区块链技术与应用

（2022年春季）

计算机科学与技术学院　李京

9章　区块链扩容

目 录

9.1 区块链扩容概述

- 可扩展性是当今应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，比特币只有4-7 TPS 。
- 以太坊作为支持智能合约和DApps的市场领导者，其平均的TPS约为15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。
- **区块链领域的扩容即围绕如何在“更短的时间实现更多的交易”，增强区块链的可扩展性（scalability）。**

	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)

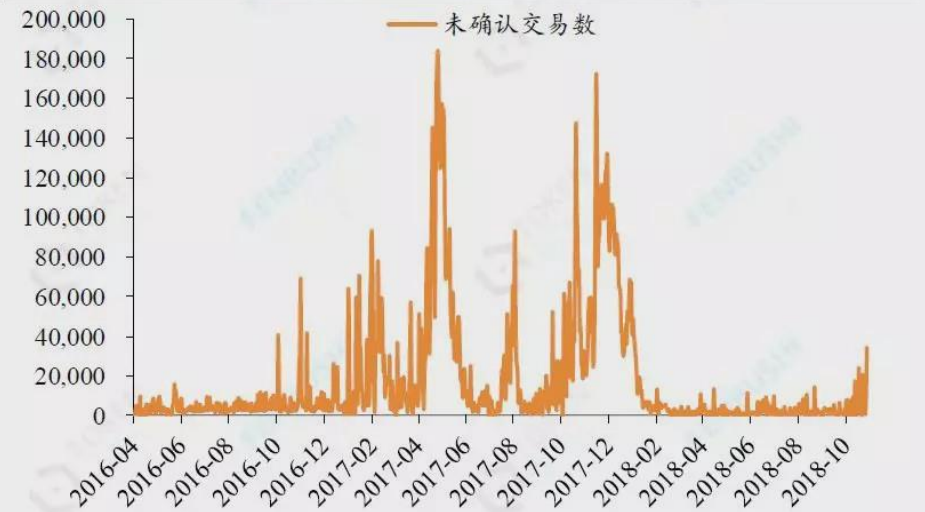
TPS（Transactions Per Second，平均每秒交易量）

拥堵的区块链

BTC：最高超过19万笔未确认交易。BTC区块大小的上限为1MB，每10分钟左右产生一个区块，从历史数据来看，BTC的TPS（每秒事务处理量）约为3.5（理论TPS可达到7）。交易笔数较少时不存在拥堵问题，但是随着交易笔数的飙升，拥堵日益显现，根据Blockchain.info数据，BTC未确认交易数最高时在19万笔左右。

ETH：一只猫造成的拥堵。2017年11月底，虚拟养猫游戏CryptoKitties（又名“云养猫”）上线后过于火爆导致ETH网络出现严重拥堵，2017年12月5日ETH未处理交易达到峰值19800笔。

图表1：BTC 未确认交易数



资料来源：Blockchain.info，通证通研究院

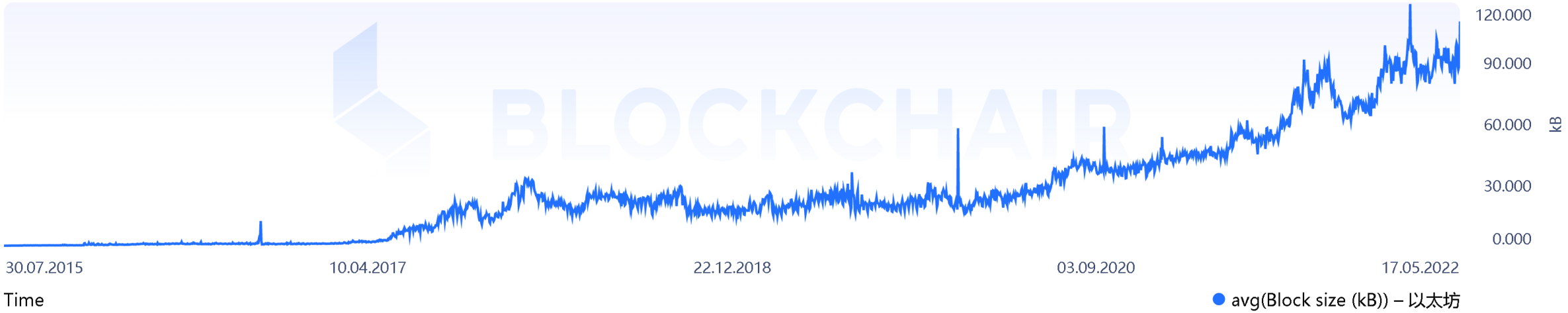
图表2：2017 年 12 月云养猫导致以太坊网络拥堵

资料来源：Etherscan.io，通证通研究院

比特币和以太坊的平均区块大小

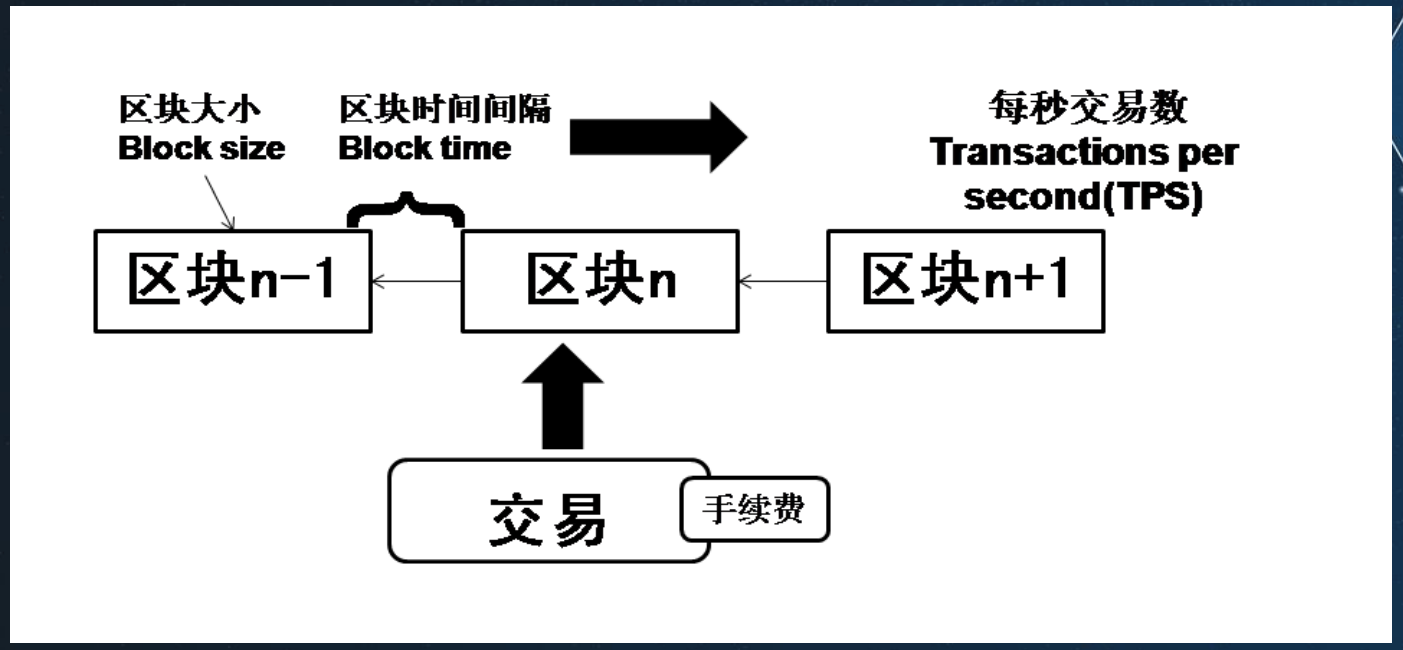
比特币平均区块大小图表

以太坊平均区块大小图表



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。



- 例如：比特币区块生成间隔约为10分钟，区块大小的限制为1MB。按一笔交易最少250字节计算，比特币交易吞吐量的上限为7笔/秒。所以一般称比特币交易的TPS是3-7笔/秒。
- 为了缓解效率问题，隔离见证，2M区块大小的方案被提出。

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

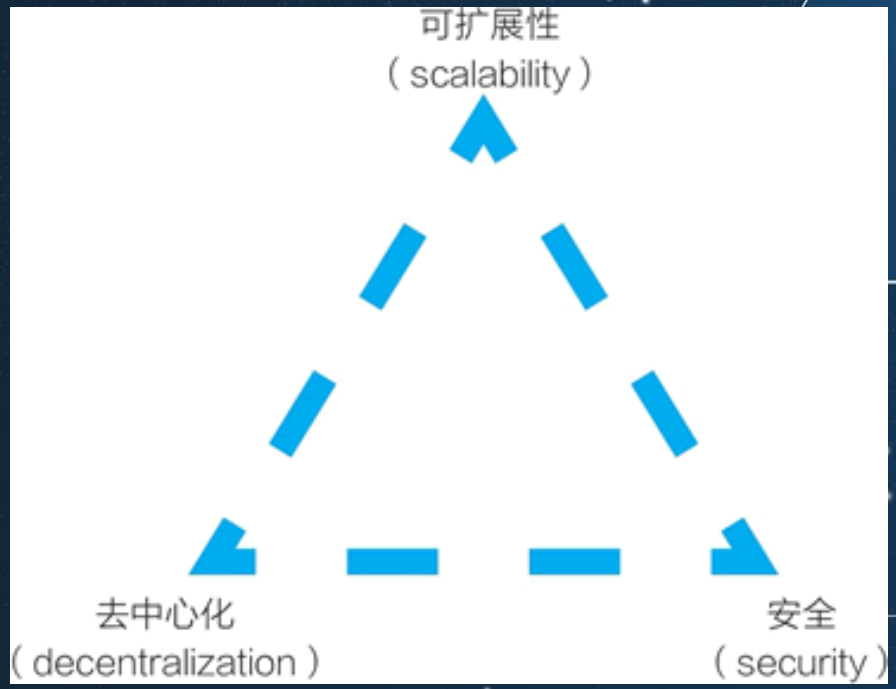
扩容的制约因素

为什么不能简单增加区块大小或缩短出块间隔时间以加快交易确认的效率呢?

