的时延，同时将单个交易的网络压力降低能够使得更多交易在网络中传播，从而支持更大的吞吐量。

1.3性能问题的产生原因

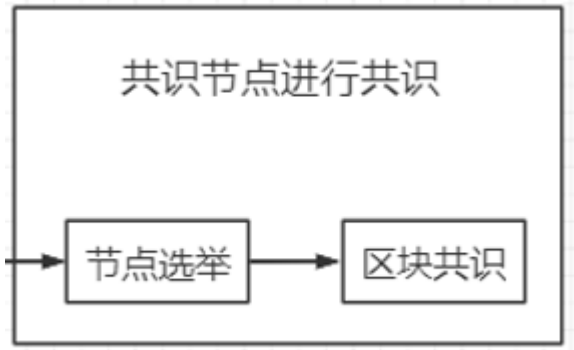


在矿工生成区块时，受限于节点的计算能力、存储能力和通信能力，当交易数量增多时，节点处理交易的压力也会增大，交易可能得不到及时的处理，进而导致交易堆积，严重增加处理时延。

区块是区块链系统中节点进行共识的基本单位，用以打包一段时间内的交易，区块的大小和结构决定了区块中包含交易的数量，在大小确定的情况下，应当优化区块结构，减少不必要的存储来容纳更多的交易。

区块链是区块通过哈希链接的方式构成的一条线性结构的链条，在此结构下为了减少分叉的发生，区块的生成频率受到了限制，这也限制了交易发布上链需要等待的平均时间。

1.3性能问题的产生原因



共识过程是区块链实现分布式一致性的核心环节，区块链系统的共识既要保证安全性，又要保障效率。共识过程对性能影响最大的环节包括节点选举和区块共识。

节点的选举过程决定了哪个节点（或哪一组节点）来生成区块，如PoW依赖算力竞争来决定哪个节点生成区块，算力竞争虽然保证了随机性和去中心化特性，却也导致了算力浪费和耗时过长的问题。

区块共识主要包含两个问题，

一是由哪些节点来参与共识。

二是如何对提出的区块形成一致性意见。

共识组的大小决定了共识网络规模，如果共识组太大，可能会减慢共识速度。共识算法决定了共识流程的复杂度和节点交换消息的数量，也决定了达成分布式一致性的代价和时间。

第 二 节

区块链性能扩展机制

01 性能扩展概述

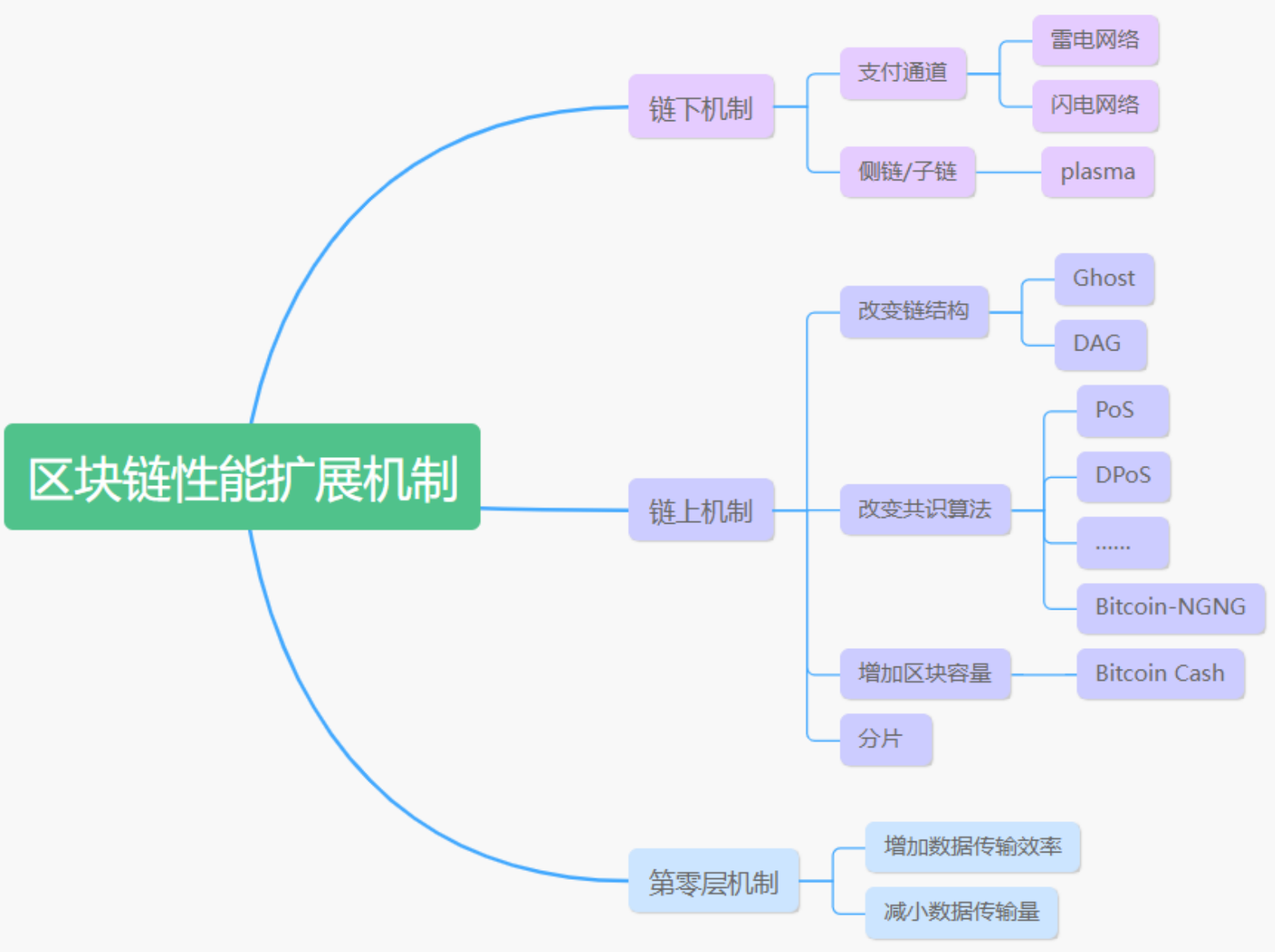
02 链下机制

03 链上机制

04 第零层机制

2.1性能扩展概述

现有的区块链性能扩展机制分为三层，即链下机制，链上机制，以及第零层机制



2.1性能扩展概述

北京大学 PEKING UNIVERSITY

链上机制

又称第一层机制，是修改现有区块链系统的结构、处理过程或其它设计参数以期提升系统性能的机制，例如增大区块容量、改变链的结构和共识以期提高出块效率，以及分片方案。

链下机制

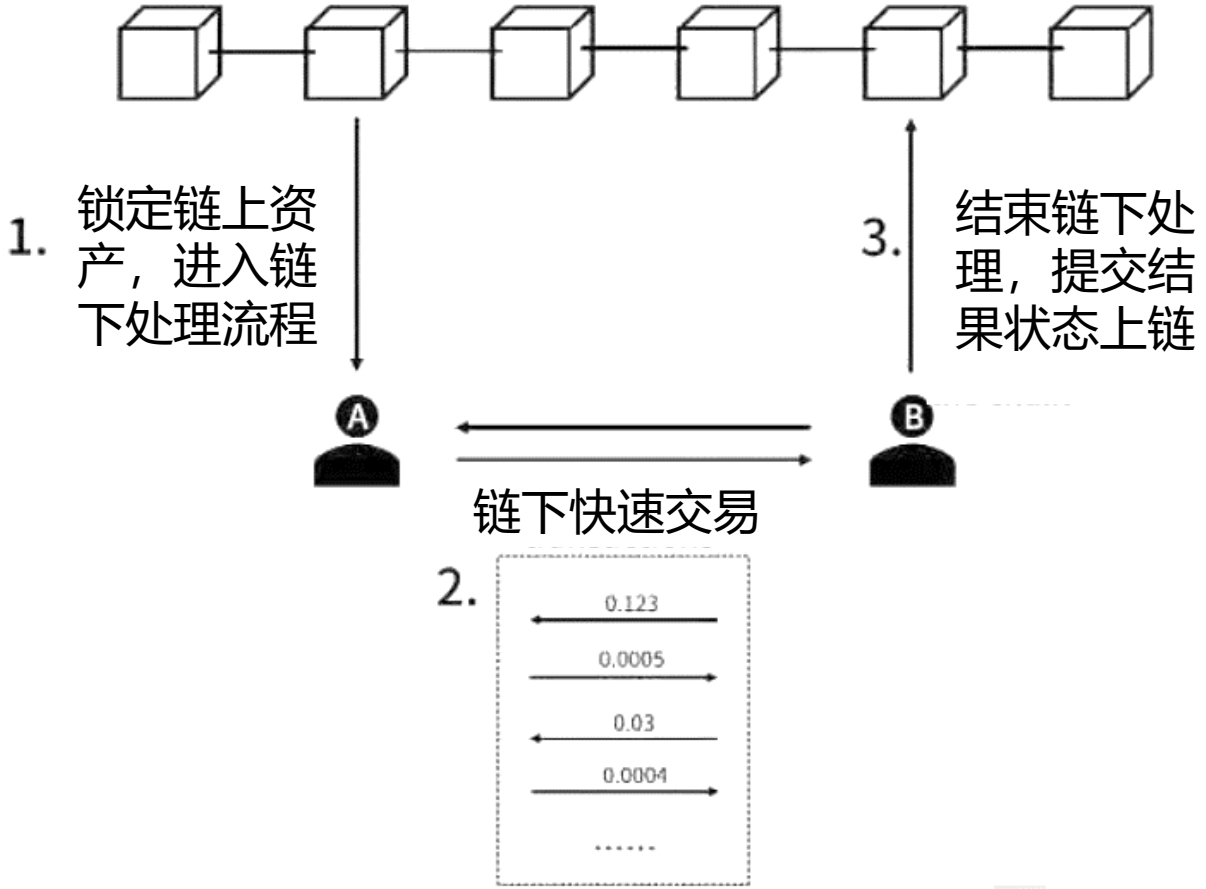
又称第二层机制，是指在保持区块链层本身不变的前提下，在区块链层之上运行其它机制来提升系统整体的性能。