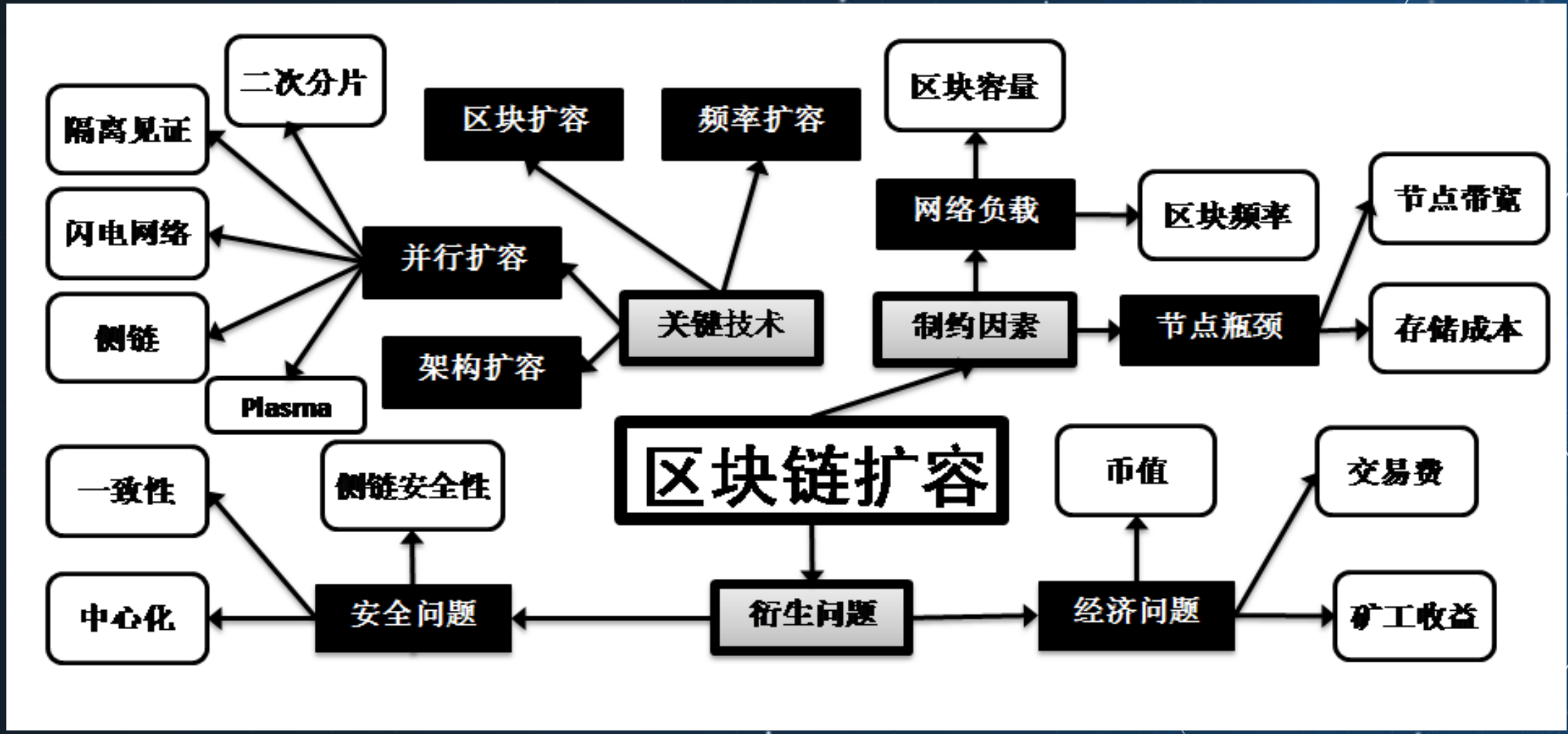
- 网络负载：由于每笔交易需要网络中每个全节点处理和验证，区块体积越大扩散至整个网络所需的时间越多，传播延时是导致区块链分叉的主要因素，会导致大量的分叉和孤块。
- 节点性能：区块变大导致区块的验证的算力成本、账本的存储成本和传输带宽成本都将上升，对节点的性能要求有大幅提高。
- 安全问题：对节点的性能要求有大幅提高带来的运营成本上升，孤块率的增加进一步可能将导致普通计算机用户甚至小矿池退出，进而算力呈中心化趋势以及安全性减弱。

区块链可扩展性不可能三角

- 区块链可扩展性不可能三角（Scalability Trilemma）是指区块链系统一般只能实现非中心化、安全性和可扩展性中的两个属性。想要显著提升可扩展性，则必然要在安全性和非中心化上有所舍弃。
- BTC和ETH重点关注的是安全性和非中心化，一定程度上牺牲了可扩展性。

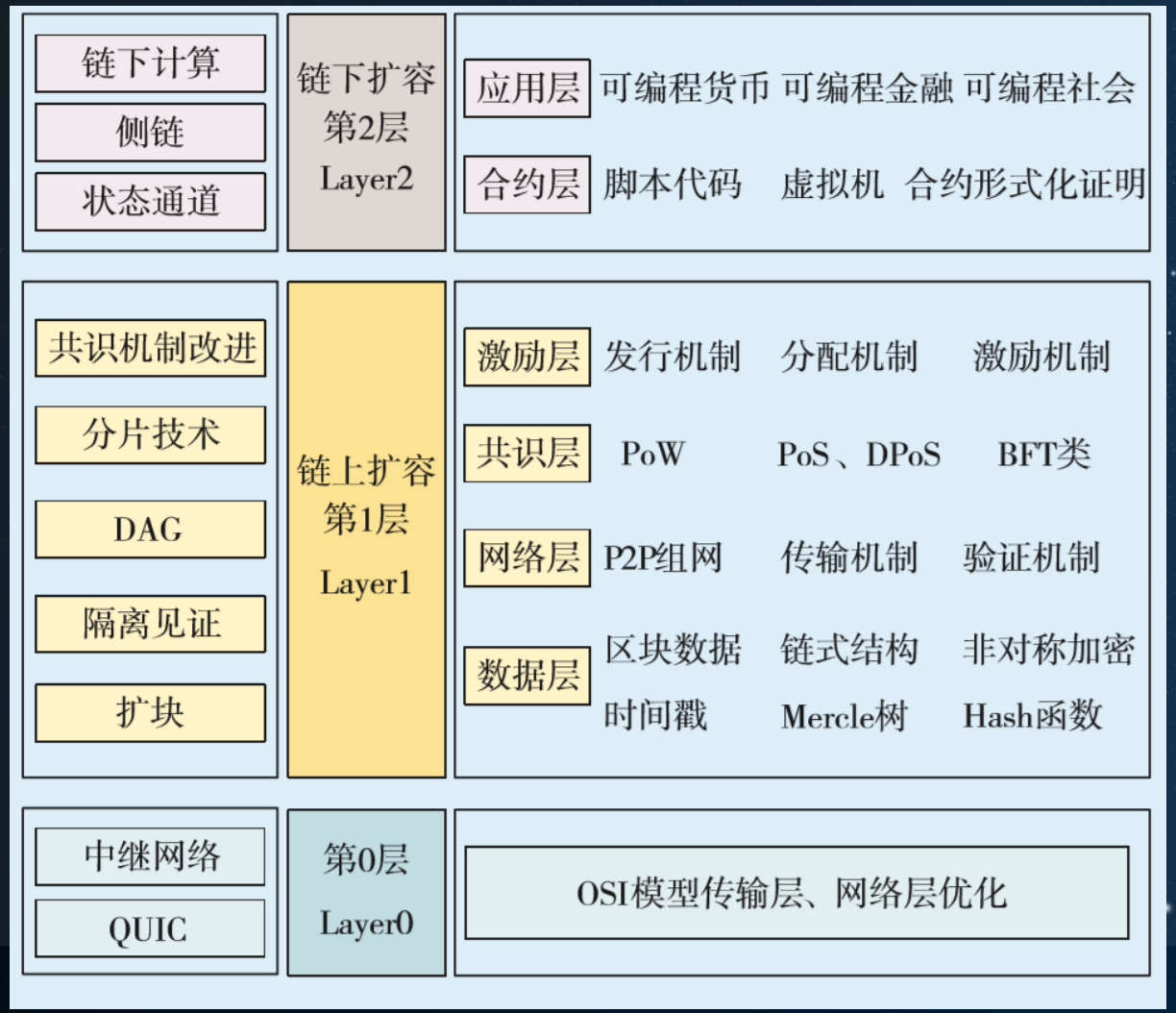


研究框架


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



- 第2层扩容（链下扩容）不改变基本协议，在应用层进行改变提升扩展性
- 第1层扩容（链上扩容）通过改变基本协议提升区块链效率
- 第0层扩容通过改变区块链底层数据传输协议提升区块链可扩展性

比特币的扩容方案

- 扩块：
- 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。

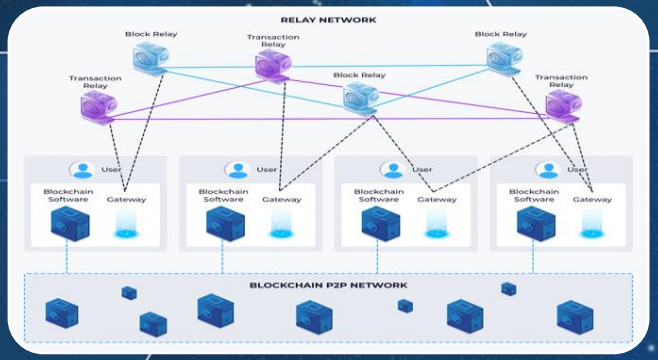
以太坊的扩容方案

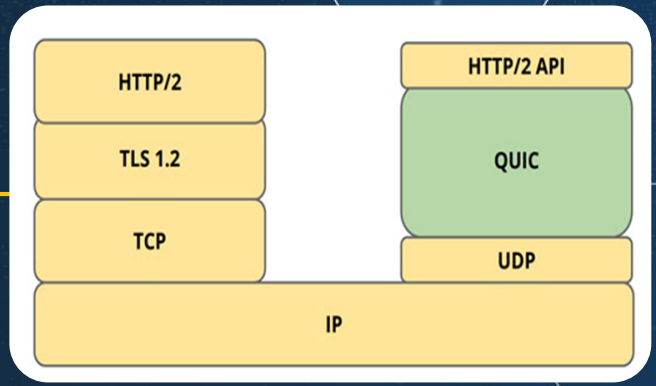
- 子链：Plasma在以太坊主链上创建“子链”，处理链下交易的技术，需要依赖以太坊底层技术去对其安全性进行保障。
- 状态通道：雷电网络(Raiden Network)是状态通道技术在以太坊上的实现。利用链下（off-chain）状态网络对以太坊交易处理能力进行扩展。
- 分片+PoS：以太坊2.0

9.2 区块链扩容-第0层扩容方案

第0层扩容方案

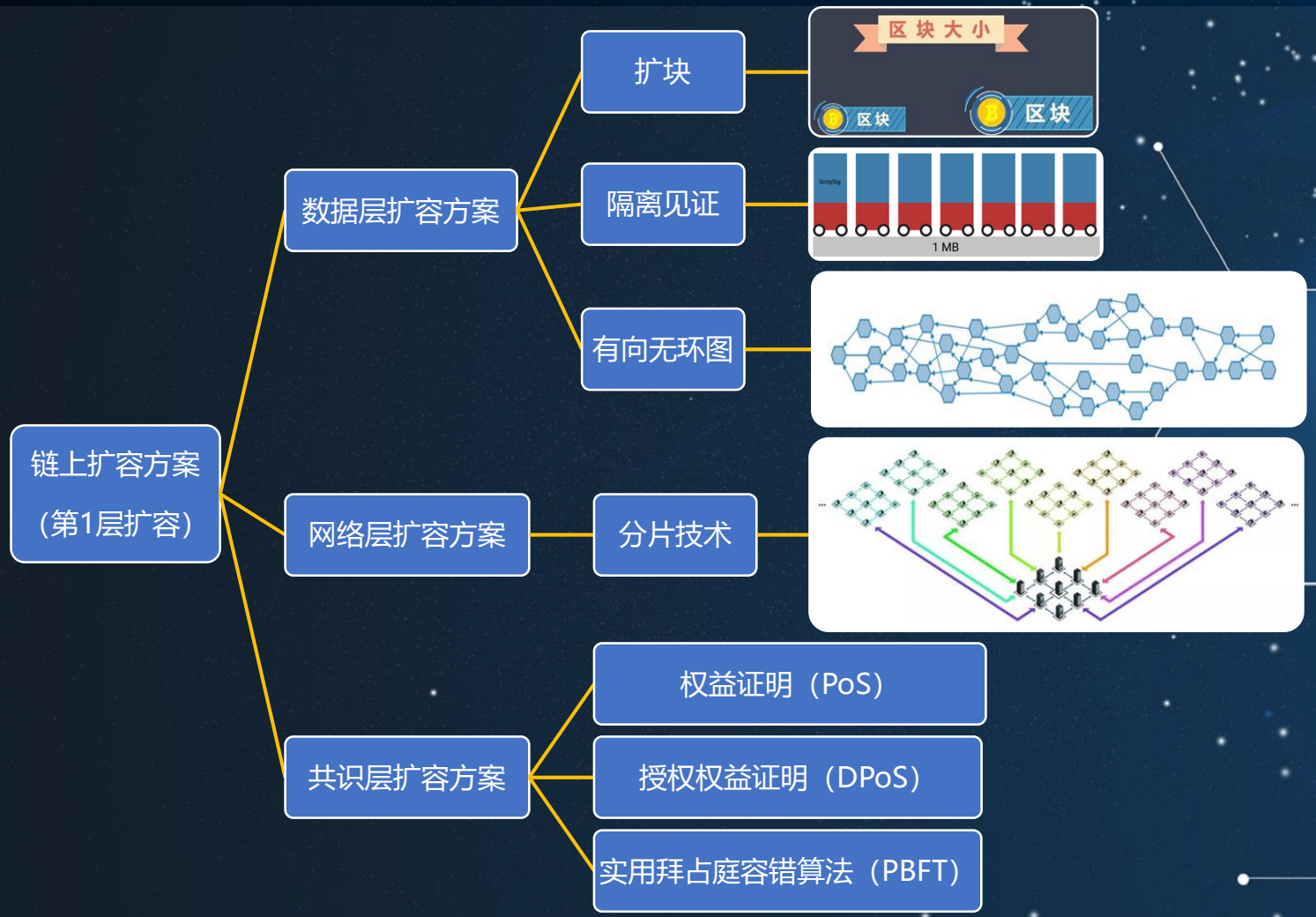
- 覆盖网络
  - 比特币中继网络
  - 区块链分发网络
- QUIC优化协议