第零层机制

运行在区块链之下，通过改善区块链底层诸如网络传播等的效率来提升区块链性能。

2.2链下机制

- **链下机制又称第二层机制，是指在保持区块链层本身不变的前提下，在区块链层之上运行其它机制来提升系统整体的性能。**

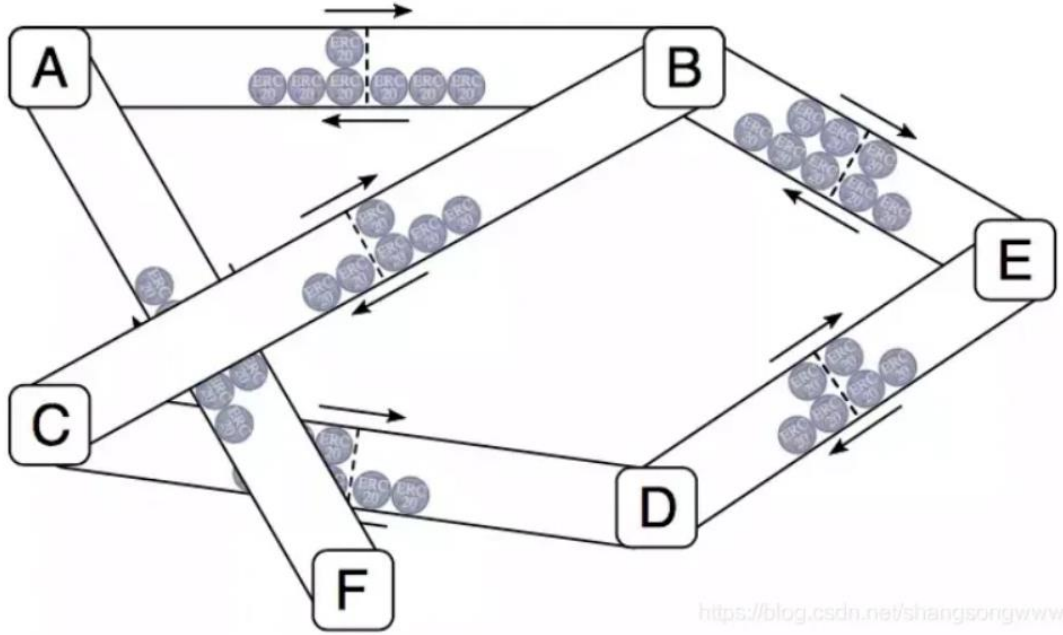


2.2链下机制

- **支付通道：**

支付通道

支付通道机制最有名的示例是闪电网络和雷电网络，如图所示。支付通道在用户之间创建了运行在区块链下的支付通道，该通道记录了参与者之间的资金池状态，资金池状态更新和参与者之间的交易处理都通过支付通道来完成。

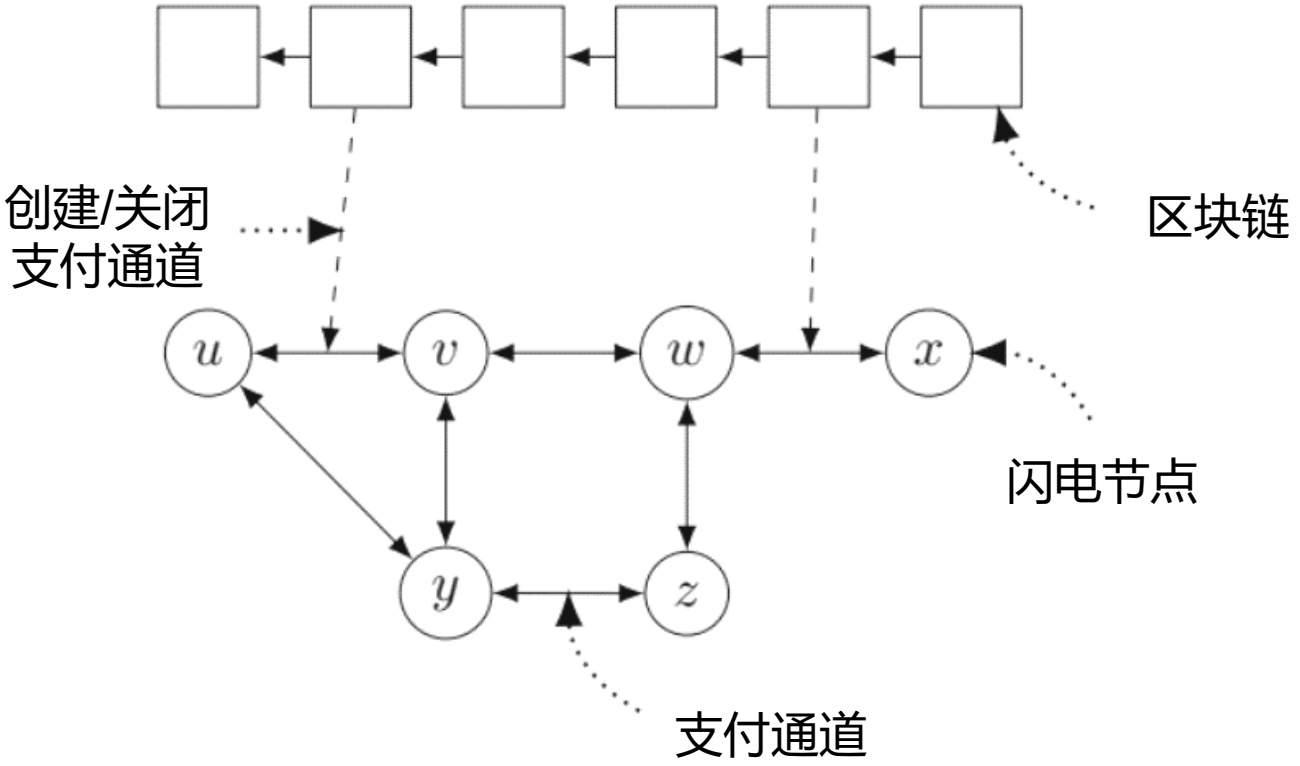


- **支付通道中，交易双方链下交易完成后的结果状态可以直接提交给区块链，无需矿工的参与，减少了时延。此外，交易双方通过支付通道进行的交易不需支付交易费，不会有区块确认时间，用户可以更高效地完成多个即时交易。**

北京大学 PEKING UNIVERSITY

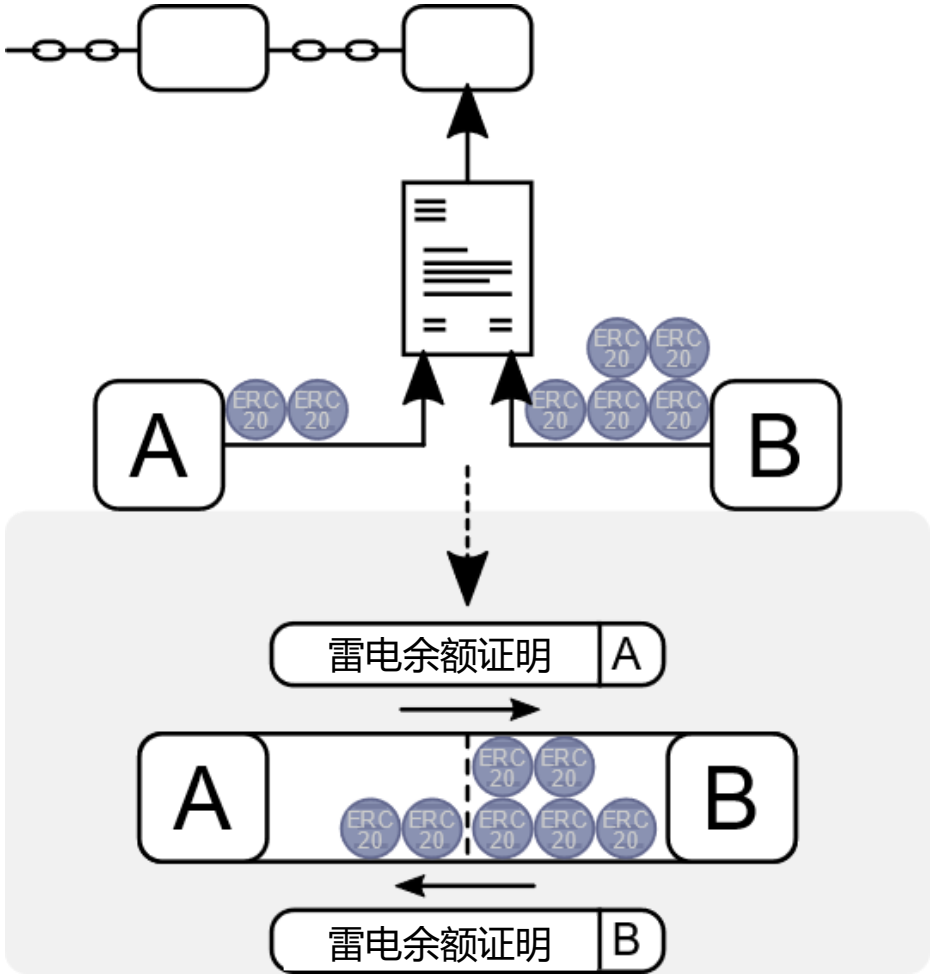
闪电网络

闪电网络中，支付通道通过HTLC（Hashed Timelock Contracts，一种哈希的带时钟的智能合约）来实现。智能合约（区块链脚本）可以在链下支付通道关闭后解锁交易双方部分锁定资产，更新双方的资产状态，保证交易的安全性。



雷电网络

雷电网络是一个针对以太坊区块链的链下性能扩展方案。雷电网络本质上是一个在支持智能合约的平台上更加通用的闪电网络。由于以太坊实现了图灵完备的脚本系统，可以实现更为灵活的智能合约，因此基于以太坊而设计的雷电网络在借鉴闪电网络模型的基础之上，对针对支付通道上作恶行为的惩罚机制进行了改造。



2.2链下机制

链下支付通道的方式也存在一些问题：

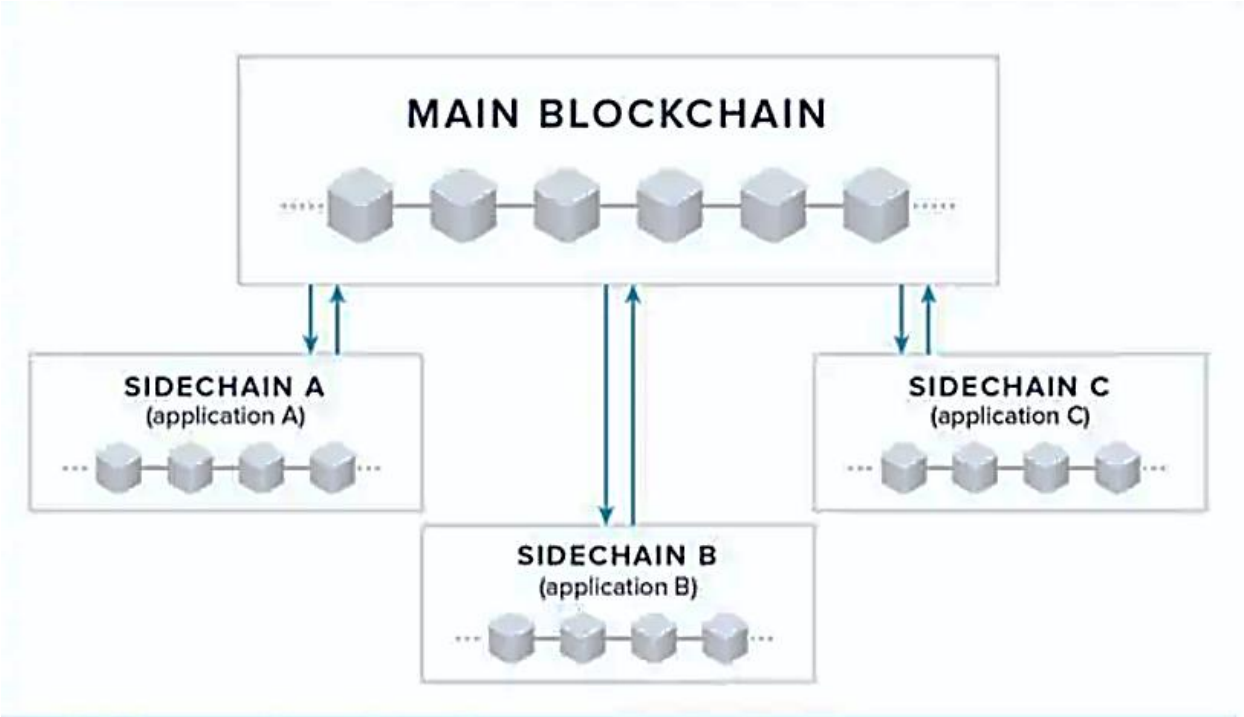
打开通道和关闭通道是两项链上交易，都将花费传统的主链交易时间，并不能实现实时的价值转移。在闪电网络中，通道的持续时间是固定的。因此，进行交易的双方之间会反复出现打开和关闭交易通道的问题。

打开通道和关闭通道需要交易费用，如在比特币网络上，每笔交易费用约30美元。链下支付通道适用于交易双方频繁小额支付的场景，应用场景并不是十分广泛。

此外，支付通道交易方案在交易双方没有直接支付通道时，允许中继节点作为服务提供者完成交易，中继节点能获取交易双方的交易信息，使得用户的隐私受到威胁。

2.2链下机制

- 侧链/子链机制：



侧链/子链机制

侧链可以实现数字资产在不同区块链之间的转移，如图所示。通过侧链技术，不同的区块链可以在保持独立的同时进行交互。通过把主链的部分交易转移到侧链上，利用侧链实现代替主链完成部分交易处理功能，减小主链的交易处理压力。

2.2链下机制

- **侧链/子链的一个例子是Plasma，它在实现资产转移功能的同时，保证了侧链中资产的安全性。**

- 当侧链安全性不足导致侧链被攻破或侧链停止服务时，即使主链仍然足够安全，用户也无法赎回主链上的资产，导致资产损失。
- Plasma确保了只要主链是安全的，转移到侧链上的资产就是安全的。在Plasma中侧链中的错误是可以检测到的，如果用户发现侧链的问题，用户可以安全地退出，资产不会受到损害。

2.3链上机制

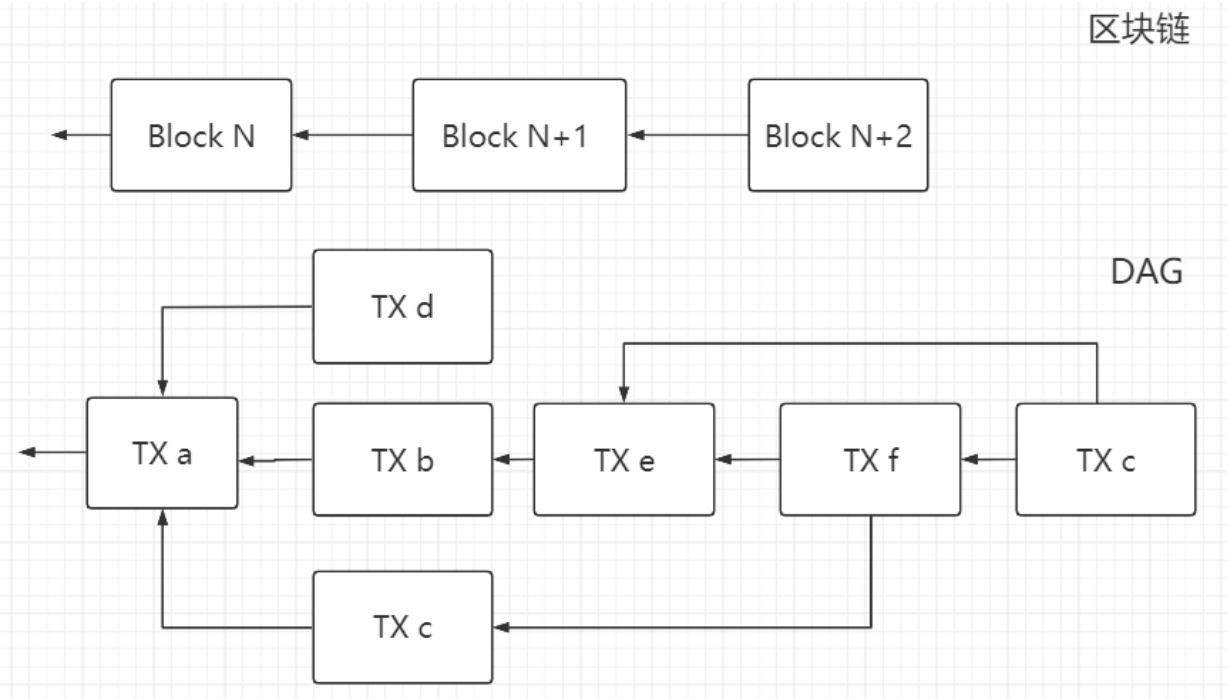
- **链上机制包括改变链结构、改变共识过程、增大区块容量、以及分片方案等，本节主要介绍前三类机制。区块链分片方案在多数分类中都被单独分为一类介绍，因此我们会在下一节中更详细介绍分片方案。**

2.3链上机制

- **改变链结构**

Ghost　　DAG

改变比特币的单链结构可以避免一些造成比特币性能下降的因素，例如分叉处理、交易验证依赖等。Ghost协议尝试解决提高区块生成频率所带来的分叉问题，其修改了接受最长链为有效区块链的规则，不仅接受每个共识周期发布最早的区块，而且接受未被大多数节点接受为最早发布的有效区块的孤立区块（在Ghost协议里称为“叔块”）。Ghost协议规定，当出现分叉时，节点选择累计子节点工作量最大的链条。



2.3链上机制

- **改变共识算法**

PoS

PoW的速度和开销都收到了很多诟病，而作为PoW的替代，很多其它共识算法以及共识过程被提出，其中一些能够更好避免PoW的低效之处，并同时保证一定的安全性。

PoS（Proof of Stake，权益证明）是作为PoW的替代技术提出的，避免使用大量算力挖矿的方法，意在解决PoW共识速度慢且耗费资源的问题。PoS系统中参与共识的节点必须具有系统中的一些权益，权益体现为节点对一定数量数字货币的所有权，如拥有数字货币的币龄或币天数。

用户如果要参与记账，需要抵押其数字货币权益。PoS根据节点在系统中持有的权益而非算力的大小获得记账权，权益越大，获得记账权的概率越大。PoS系统中，恶意破坏者会失去自己的权益。PoS在一定程度上解决了PoW机制能耗大的问题，缩短了区块的产生时间和确认时间，提高了系统的工作效率。

2.3链上机制

DPoS

DPoS（委托权益证明）是投票选出可信度较高的节点代表作为共识达成过程中的决策者,每个投票节点持有的票数由其所持有的数字货币的数量来决定。

与传统PoX机制（如PoW和PoS）不同，DPoS是协作系统，在该系统中，代表们协同工作以生成区块。尽管DPoS是部分集中的，但DPoS区块链能够比其他传统的公共区块链运行得更快。DPoS能耗低，区块生成频率也比较快。。

2.3链上机制

- 此外，还存在其它一些形式不同与POW和POS的共识算法，如PoA、PoET、以及Algorand等。

PoA

PoA（Proof of Authority，权限证明）是一种基于信誉的共识算法，被选中的节点负责验证区块链网络中的交易。这些节点类似于系统管理员，决定了区块链中的交易状态。