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。

9.3 区块链扩容-第1层扩容方案（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。

链上扩容方案包括数据层扩容方案、网络层扩容方案和共识层扩容方案，基本思路是增加区块大小（直接或变相）或减少区块验证传播时间和形成共识时间。

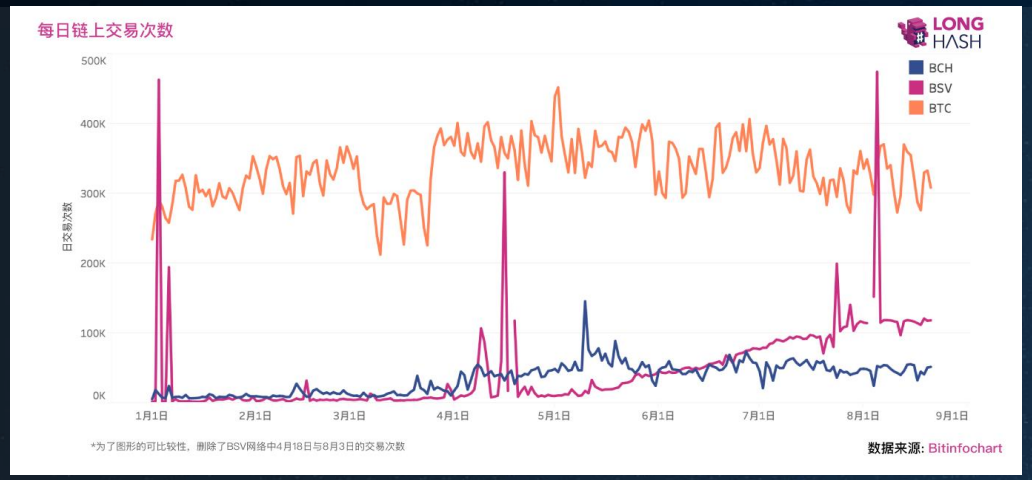
数据层扩容-扩块

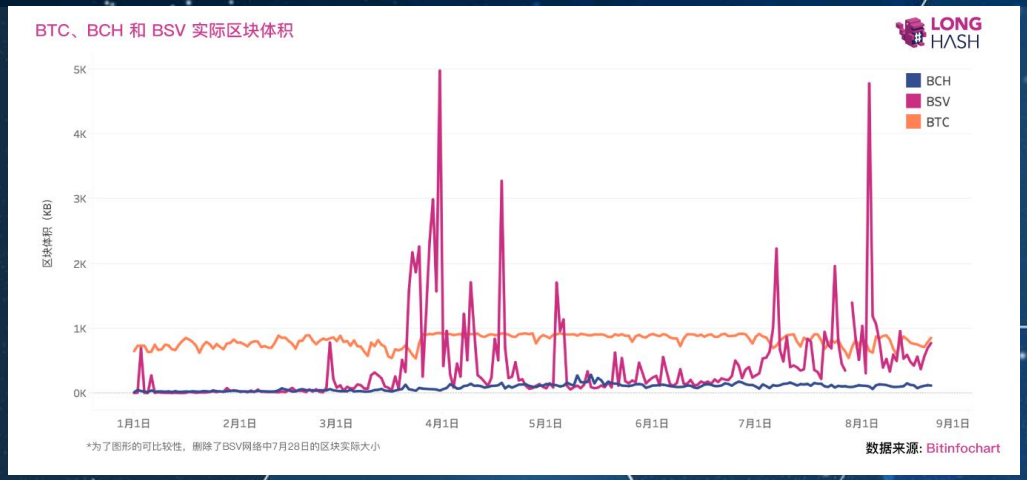
- 扩块方案即增加区块容量，从而单个区块包含的交易数量相应增加，实现扩容目的。
- 以Bitcoin Cash（BCH）为例，2017年BCH区块大小提升至8M，2018年5月又再次提升至32M。从理论上说，在平均区块间隔固定的情况下，网络TPS上限与区块大小成正比。但由于前述制约因素的存在，区块的大小不能无节制随意扩大。
- 2018年年末，因为对BCH的升级内容不满，以“澳本聪” Craig Wright为代表的Bitcoin SV团队宣称要恢复部分中本聪设定的操作码，并于11月15日进行了硬分叉，诞生的Bitcoin SV区块上限为128MB，随后又在 2019年7月升级为2GB。

数据层扩容-扩块

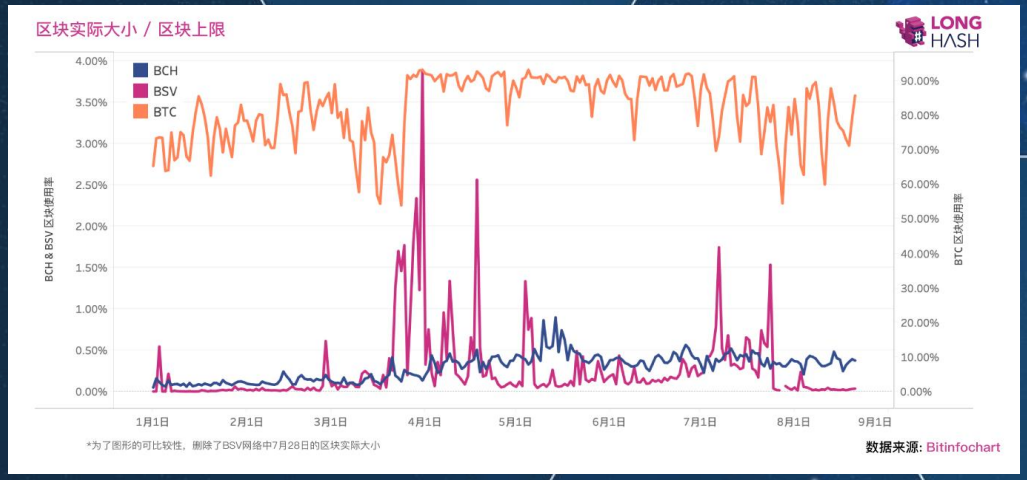
- BIP100提议将区块容量控制权交给矿工，曾得到占据全网算力25%的三家矿池（f2pool、Kano pool以及Bitclub）的支持，但同时也引发了许多争议；
- BIP101曾获得业内多家公司支持，曾一度被加入BitcoinXT代码库，但BitcoinXT后来转而支持Classic的2MB区块方案；
- 2016年2月份，Gavin Andreesen基于BIP109创立了Bitcoin Classic。Bitcoin Classic得到了一些比特币公司、开发商、投资者和矿商的支持。2017年11月10日，在通过硬分叉将比特币区块容量扩大到2MB的计划失败后，Bitcoin Classic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

BTC、BCH、BSV的现状





	市值	区块上限	在线全节点数	算力	24H链上交易次数	链上交易平均手续费	ATM机
BTC	$180,680 M	1MB	9,078	78.55 EH/s	280,974	$1	5,000+
BCH	$5,489 M	32MB	1,421	2.13 EH/s	42,651	$0.0028	2,000+
BSV	$2,382 M	2GB	480	903.78 PH/s	121,421	$0.00097	NA



从防范 51% 算力攻击的网络安全层面上看，Bitcoin 的算力维持在 80 EHash/s 左右，Bitcoin Cash 的算力维持在 2 EHash/s 左右，约为 Bitcoin 网络的 1/40；Bitcoin SV 的算力维持在 1 EHash/s 左右，约为 Bitcoin 网络的 1/80。

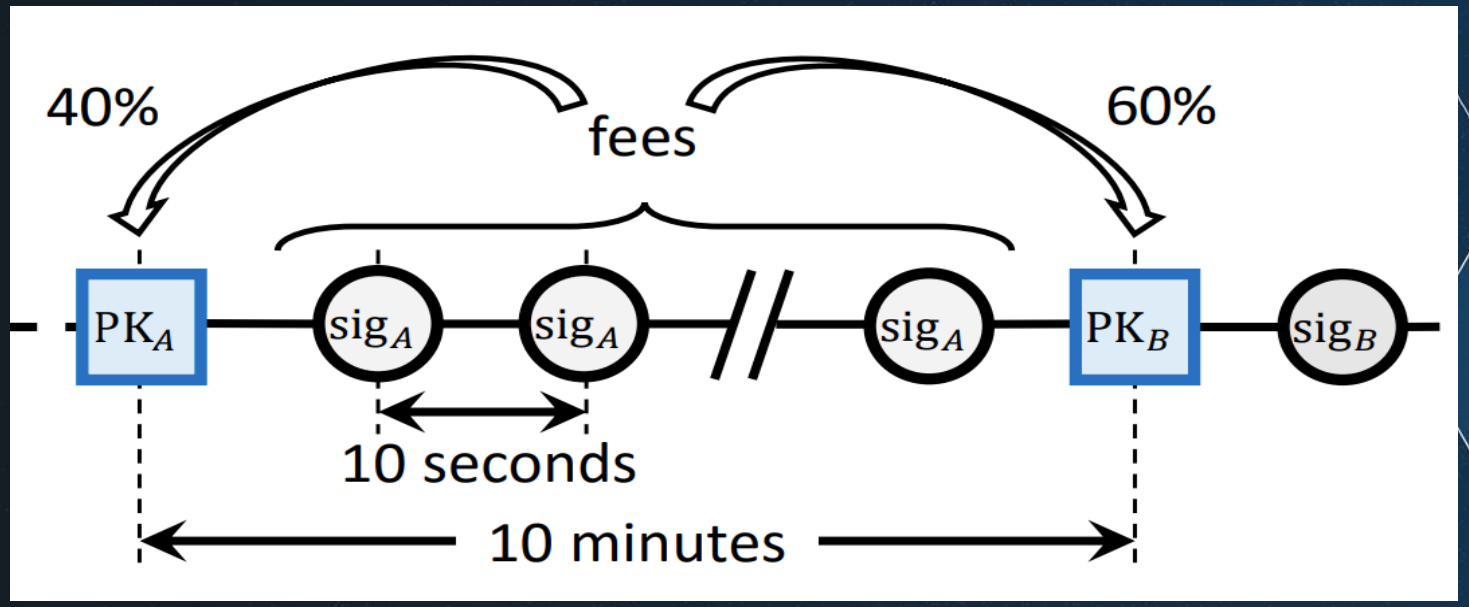
摘自：“从 1 MB 到 2 GB，BSV 大区块真的有必要？”，https://www.longhash.com/cn/news/2876，2019年

数据层扩容-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。

数据层扩容-出块时间-Bitcoin-NG

Ittay Eyal, et al，Bitcoin-NG: A Scalable Blockchain Protocol，Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16). March 16–18, 2016 • Santa Clara, CA, USA



- 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)