PoET

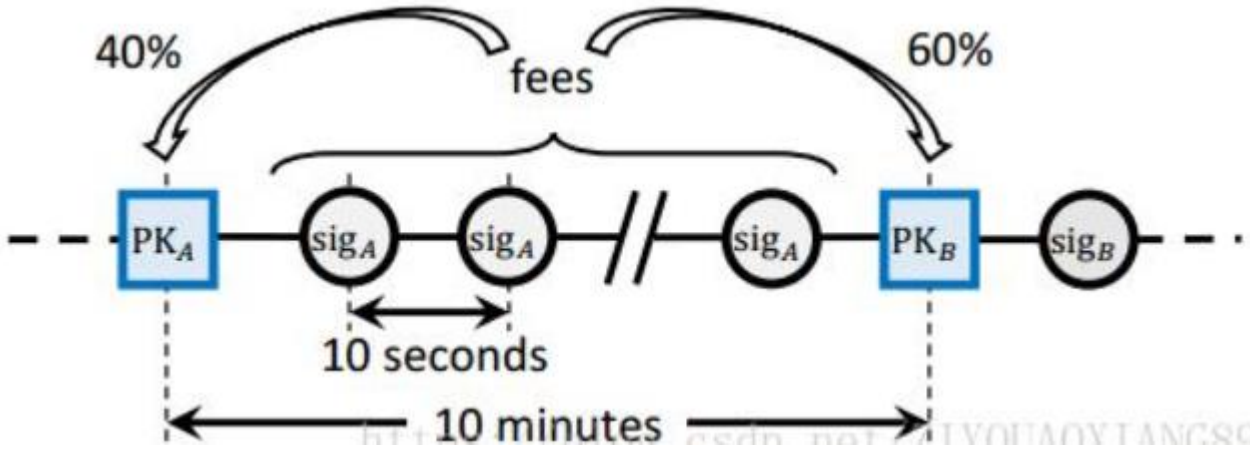
PoET（Proof of Elapsed time，流逝时间证明）是为改进PoW效率的基于可信环境的随机共识算法。其基本思想是网络中的每个参与节点都必须等待一个随机的等待时间，首个完成设定等待时间的节点将获得下一次记账权。

Algorand

Algorand是将PoS与BFT一类的传统分布式一致性算法结合的混合共识机制。在Algorand中，每一轮的共识节点是使用由VRF函数生成的可验证随机数，结合区块链节点账户的余额比例随机确定。共识节点运行BFT算法对新区块达成共识。

北京大学 PEKING UNIVERSITY

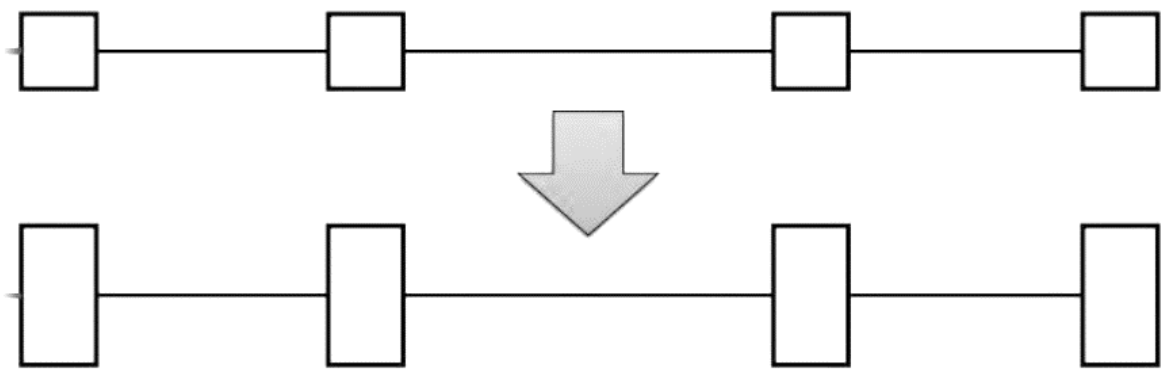
- 改变共识算法



Bitcoin-NG

除了完全改变共识，也可以将共识变为一轮节点选择+多轮区块发布的模式，例如Bitcoin-NG，它的基本思路是使选举记账节点的流程与交易验证打包形成区块的流程分开。此外，将时间切分成连续的时间段，每个时间段内，由一个竞争获得记账权的节点连续以较快速率打包交易，生成交易记录区块。

- 增大区块容量



增大区块容量

在区块链系统中，区块大小受到限制。在比特币中，区块大小为1MB。更大的区块可以容纳更多的交易。同等区块生成间隔下，增大区块大小可以提高区块链性能。例如，比特币现金（Bitcoin Cash）将区块大小限制从1MB增加到了8MB。

2.3链上机制

北京大学 PEKING UNIVERSITY

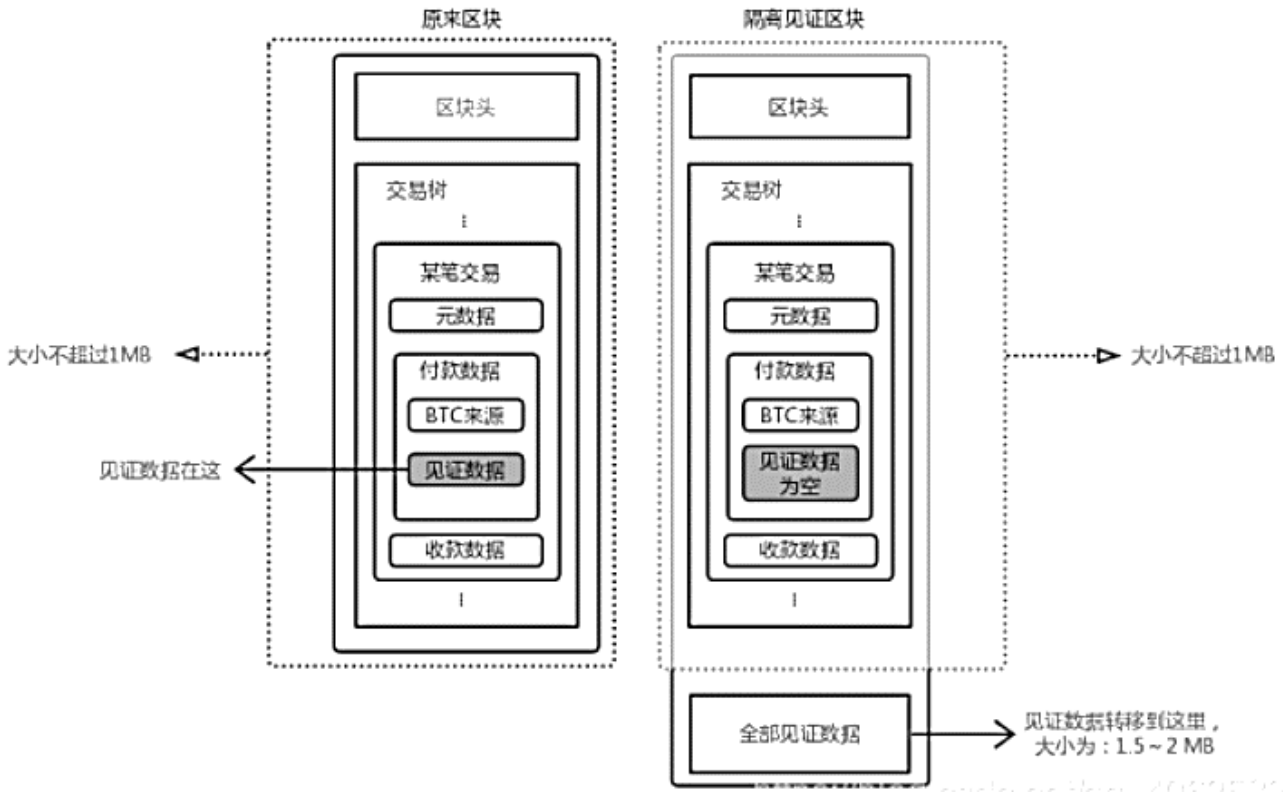
- **增大区块容量**

实践中，单纯增加区块大小的方式面临一些问题：更大的区块会增加区块的传播时间；包含更多的交易导致验证所需的时间也更长，这使得挖矿成功得到合法区块的节点在挖下一个区块时会获得先发优势，以此循环下去，拥有更多算力的矿工或者矿池就会更有优势，从而导致挖矿的集中化。

此外，增加区块大小会导致硬分叉，失去向后的兼容性。可见，这种性能扩展机制灵活性较低。

2.3链上机制

- 增大区块容量



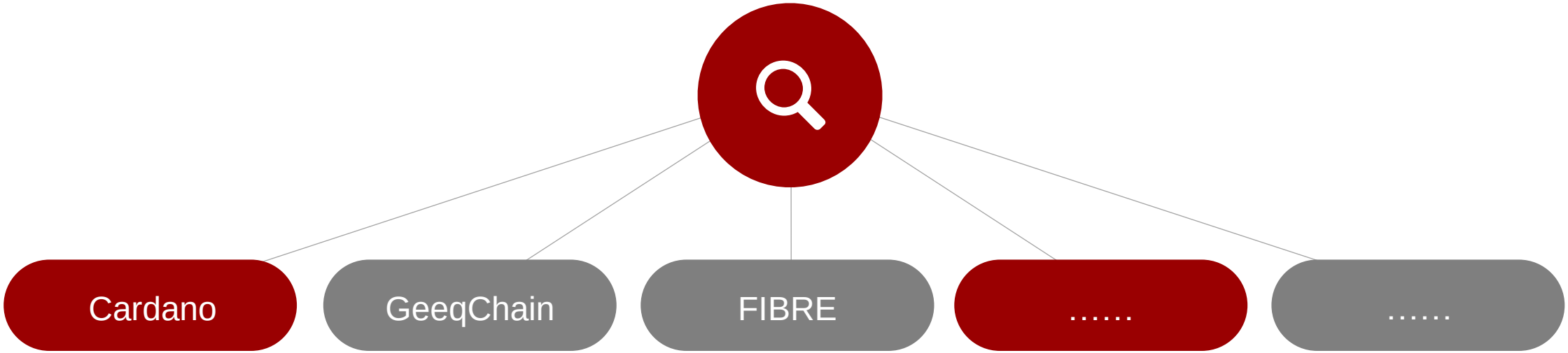
隔离见证

在区块链中，交易发起者提供的用以验证数字资产所有权和可用性的数字签名占整个交易存储空间的近70%。通过减小验证信息的占用空间，可以在区块中存储更多的交易，获得更好的吞吐量。隔离见证（Segwit）是比特币的一个升级，修改了比特币区块的存储结构。隔离见证的基本思路是删除每笔交易的签名(即交易见证)数据，释放区块中的存储空间，以便将更多交易存储在比特币的1MB的区块中，隔离出来的见证数据放到了区块末尾。隔离见证已经在莱特币中实现。

2.4第零层机制

北京大学 PEKING UNIVERSITY

- 第零层机制通过直接提升区块链底层要素的效率从而改进区块链性能，例如增加区块链通信效率和减小需要的传输量。增加传输效率主要在于改善底层网络的拓扑结构，设计更好的区块链交易中继网络，加速了交易在底层网络中的传播速度，减小了交易的网络开销。