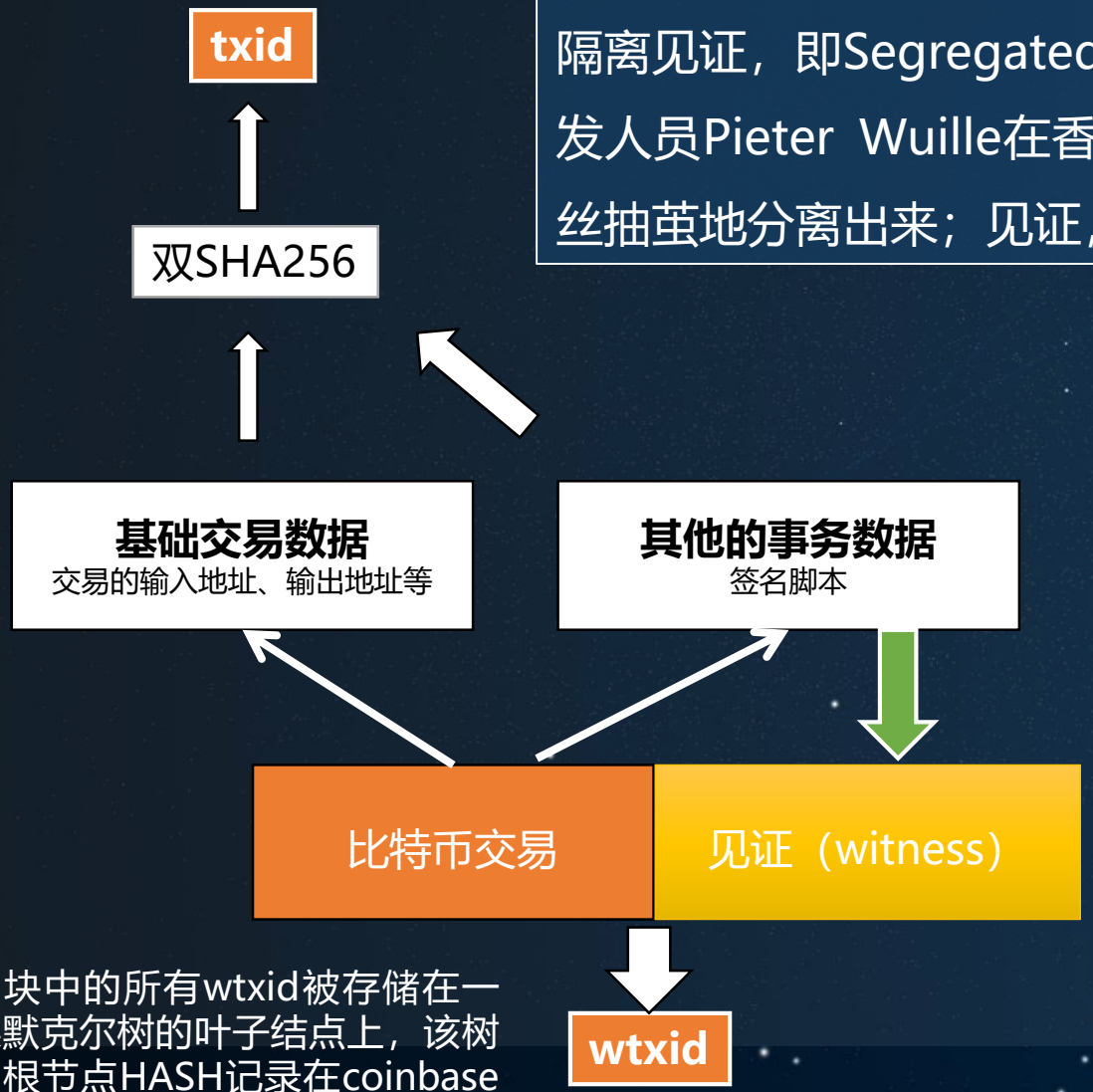
（康奈尔大学，Ittay Eyal等）

数据层扩容-出块时间-Bitcoin-NG

bitcoin block	key block	microblock
* 前一个区块的哈希值	* 前一个区块的哈希值	前一个区块的哈希值
* 当前的Unix时间	* 当前的Unix时间	* 当前的Unix时间
* 一份交易用于支付挖矿酬劳给自己	* 一份交易用于支付挖矿酬劳给自己	* 当前区块的哈希值
* target 值	* target 值	* header的加密签名(使用和公钥相匹配的私钥进行签名)
* nonce 值	* nonce 值	* 区块包含的交易
* 当前区块的哈希值	* 当前区块的哈希值	
* 区块包含的交易	* 领导者的公钥public key(会被用来验证微块的所属)	

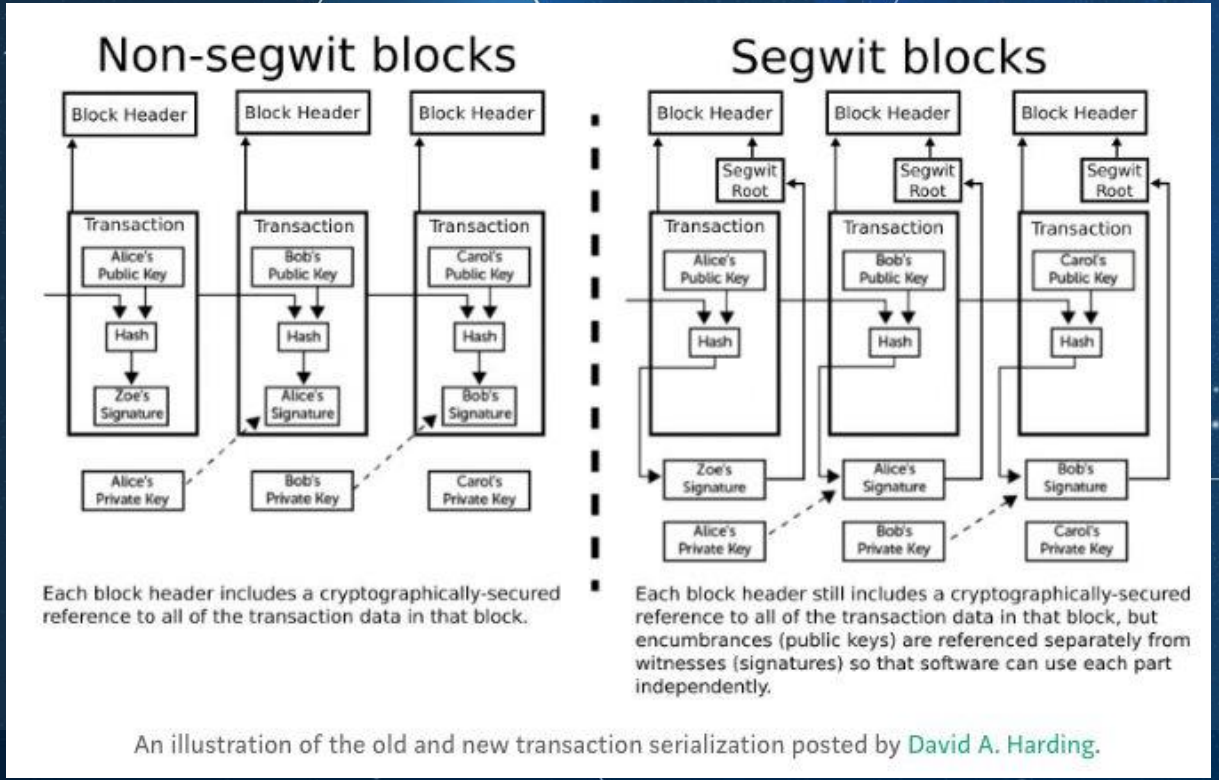
截图(Alt + A)

数据层扩容-隔离见证



隔离见证，即Segregated Witness（简称 SegWit），2015年12月，由BTC核心开发人员Pieter Wuille在香港首次提出。隔离，可理解为把见证数据从交易信息中剥丝抽茧地分离出来；见证，指的是在BTC网络中对交易合法性的公开验证。

2015年12月香港比特币扩容会议



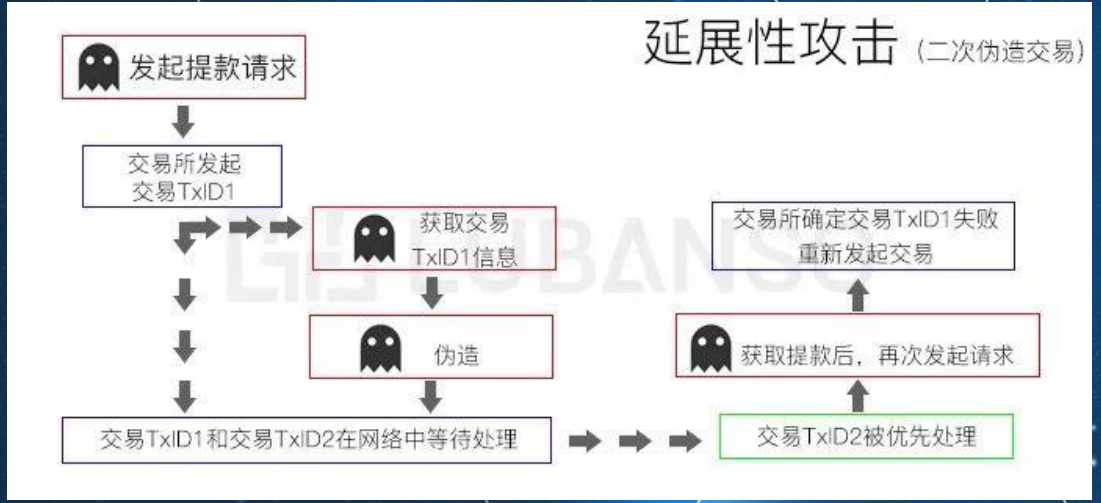
区块中的所有wtxid被存储在一棵默克尔树的叶子结点上，该树的根节点HASH记录在coinbase交易的scriptPubKey中。

数据层扩容-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。

- 比特币交易一部分是基础交易数据，包括交易的输入地址、输出地址；第二部分为其他的事务数据，包含了签名脚本等验证交易有效性的数据。
- 签名脚本（signature script）包含一个secp256k1的椭圆曲线加密签名，但是不能签名脚本自己，这使得攻击者可以对交易进行非功能的修改，这一性质被称为交易延展性（transaction malleability）
- 攻击者利用交易延展性在交易未被写入区块前更改其txid，将有一定概率“顶替”原交易被打包。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，造成有限的DOS攻击。



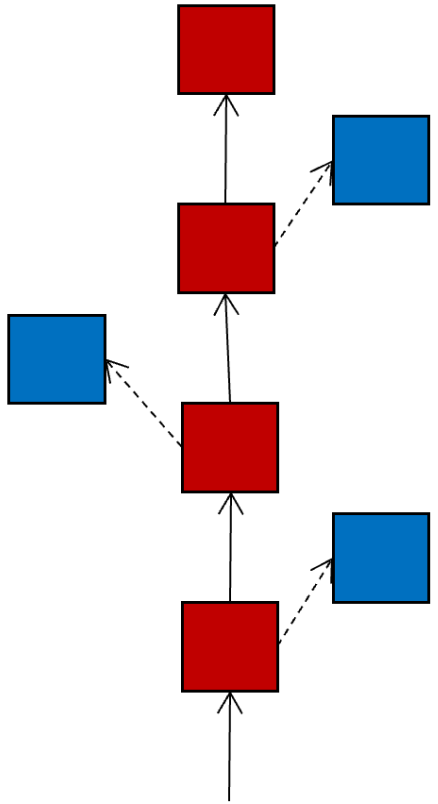
- secp256k1的椭圆曲线加密签名
- 攻击者可以进行非功能的修改
- 当交易所或用户基于txid查询交易时，会无法确认交易完成，发送大量交易请求