2.4第零层机制

北京大学 PEKING UNIVERSITY

- 第零层机制的另一个例子是区块压缩。区块压缩的思想是减少区块中所包含的已经存储在验证节点交易池中的冗余数据，如Compact block relay和Txilm。

Compact block relay

Compact block relay改变了比特币中原始区块的结构，仅包含区块头和一些短的TXID（交易ID），这些TXID将用于匹配已经存在于验证者交易池中的交易。

Txilm

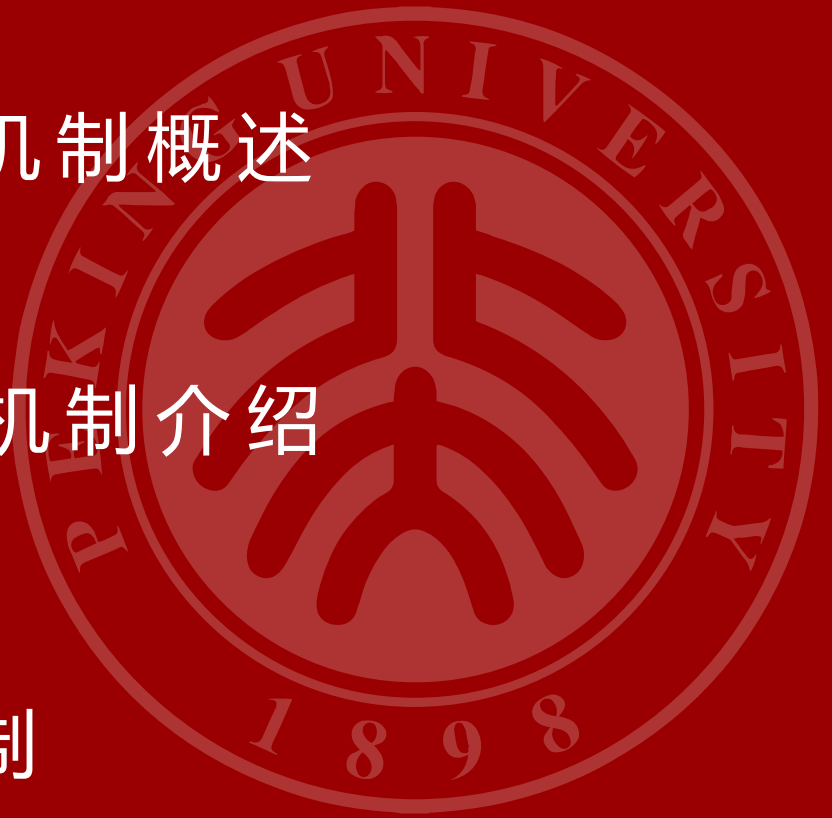
Txilm是基于Compact block relay的协议，该协议利用TXID的短哈希表示交易，但是使用短哈希时可能会发生哈希碰撞。因此， 利用Txilm协议计算TXID的哈希值时，结合规范交易排序的规则（如CTOR算法）来优化该协议以降低哈希冲突的可能性，并通过“哈希加盐”（如添加CRC32- Merkle根）来防止系统受到碰撞攻击。基于Txilm，在模拟实验中实现了80倍的数据缩减，从而提高了区块链的吞吐量。

第 三 节
分片机制

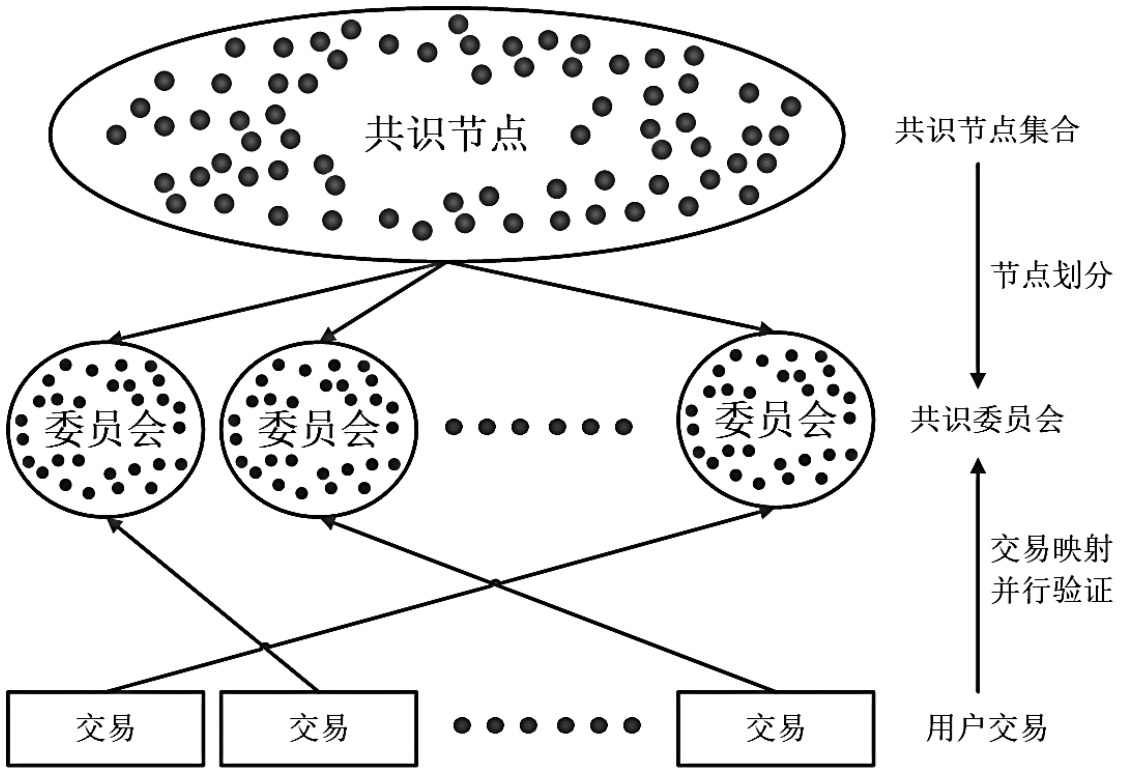
01 区块链分片机制概述

02 区块链分片机制介绍

03 重叠分片机制



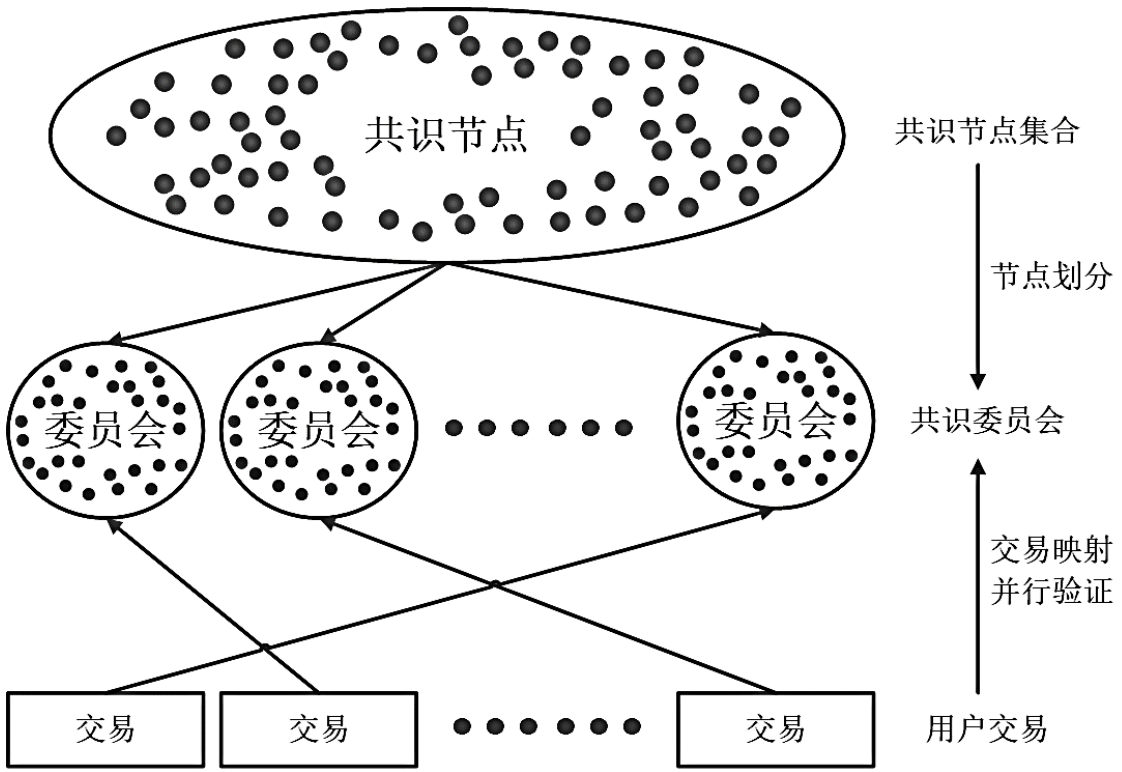
3.1区块链分片机制概述



分片技术

- 分片技术源于传统的数据库领域，在数据库分片中，数据的不同部分由不同服务器分别存储，增加访问的并行性。当数据库的数据量庞大导致单一数据库存储压力过大，响应请求能力会不足。在对不同数据表进行切分后，数据库将不同的逻辑分片映射到相应的物理节点之上