数据层扩容-隔离见证

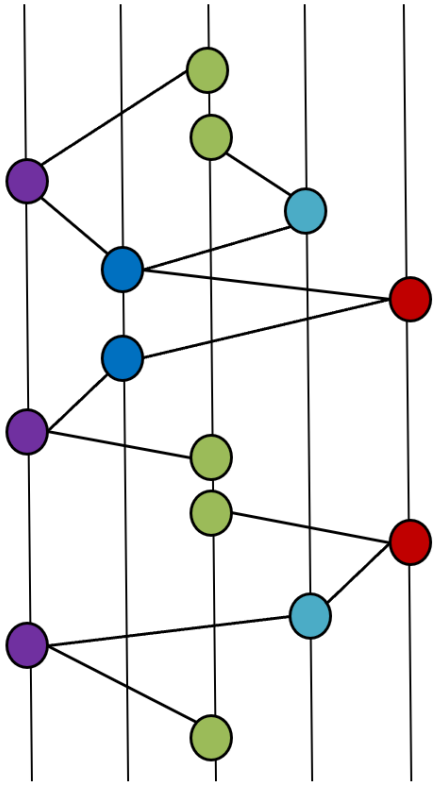
2017.5.11，莱特币正式激活隔离见证;

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;

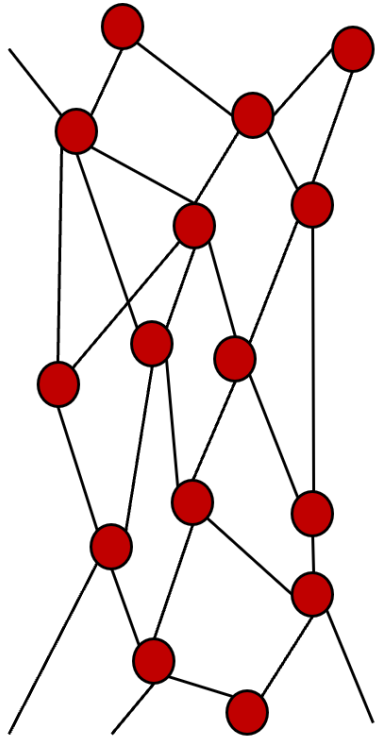
数据层扩容-基于DAG的新型区块链架构



链式结构



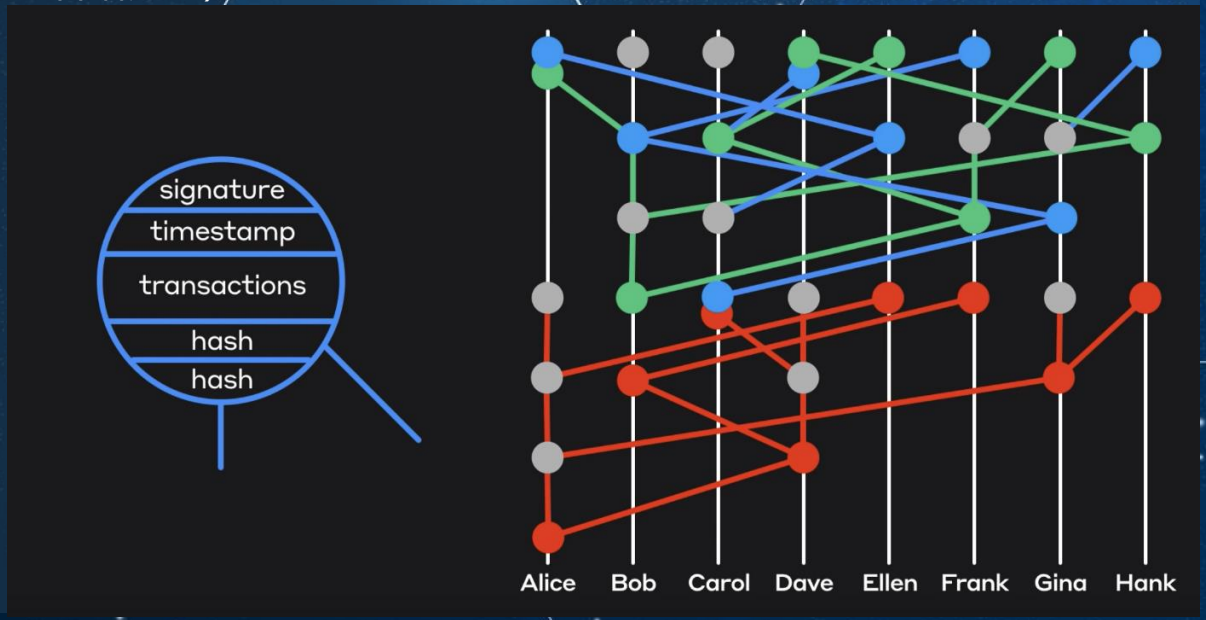
哈希图（Hash Graph）



缠结（Tangle）

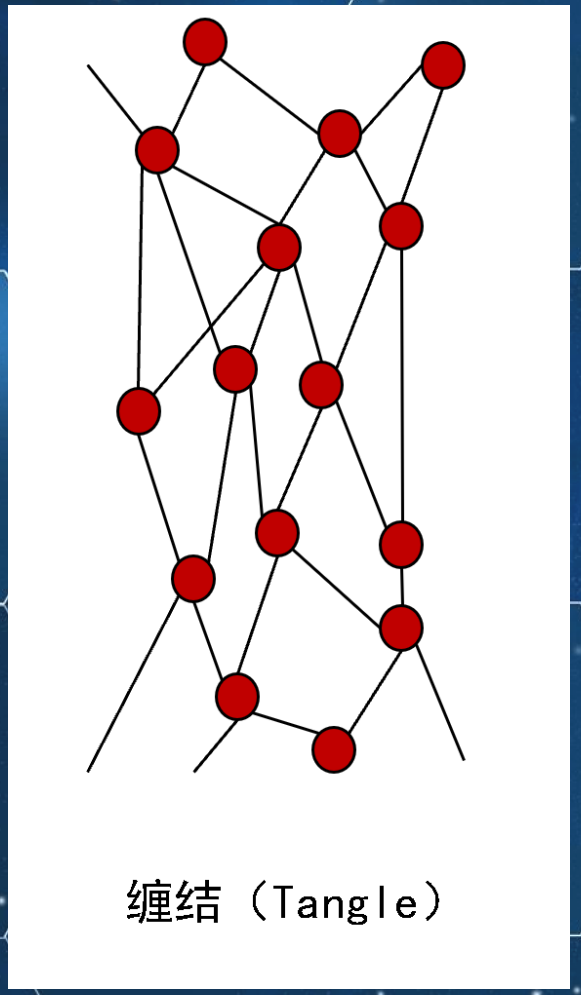
区块链扩容-架构扩容-HashGraph

- Hedera Hashgraph是一个公共分布式分类帐，支持以Web规模运行的分布式应用程序。 Hedera的数据将记录在DAG（有向无环图）上，而不是像当前流行的区块链平台那样记录在链上。
- 哈希图（hashgraph）的解决方法是，不抛弃事件，结构的增长不会受到限制。任何人都可以创建交易，这样，交易的吞吐量就会大增。从这角度看，哈希图提出了新的思路，它无需修剪，试图用新的数据结构和共识算法实现更高的交易速度。
- 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（节点）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（Gossip）



数据层扩容-IOTA

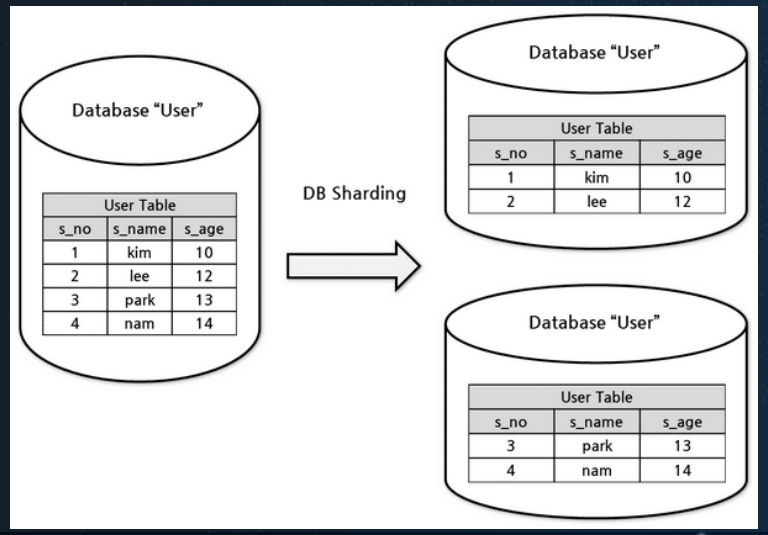
- IOTA是2014年众筹的一个项目，宗旨是利用DAG(有向无环图，IOTA里叫Tangle缠结)代替区块链实现分布式、不可逆(由密码学保证)信息传递的一种技术，在此基础上集成加密货币功能，服务于物联网，而IOTA是为物联网(IoT)而设计的一个革命性的新型交易结算和数据转移层。它基于新型的分布式账本—Tangle(缠结)。Tangle(缠绕)是分类帐结构的名称，Tangle就像区块链一样，但它使用网络结构而不是链状结构，这使它更具拓展性和稳定性。
- 在IOTA里发起一笔交易，需要先找到网络里的两笔交易，验证它们的合法性，然后做一点小小的 PoW（就是付出一些计算），把自己的交易与它们绑定，再广播到网络。该交易也会被后来的交易以相同的方式验证。如果交易被验证的次数越多，则该交易的确定性越高。当达到一个阈值时，就认为这个交易被确定了。IOTA把算力作为交易的一部分，要加入网络，那必须先成为矿工。零交易费。
- 非法交易的处理。IOTA的节点会计算每个交易的权重值，选择权重高的交易来进行验证，这会有助于增加自己的交易被后来交易验证的可能性。如果绑定了非法交易，那后来的交易则不会选择该交易来验证。时间一长，这个交易就被网络抛弃了，不再是网络的一部分。
- DAG避免了因网络延迟和数据同步造成的时间浪费，可以做到高并发。

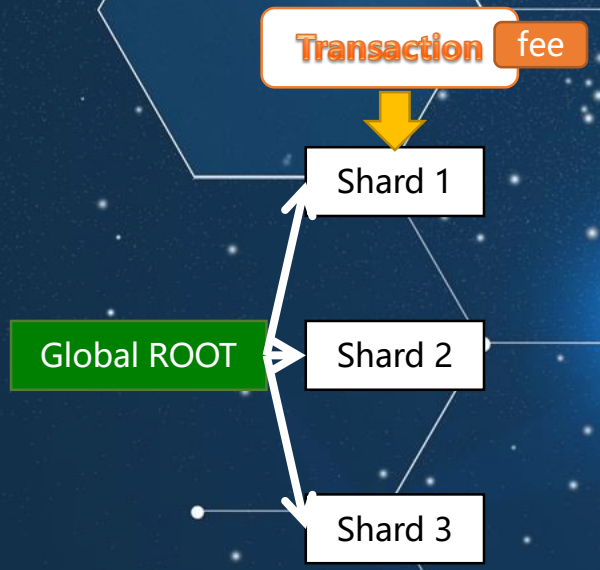


缠结（Tangle）

网络层扩容-分片（Sharding)

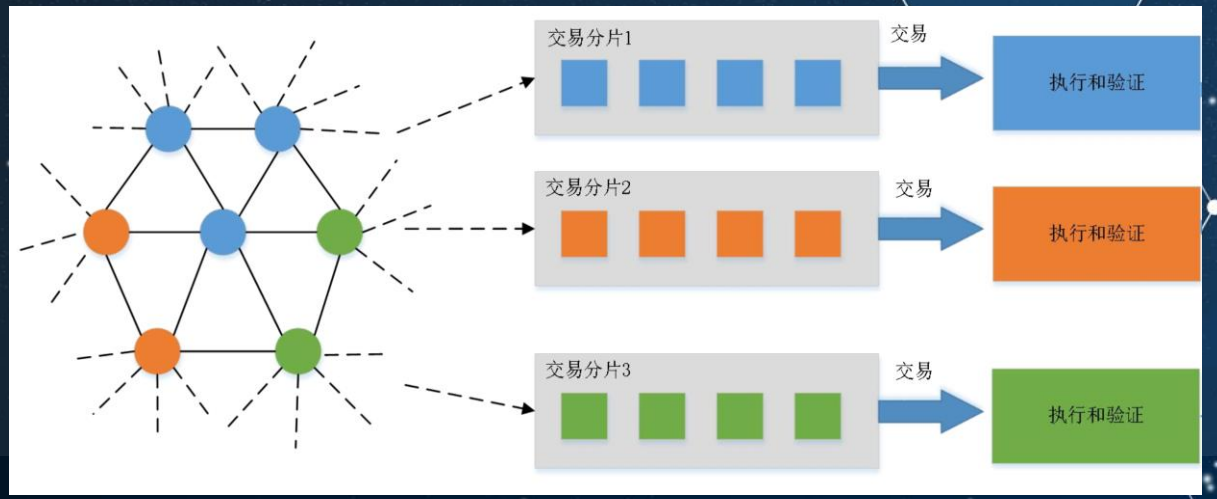
- 分片（Sharding）是指将区块链分成不同部分，即多个分片，分片可以并行处理事务，从而提升了单位时间内处理交易的数量。
- 分片原本是种数据库扩展方案，它把数据库横向扩展到多个物理节点上，其目的是为了突破单节点数据库服务的I/O能力限制；而区块链的分片方案是将原来的单条区块链进行二次扩展，以突破单个节点的计算能力限制。





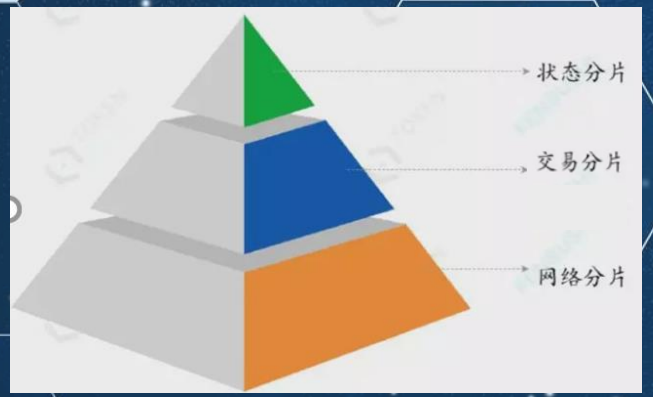
分片的原理

- “区块链分片方案”最早由Zilliqa团队成员、新加坡国立大学的Loi Luu等人于2015年在CCS会议上提出。 区块链网络中的分片技术通常指的是整个区块链网络被划分为若干个子网络， 每个子网络中包含整个网络的部分节点， 每个子网络就叫做分片 。每个分片各自处理一小部分的客户端交易，并且通过与网络上的其他节点并行处理就能完成大量的验证工作。所以，分片技术使用的是并行处理的方式，有越多的节点加入，网络中批准的速度也会加快。简单来说，分片的就是将一个大任务拆分为多个可以并行处理的小任务，从而提升性能。
- 主要的核心在于分片内节点需要达到一致，并且防止被恶意攻击者控制，而分片之间需要信息传递机制，保证交易及智能合约的状态在不同分片间达到一致。



分片的层级

1. 网络分片：网络按照一定规则选取节点形成分片。实施分片的第一步就是创建分片，因此网络分片是交易分片、计算分片和状态分片的基础。
2. 交易分片：按一定规则将交易分配到同一个分片处理，达到既能并行处理又能避免双花问题的出现。在不同的记账方式下，对交易分片的要求有所区别。
    - UTXO模型下，交易分片需要跨分片通信。一笔交易可能包括多个输入和多个输出，仅仅按照地址分片无法避免双花问题，分片之间不得不进行通信。
    - 在账户/余额模型下，由于一笔交易只有一个输入，因此只要将交易按照发送者地址进行分片，就可以保证同一个账户的多笔交易在同一个分片中处理，有效防止双花。
3. 状态分片：特定的分片只存储部分状态，而不是完整的区块链状态。状态分片能够减少状态储存冗余，状态分片是最为理想化的分片方式，但是面临着一系列挑战，如跨分片通信、数据有效性和数据可用性等。



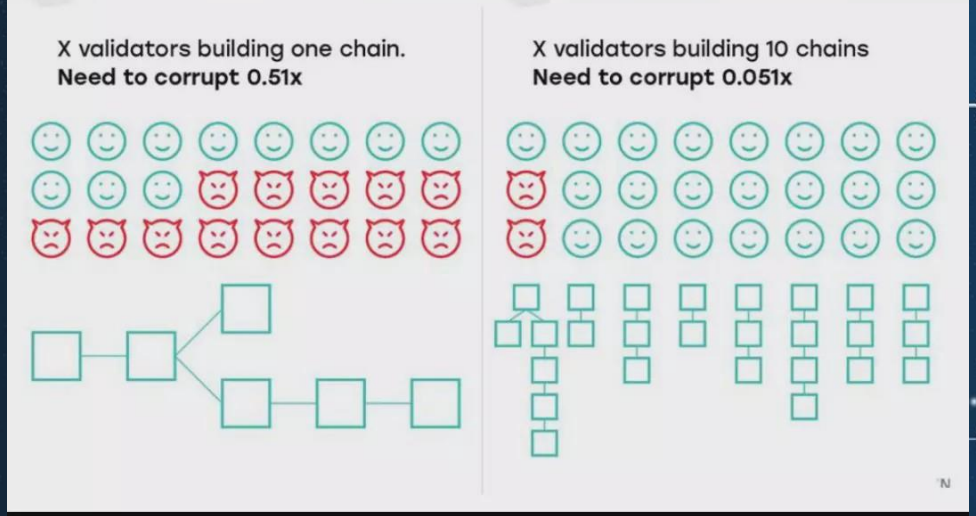
分片的挑战

- 分片在提升了效率的同时也带来了新的问题，主要包括
  - 分片内部的安全和效率问题
  - 跨片交易引发的跨分片安全和效率问题

分片安全

- 单个分片的算力以及单个分片内的验证节点数量远低于分片之前的整个区块链网络，从而导致对采用PoW共识的单个分片发起51%攻击，或者对采用非PoW共识的分片发动女巫攻击（Sybil Attacks）的成本也极大地降低了。
- 采用何种共识机制、如何划分分片大小以及如何为分片分配节点以防止恶意节点控制分片变得至关重要。现有的分片设计主要通过某种随机性分配验证节点，降低作恶者控制单个分片的概率；针对恶意分叉问题可以通过将部分分片链上的区块连接到信标链（信标链负责协调系统的参与者，如随机分配验证节点到分片及从分片接收状态更新等），并将分叉选择规则设定为首选交叉连接到信标链的链。对女巫攻击问题的解决方案包括要求节点提供抵押物或执行PoW等，以提升作恶成本。

图表5：分片后攻击单个分片的成本相比于分片前极大降低



资料来源：The authoritative guide to Blockchain Sharding, part 1，通证通研究院，FENBUSHI DIGITAL

跨片交易和热点分片

- 跨片交易带来跨分片通信，需要权衡通信导致的成本和性能提升带来的收益。极端情况下，系统内的交易全部是跨分片交易，此时系统的性能将低于分片之前。
- 跨片交易问题的解决方案通常包括同步和异步两种方式，同步方式下，当跨分片交易发生时，各个分片的验证节点协作执行跨分片交易；异步方式下，跨分片交易在各个分片中异步执行，即在有足够证据表明发送方所在的分片已执行其负责的任务后，接收方所在的分片处理其负责的任务，这种方式相对简单且容易协调，因此目前更为普遍。
- 分片理论上能够提升整个网络层面的性能，但是对于单个分片仍然可能存在单点过热问题，即单个分片内部仍然存在交易量过大导致拥堵的可能。

Zilliqa分片

- 利用PoW防范女巫攻击。Zilliqa的共识算法为PBFT+PoW，分片内部运行PBFT共识，使用PoW防范女巫攻击以及实现网络分片。
- 网络分片实现：基于PoW结果随机分配节点到分片，防止作恶者控制单个分片。Zilliqa基于PoW选举一组特殊节点组成目录服务委员会（Directory Service Committee，简称DS委员会）。DS委员会形成后便开始分片，网络中的其他节点执行PoW并提交给DS委员会验证，PoW的后几位二进制数字决定了节点被分配到哪个分片。
- 交易分片实现：依据事务分类进行分配。Zilliqa将事务分为三类：第一类事务为用户之间的交易，不涉及智能合约；第二类事务为用户调用单一智能合约，不涉及转移资金给其他用户；第三类事务为除第一类和第二类以外的其他事务。其中，前两类事务按照一定规则分配给普通分片处理，第三类交易在普通分片处理完第一类和第二类事务后由DS委员会处理。这种方式的问题在于，随着分片的增加，DS委员会将会面临越来越大的处理压力。

共识层扩容

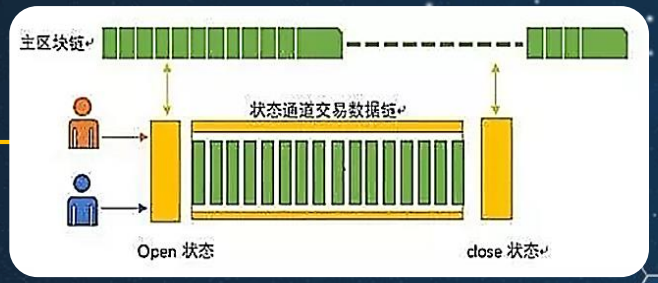
证明类共识。通过降低共识算法复杂度和减少传播节点数量等方式减少验证时间、传播时间及形成共识时间，能够显著提升处理效率。

- PoS（Proof of Stake，权益证明）。相比于PoW（Proof of Work，工作量证明），PoS以权益（持有通证数量×通证持有时间）代替算力决定区块记账权，减少了PoW工作量证明过程的能源消耗，在一定程度上解决了可扩展性问题。但是又带来了马太效应、记账激励、无利害关系攻击（Nothing-at-Stake attack）等新的问题。
- DPoS（Delegeted Proof of Stake，委托权益证明）。DPoS在PoS的基础上将记账人的角色专业化，通证持有人通过权益选出多个授权代表（EOS有21个“超级节点”，Bitshares有101位代表，理论上单数节点均可），授权代表轮流记账。这种共识下效率得到了明显提升，但是牺牲了非中心化。

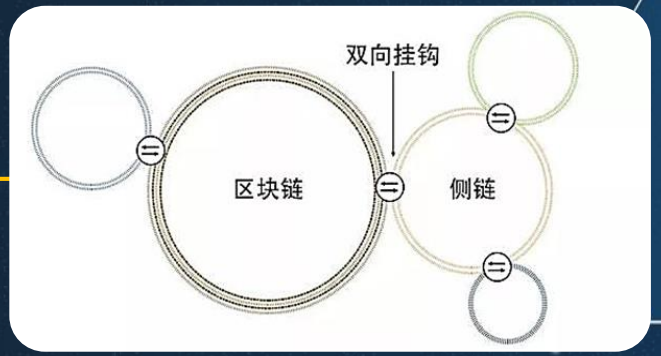
9.4 区块链扩容-第2层扩容方案（链下扩容方案）

链下扩容方案

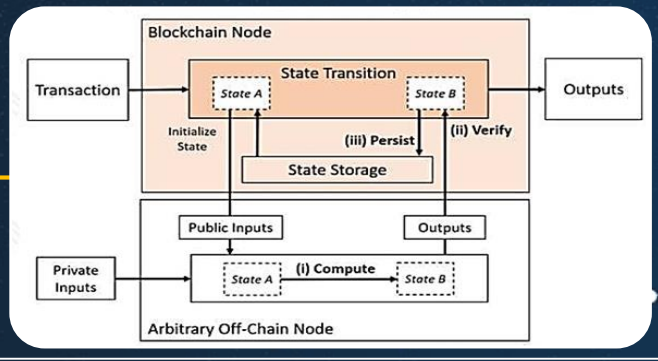
- 状态通道
- 侧链
- 链下计算



状态通道：建立通信双方间的私密双向通道，将大量交易下放到通道进行，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。