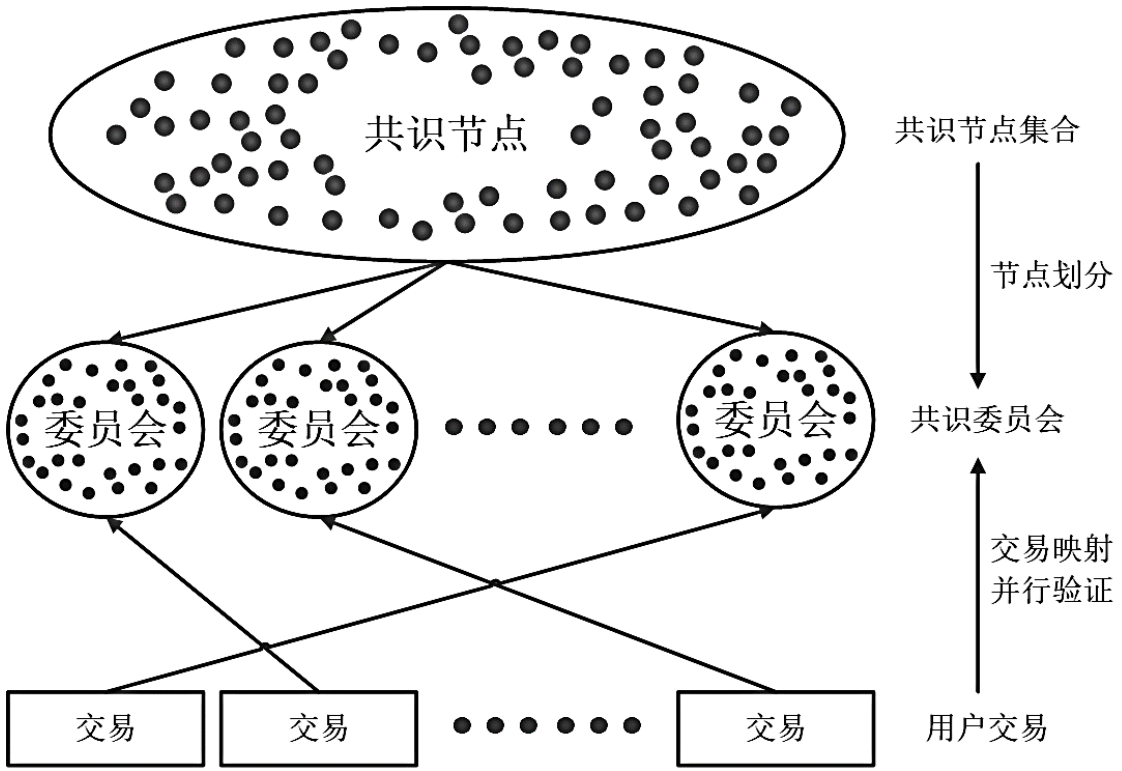
3.1区块链分片机制概述



分片技术

- 区块链本质上是一种数据库，而区块链系统不仅需要实现交易的存储功能，还需要实现交易的验证处理。因此区块链中分片技术更加接近分布式系统领域的并行任务概念。在区块链的分片模型中，交易的验证节点被分为很多组，每组使用相同的交易验证流程，以验证处理不相交的交易数据。

3.1区块链分片机制概述

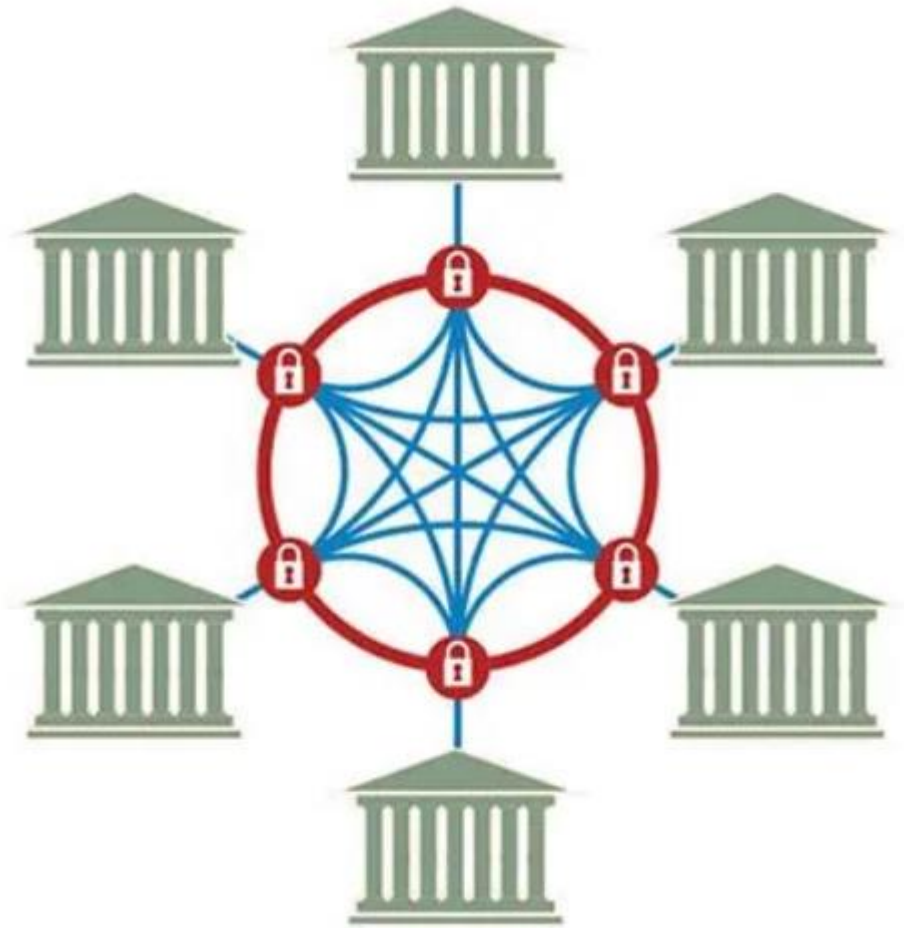


分片技术

- 在区块链分片系统中，分片技术的核心是将系统的矿工分为不同的验证委员会(committee)。当网络中发生交易时，每个交易根据某种原则被映射到确定的委员会进行处理。每一个委员会只负责处理系统全部交易的一部分。各个委员会可以并发地处理各自负责的交易，系统整体的交易处理吞吐量因而得到提升，理想情况下分片带来的性能提升的倍数接近于划分得到的矿工验证委员会的数量。

3.2区块链分片机制介绍

- RSCoin

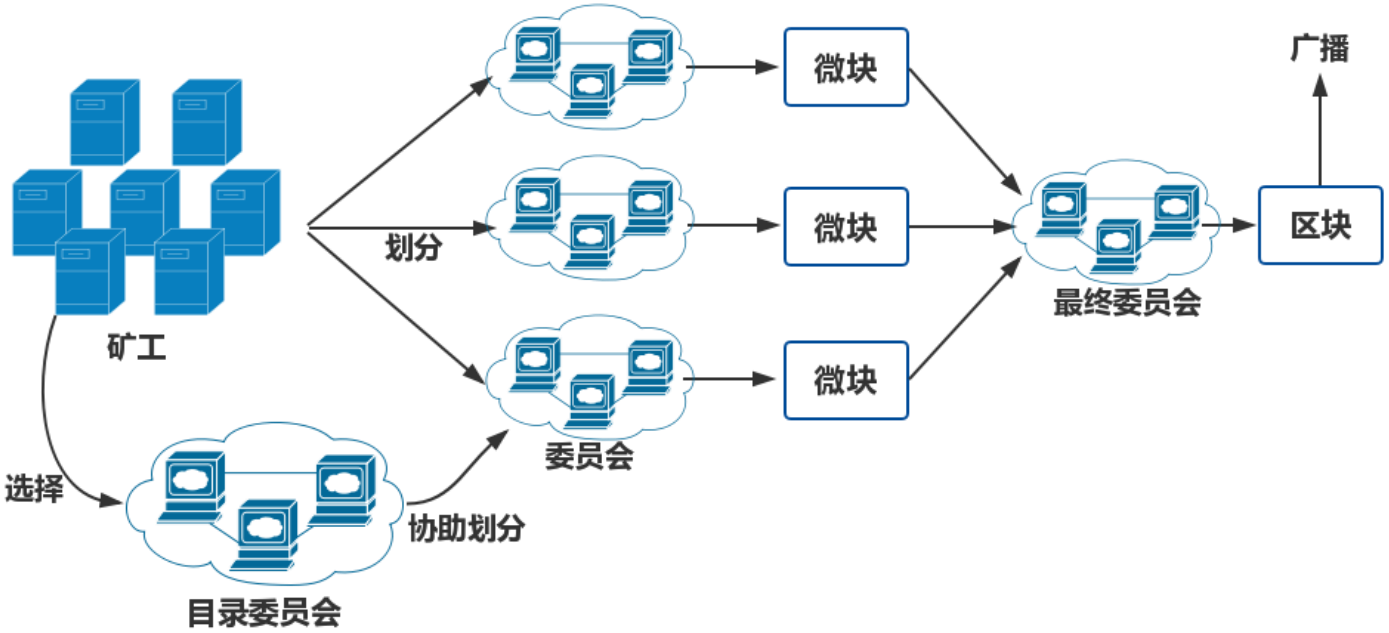


RSCoin

RSCoin是利用中心化的系统减少共识开销，从而增大吞吐量的分片方案。该方案提出，如果有可追责的中央机构保证验证节点诚实可信，就能通过减少共识开销大幅提升系统性能。RSCoin中提出了一个具有分片特征的系统，具有中心化代币来源，即中央银行系统提供的代币。中央银行给每个认定的下属机构公钥进行签名，由这些下属机构验证交易，由中央银行生成代币。按照哈希将不同的交易分配到不同下属机构中验证，在采用并行方案提升处理效率的基础上，由于不需要复杂的共识（具有可信节点），处理的吞吐量更大。

3.2区块链分片机制介绍

- ELASTICO



ELASTICO

在保证去中心化的公共区块链中，ELASTICO模型是较早提出的一种分片方案，该模型讨论了面向开放身份形成共识，并且可以防止女巫攻击的方法。模型考虑到恶意节点的存在，为了使得每个委员会恶意节点比例接近，防止任何单一委员会内恶意节点过多，需要尽可能对片划分均衡随机。为了应对适应性的对手不断尝试获取对单一片的控制，系统还需要频繁重新对节点进行分组。系统吞吐量随计算能力增长的效果十分明显，但吞吐量提升需要付出相应的安全代价，ELASTICO仅能抵御至多相当于系统1/4算力的恶意攻击。