链下扩容方案主要有状态通道、侧链、链下计算三种方式，思路均为将部分链上交易转移到链下执行，减轻链上处理压力，提升整体效率。

状态通道-闪电网络（Lightning Network）

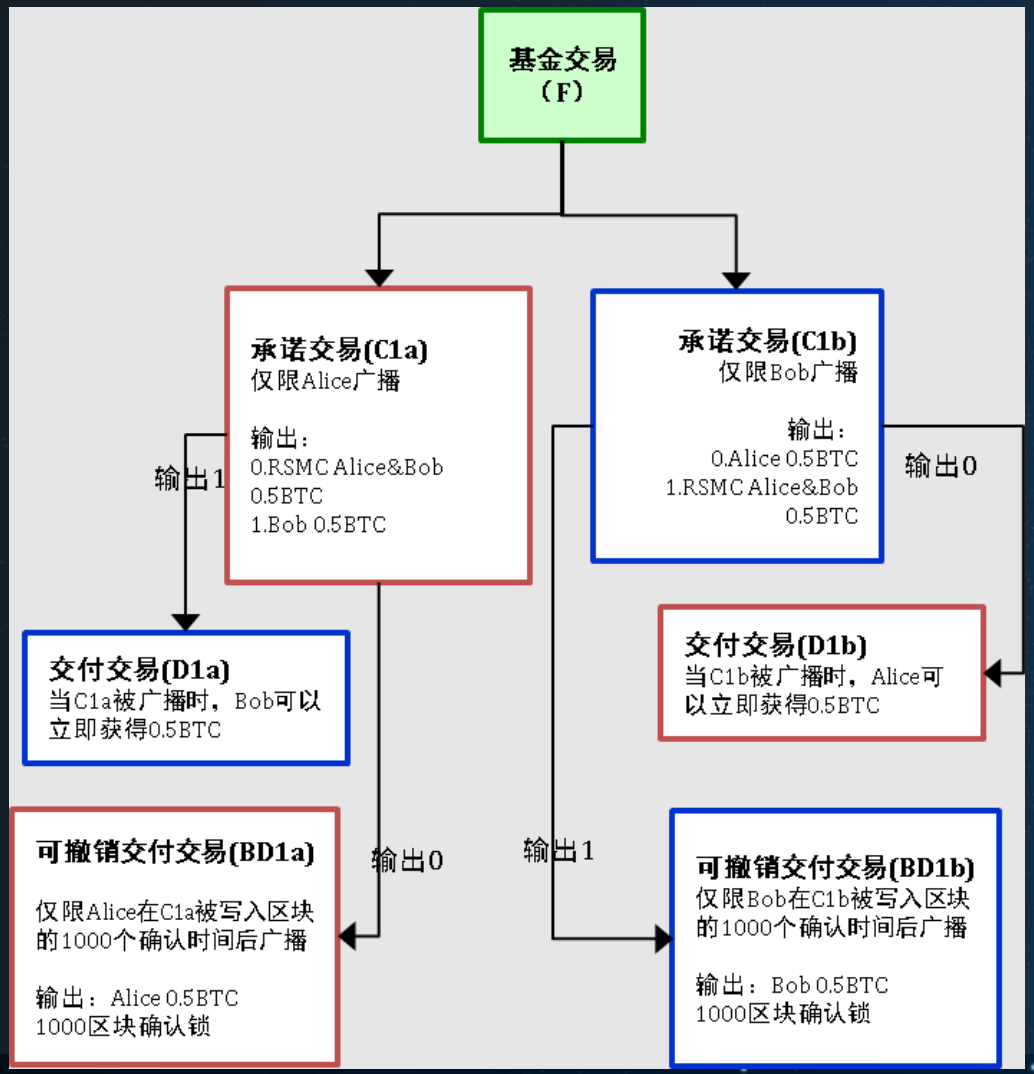
- 闪电网络的主要思路十分简单——将大量交易放到比特币区块链之外进行，只把关键环节放到链上进行确认。该设计最早于2015年2月在论文《The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments》中提出。
- 引入智能合约的思想，通过在链下建立交易方的微支付渠道（Micropayment Channels）网络，将小额交易带离比特币，从而促进比特币的交易吞吐量达到每秒百万笔。
  - 双向支付通道(Bidirectional Payment Channels)
  - 序列到期可撤销合约（Revocable Sequence 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)

状态通道-闪电网络

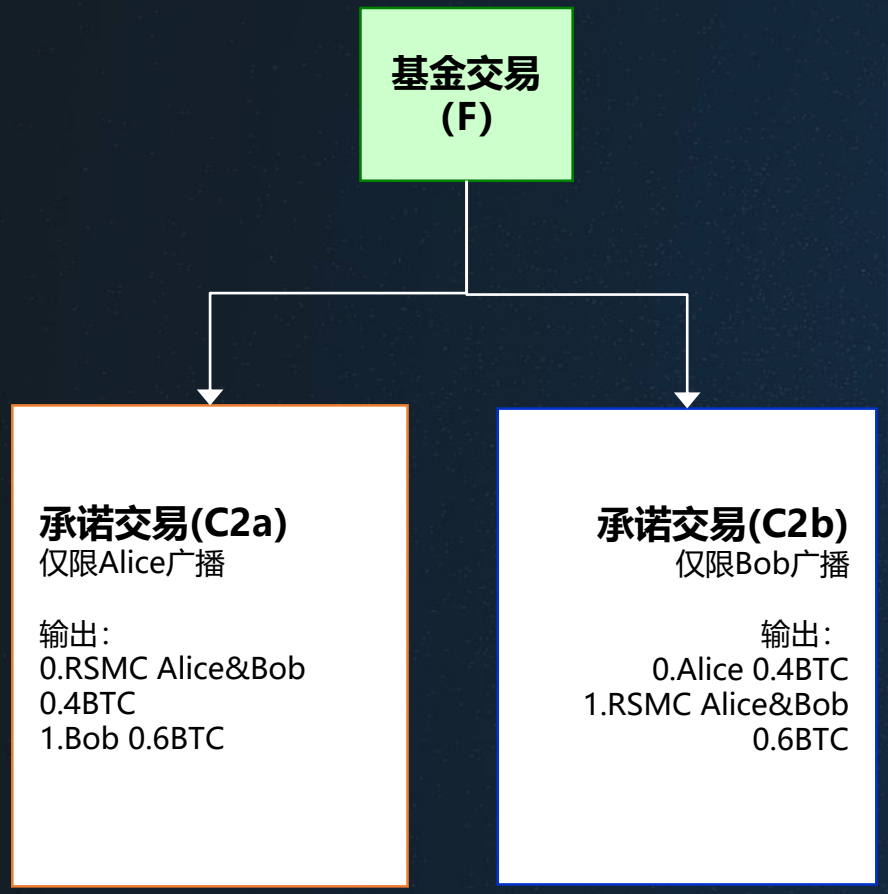
- RSMC（序列到期可撤销合约）的主要原理类似资金池机制。
  - 首先假定交易双方之间存在一个“微支付通道”（资金池）。交易双方先预存一部分资金到“微支付通道”里，初始情况下双方的分配方案等于预存的金额。
  - 每次发生交易，需要对交易后产生资金分配结果共同进行确认，同时签字把旧版本的分配方案作废掉。
  - 任何一方需要提现时，可以将其手里双方签署过的交易结果写到区块链网络中，从而被确认。在一定时间内，如果另外一方拿出证明表明这个方案其实之前被作废了（非最新的交易结果），则资金罚没给质疑方；否则按照提出方的结果进行分配。

状态通道-闪电网络-创建通道

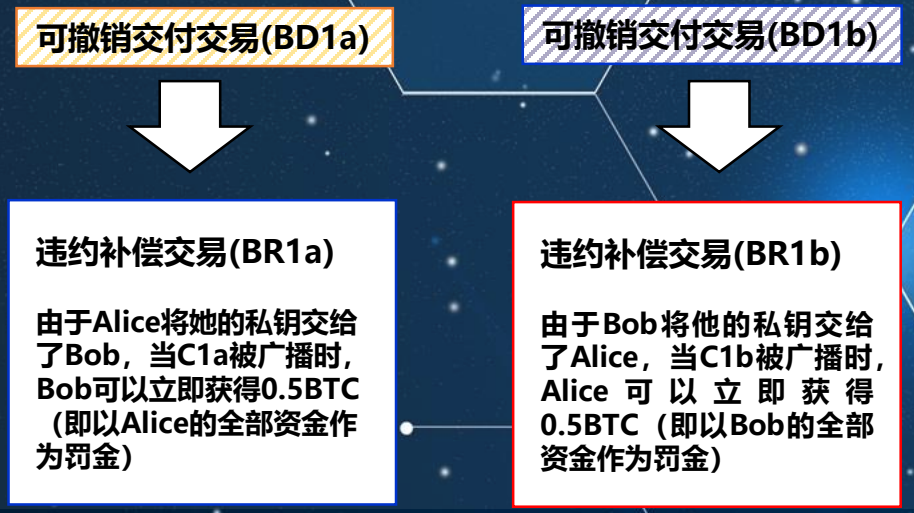


- Alice和Bob同意建立支付通道，双方各拿出0.5BTC用于创建基金交易(未签名)；
- Alice创建一笔初始的承诺交易C1b，该交易的输出为Alice:0.5BTC,Bob:0.5BTC，Alice对C1b签名后将该笔交易发送给Bob；
- Bob以同样的方式创建并签署C1a，并发送给Alice；
- 双方交换完毕后，就可以对基金交易进行签名，并在比特币系统中广播。