3.2区块链分片机制介绍

北京大学 PEKING UNIVERSITY

- **ELASTICO**

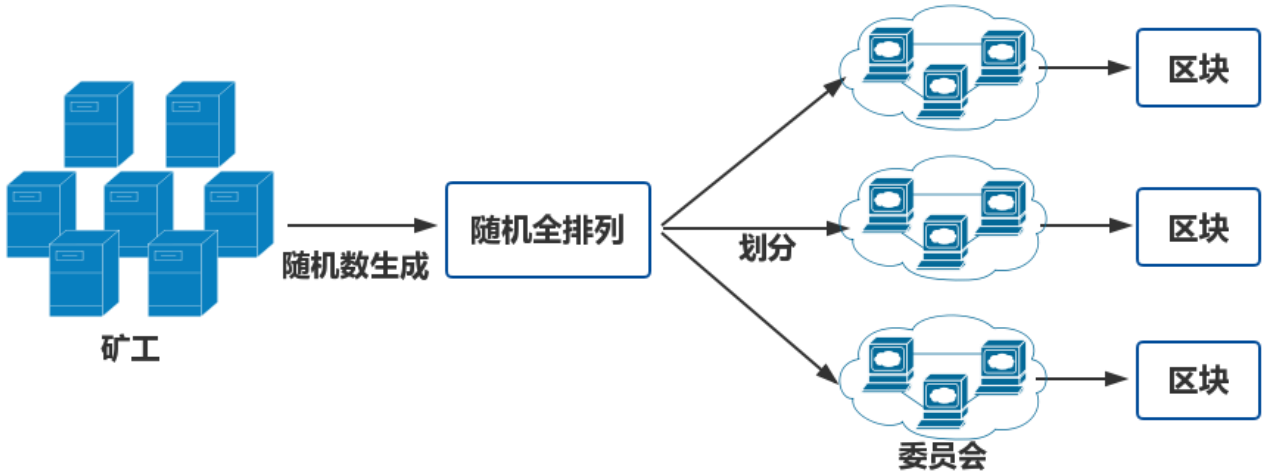
作为分片思想的早期实践，ELASTICO的优点是吞吐量得到显著提升，且共识结果具有强一致性。

但该模型还有很多不完善之处，使之难以立刻部署：

如第一轮委员会形成时的随机数没有明确界定，没有明确规定每个交易由哪些片处理，因此对交易冲突、双花攻击等都没有具体抵抗措施。在分片的方案最初被提出时，还没有应用存储的分片。存储压力的增长没有被改善，存储时每个节点都保存整个区块链的全部数据，参与记账的都是全量节点。因此ELASTICO并不能缓解矿工节点的存储压力。但即便如此，作为一种分片方案，这个模型仍然十分具有启发性。

3.2区块链分片机制介绍

- **OmniLedger**



OmniLedger

OmniLedger是一种主流的区块链分片方案，它的吞吐量可以接近甚至超过VISA系统（实验达到每秒6000次交易），而且一个典型的交易延迟在2秒以下。OminiLedger的分片层次包括了节点分片、交易分片和存储分片。该方案通过每个委员会维护UTXO池来记录当前系统状态。OminiLedger使用基于VRF的领导节点选择算法(VRF-based leader election algorithm)来选出领导节点。选择领导节点后通过RandHound算法生成随机数，并根据随机数生成一个随机全排列，用以划分每一个节点属于哪个委员会。

3.2区块链分片机制介绍

北京大学 PEKING UNIVERSITY

- **OmniLedger**

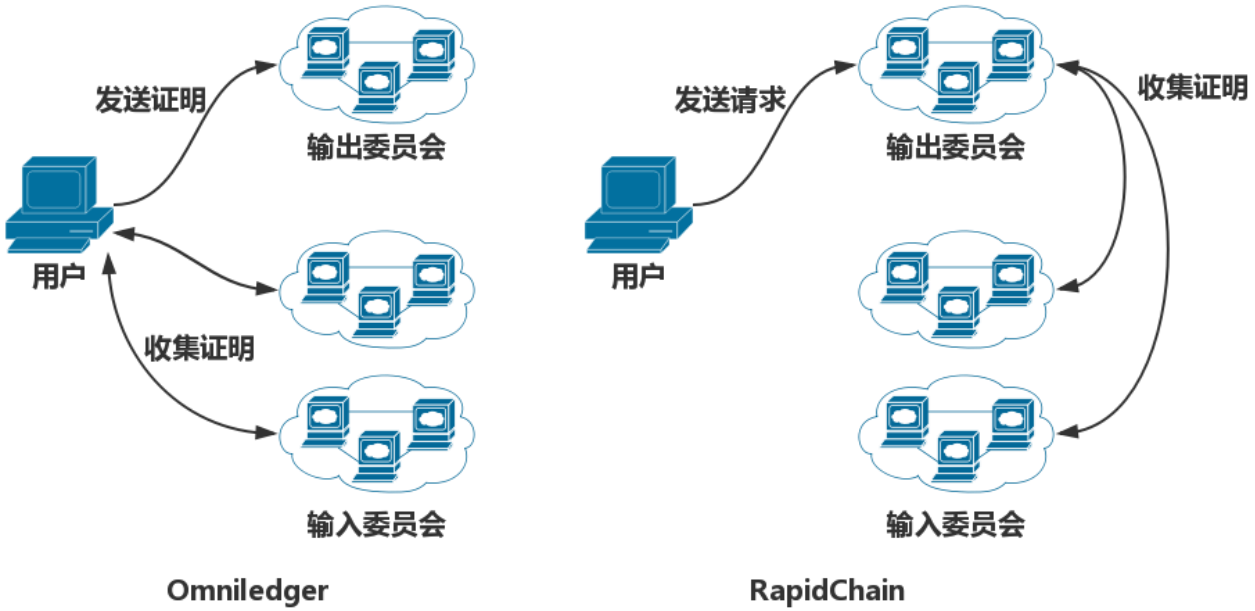
OmniLedger对系统定义明确，行为清晰，相比ELASTICO更加适于实际部署。且其委员会大小固定，节点和交易的分片过程都有良好定义。

相对于ELASTICO，OmniLedger使用存储分片，使每个委员会内的节点只存储委员会负责的一部分数据，减小了节点的存储压力。

然而，OmniLedger仍然具有一些有待改进之处。系统的共识依赖于委员会的领导节点。当交易涉及不同的委员会时(如需要的历史交易存储在多个委员会中)，用户需要向多个委员会发送请求信息，增大了网络开销。当委员会的成员重组时，由于存储内容不同，需要进行内容交换，时间和带宽开销很大。

3.2区块链分片机制介绍

- RapidChain



RapidChain

RapidChain相比OmniLedger在一些方面更加完善，其吞吐量据称超过每秒7300笔交易。它能够抵御具有1/3系统算力的恶意节点攻击，相比ELASTICO在安全性上有所提升。RapidChain的通信、计算和存储实现完全的分片，每个节点只需要存储整个区块链的一部分数据量即可维持系统正常工作。

RapidChain完全进行了共识和存储两个方面的分片，最大限度提升了吞吐率和减小存储开销。同时该系统每次只更新委员会中的少量成员，保证了更新时的服务能力。

3.2区块链分片机制介绍

北京大学 PEKING UNIVERSITY

- **RapidChain**

在OmniLedger部分的最后提到，跨片交易会大大增加网络开销，降低系统整体性能。

而在RapidChain中尝试解决了这一问题。在RapidChain中，用户只需要将交易发送给一些矿工，由矿工代理收集各委员会认证。

由于涉及到多个委员会的交易验证加大网络开销，RapidChain引入了打包传输的特性，即委员会间的验证信息交流可以等待一段时间，将此段时间内一系列的交易打包同一发送，减少了跨委员会的通信次数。这种方式略微增加了时延，但减轻了网络负担。

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- **重叠分片机制**

分片机制通过增加系统并行性，在多个片内同时处理不相交的交易集合增加了区块链系统的性能。然而，分片机制仍然面临着一些问题，频繁的跨片交易就是其中之一。为了减少跨片交易的影响，提升分片机制性能，一种重叠分片的机制被提出。

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- **跨片交易**

在区块链分片系统中，交易集合被映射到不同的分片中，每个分片并行处理交易集合的一个子集。通常一个交易可能具有多个输入和输出。由于每个输入输出相对独立地映射到各自对应的分片，同一个交易的输入和输出可能位于不同的分片中，这样的交易就称为跨片交易。

由于现有分片协议中，交易输入输出往往使用一个基于哈希的映射函数分配给对应的分片，其分布具有一定随机性，因此跨片交易在分片系统中较为普遍。跨片交易可视为一种全局交易，需要由数个不同的分片参与执行。

3.3重叠分片机制

- **跨片交易**

我们对跨片交易进行简单的概率分析：

若一笔交易包含v=p+q个输入输出，在采用基于哈希的随机映射将交易输入输出映射进入不同分片时，输入输出倾向于均匀分配给不同分组处理。
当系统记账节点总数为n，存在k个分组，输入输出单元映射到每个分组的概率均为1/k。对于交易tx，含有v个输入输出单元且其中的每个单元都以 1/k 的概率任意映射到一个分组中。则跨片数为C的概率为：

$$P_{C,\ v,\ k} = \frac{C_k^C S(v,\ C) 1 C!}{k^v} = \frac{k!}{C!\,(k-C)!} \frac{S(v,\ C) C!}{k^v} = \frac{(k-1)!}{(k-C)!} \frac{S(v,\ C)}{k^{v-1}}$$

而不发生跨片的概率 P_(1，v，k)为：

$$P_{1,\ v,\ k} = \frac{1}{C^{v-1}}$$

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- **跨片交易**

在UTXO模型中，UTXO空间被随机均匀地划分给每个分片，因此可以预计大多数交易都是跨片的。

Omniledger中分析到其90%以上的交易为跨片交易，RapidChain发现其96.3%的交易为跨片交易，基于分片机制的种种研究发现，在使用随机输入输出映射的条件下，几乎所有的交易都会是跨片的。

而对于基于帐户或余额的交易模型中，当分片数量大于64时，跨片交易的比例也可以达到90%。

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- **跨片交易**

跨片交易对区块链分片系统带来的性能影响，主要有两个方面：

一是由于一笔跨片交易的验证处理需要多个分片参与，这涉及到不同分片之间的大量通信过程，增加了用户与分片或不同分片之间的通信开销；

二是跨片交易需要多个分片同时处理一笔交易，导致占用的系统处理资源更多，降低了分片系统的并行性。

跨片交易的数量越多，对分片系统的性能折损越大。可见，为了提升分片系统的效率，跨片问题是亟待解决的。在下一节，我们将介绍一种重叠分片方案，通过减少跨片交易发生增加分片系统的效率。

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- **重叠分片**

在多数传统分片方案中，n个记账节点被均匀分布在k个片中，每组分片的记账节点数目为m，每个节点被随机分配到一个片中，不同的分片之间不存在节点的重叠。

这种每个分片仅仅保存该分片的账本子集的分片方式就是状态分片，但是依前文对于跨片交易的问题描述中可以得出，状态分片很可能导致跨片交易的产生，而跨片交易的验证处理会涉及到多个分片的共识和通信过程。

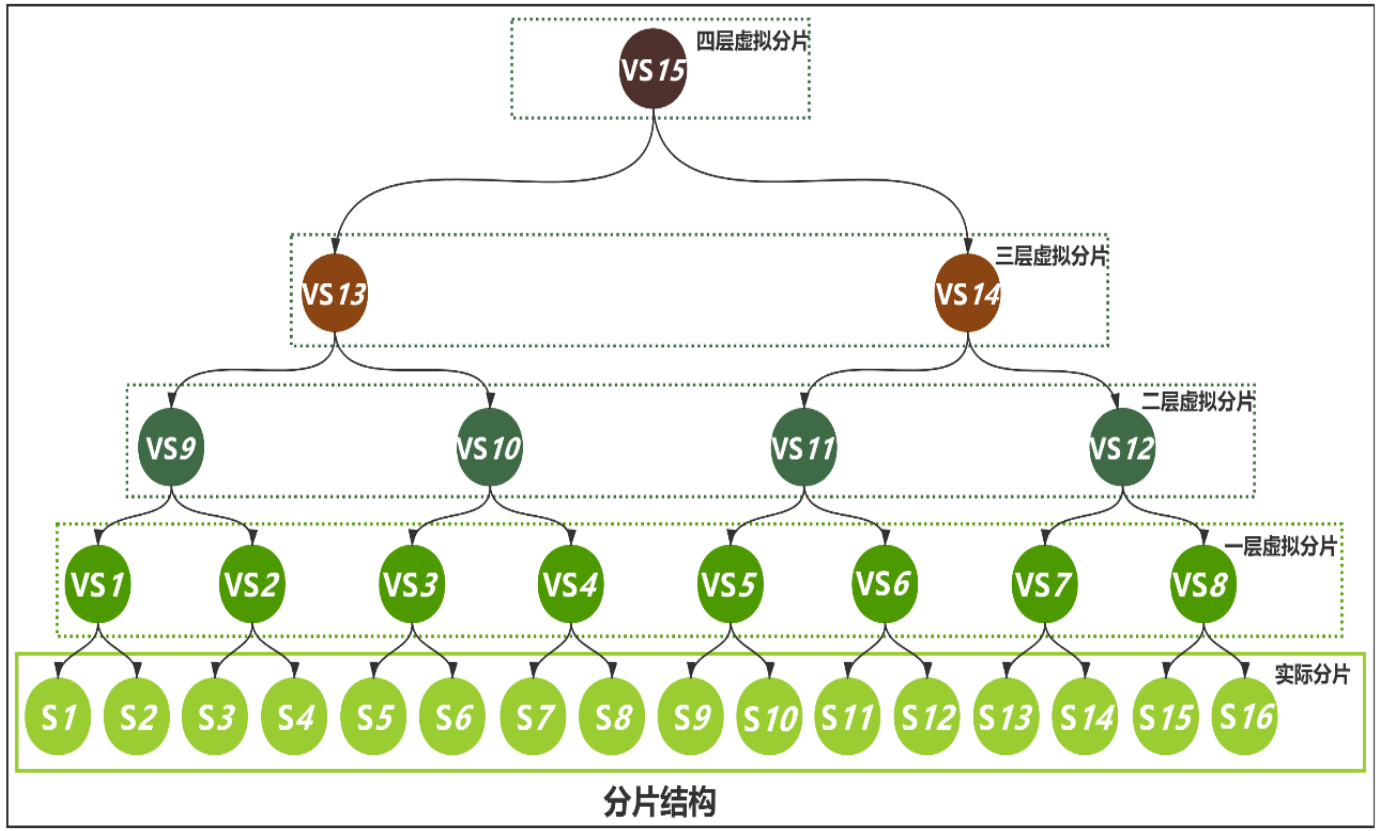
重叠分片认为，更改节点与分片之间的单一映射关系，使得在原本的分片基础上，通过不同分片之间共有的重叠节点重新排列组合成新的分片，可以利用这些排列组合成的新的分片解决涉及到复数分片的跨片交易。

具体而言，重叠分片机制考虑将一些节点映射到多个分片使之共有，而任意两个分片之间的重叠部分就可以处理包含这两个分片的跨片交易。

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- 重叠分片



分片结构

为了兼顾共识的安全性，一种树状重叠分片机制被提出。在不改变区块链系统片数的基础上，树状重叠分片倍增了部分节点存储的分片账本数，通过树形分片结构使得有的节点能够同时存储多个不同的分片账本。

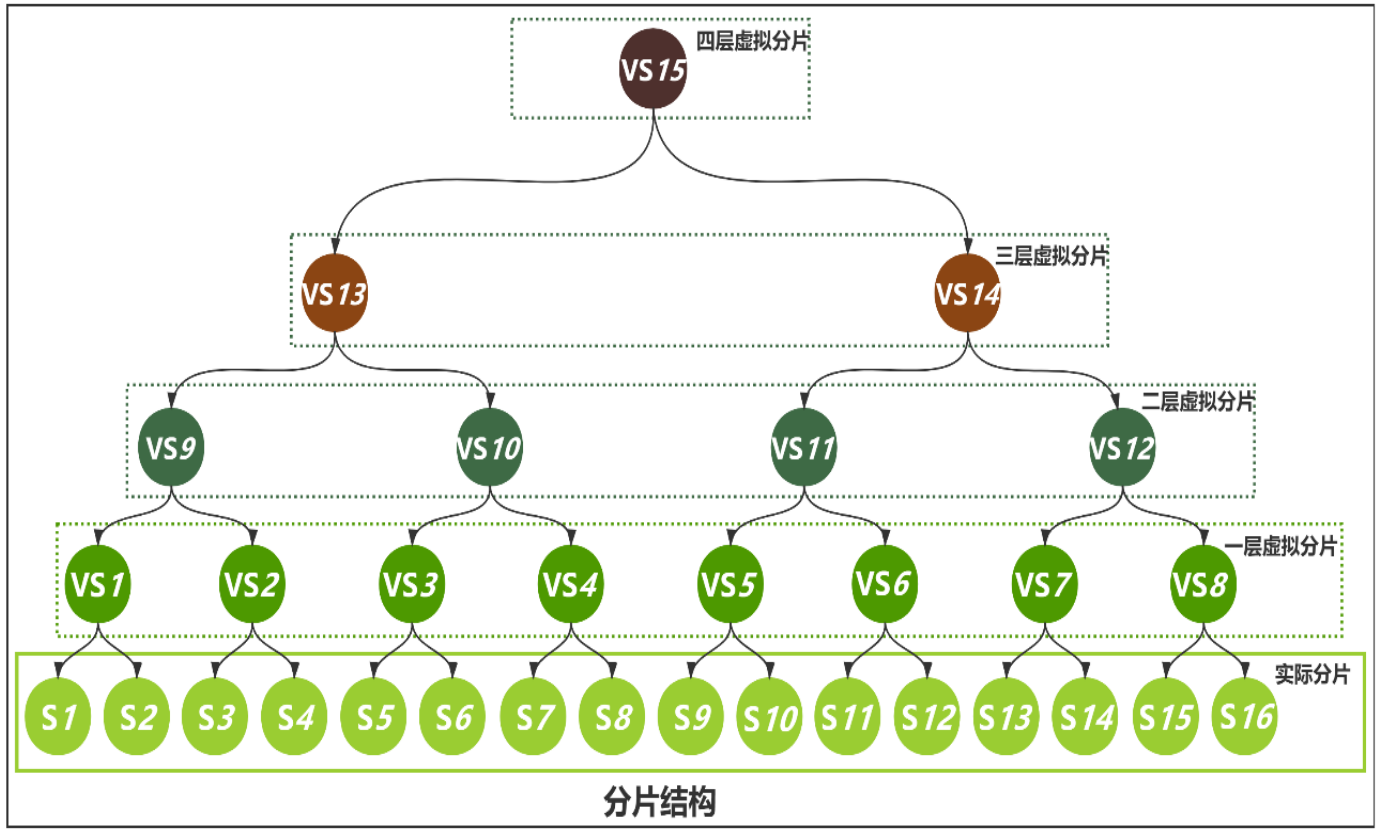
具体而言，该方案使用完全二叉树的结构排列k个分片，每个父分片同时存储其左右子分片的账本子集，整个分片排列的完全二叉树构成由上到下的重叠存储关系。每个验证节点被映射到完全二叉树分片结构中的某个分片，根据分片的位置编码决定了这个节点的重叠存储倍数。

这样的由上到下重叠存储的分片结构决定了在任何一笔跨片交易发生时，都能够找到同时包含相关账本子集的分片用来处理该跨片交易。

3.3重叠分片机制

北京大学 PEKING UNIVERSITY

- 重叠分片



分片结构

实验表明，与非重叠分片机制相比，重叠分片机制的平均通信开销降低了越60%。

并且若从叶子节点开始构建，只需要三层重叠分片，系统跨片交易数量就可以降低到50%。当然，值得注意的是，现有的树状重叠分片仍然存在负载不均衡的问题，即那些位于“存储树”树根上的高层节点，会参与到多个虚拟片的共识之中。因此这些节点的负载可能远高于系统中的其它节点。这也是重叠分片机制一个需要改进的问题。

本章小结

区块链的广泛应用离不开高效的性能支持。在本章中，我们介绍了区块链现有的性能问题，以及造成这些性能问题的可能原因。

面对这些性能上的挑战，各种区块链性能扩展机制相继被提出，本章介绍了性能扩展机制分类中的链下、链上和第零层扩展机制。特别的，本章还详细介绍了链上机制中的分片机制，以及对分片机制的一种改进，即重叠分片。

我们可以看到，在交易处理的各个环节中，都可能存在影响区块链系统性能的因素，而对各个环节的改进都可能产生一种区块链性能扩展机制。在实际应用中，多种性能扩展机制往往可以被同时采取，以期获得更好的系统性能。时至今日，区块链性能扩展仍然是一个活跃的研究领域，更好、更快的系统机制不断被提出，给区块链技术的大规模应用给予更好的保障。

北京大学
PEKING UNIVERSITY

感 谢 观 看