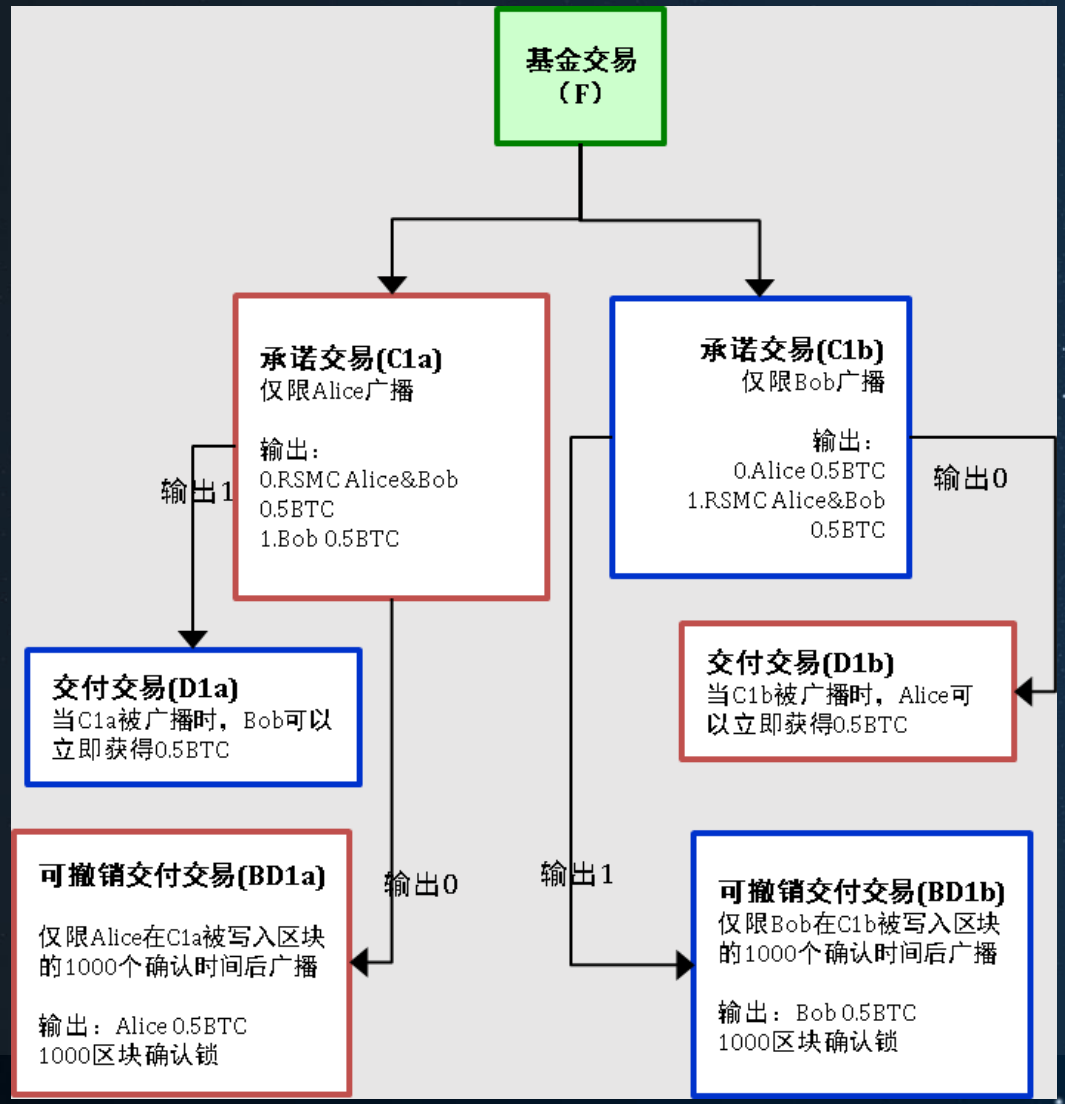
状态通道-闪电网络-交易方式



- 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



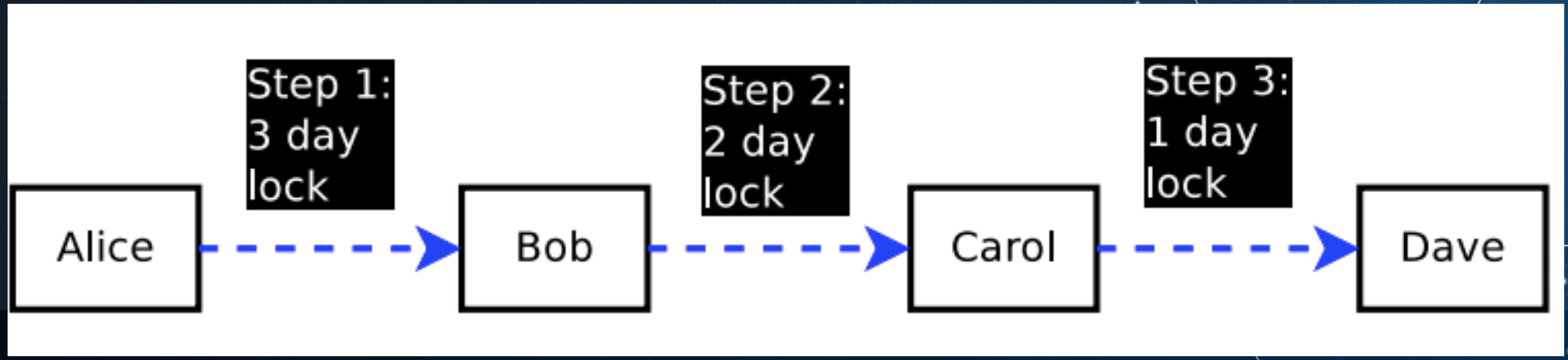
状态通道-闪电网络-关闭通道



- 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

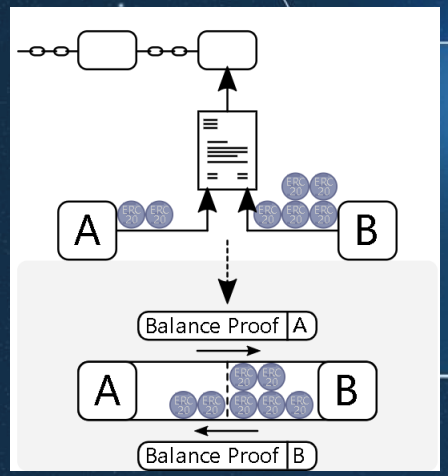
状态通道-闪电网络-HTLC

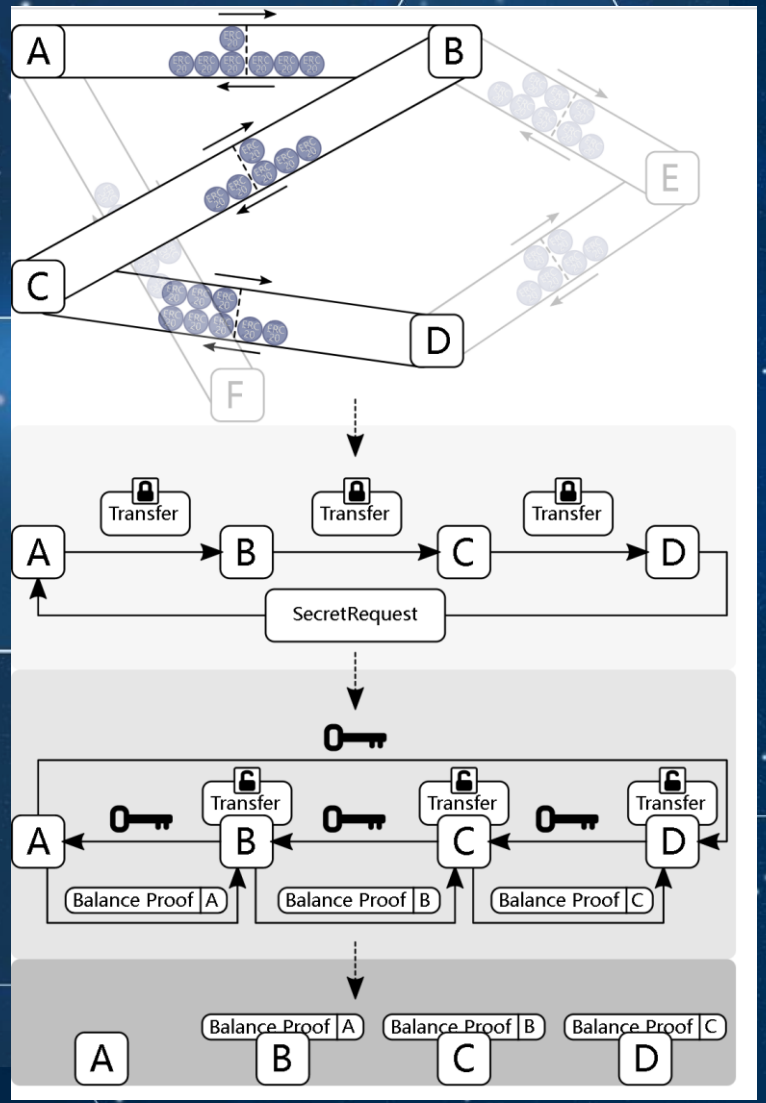
- HTLC（哈希时锁合约Hashed Timelock Contract) 就是限时转账。通过智能合约，双方约定转账方先冻结一笔钱，并提供一个哈希值，如果在一定时间内有人能提出一个字符串，使得它哈希后的值跟已知值匹配（实际上意味着转账方授权了接收方来提现），则这笔钱转给接收方。
- 基于RSMC，闪电网络实现了节点之间的直接支付通道，基于HTLC，闪电网络实现了节点之间的间接支付通道。
- HTLC的目的是通过哈希运算允许跨多个节点的全局状态。具体而言，它可以锁定一项交易，并以一个约定的时间（未来某个区块的高度）和承诺披露的知识作为解锁条件。



状态通道-雷电网络（Raiden Network）

- 雷电网络（Raiden Network）是状态通道技术在以太坊上的实现。雷电网络允许在参与者之间安全传输代币，而无需全球共识。这是通过使用数字签名和 散列锁定传输来实现的，称为余额证明
- Universal Payment Channels (Jehan Tremback and Zack Hess, 2015)



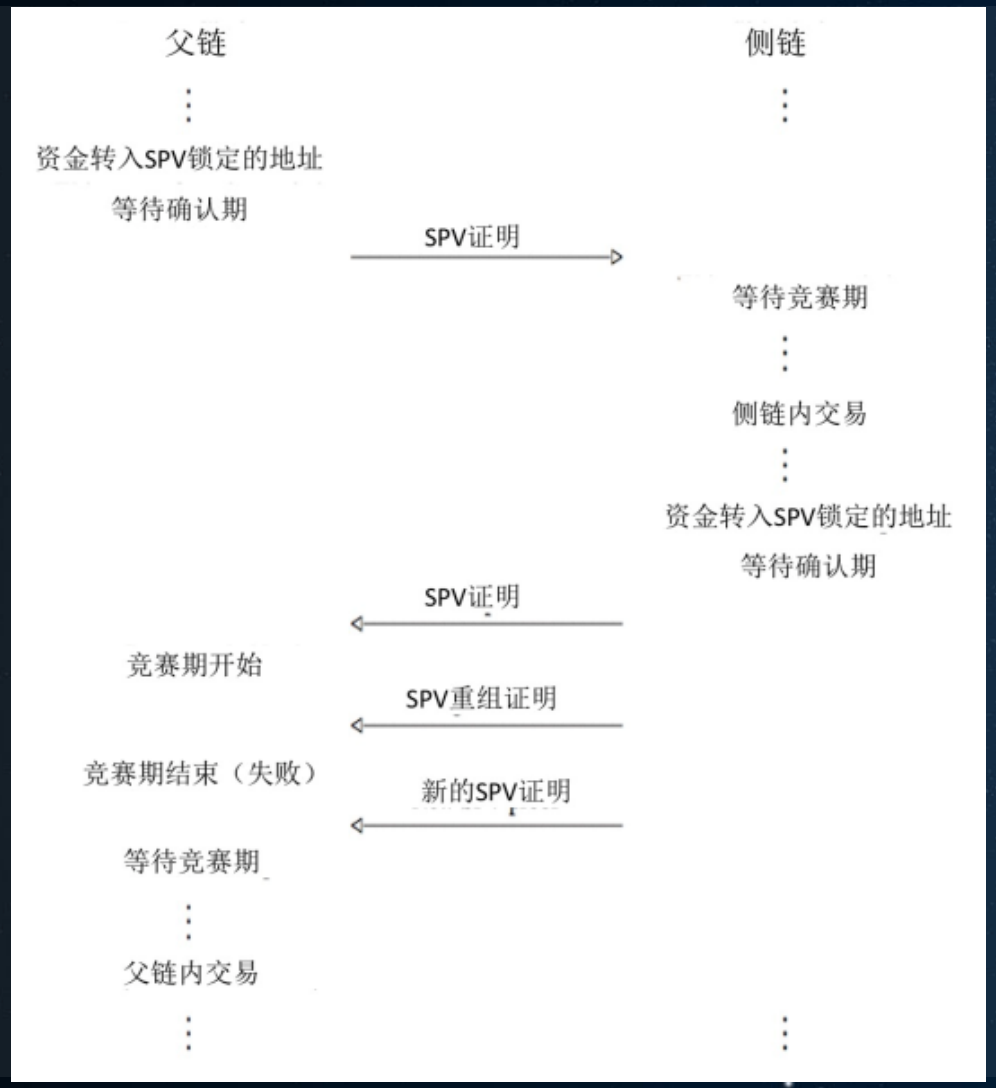


侧链-楔入式侧链技术(pegged sidechains)

- 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）

侧链



- 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

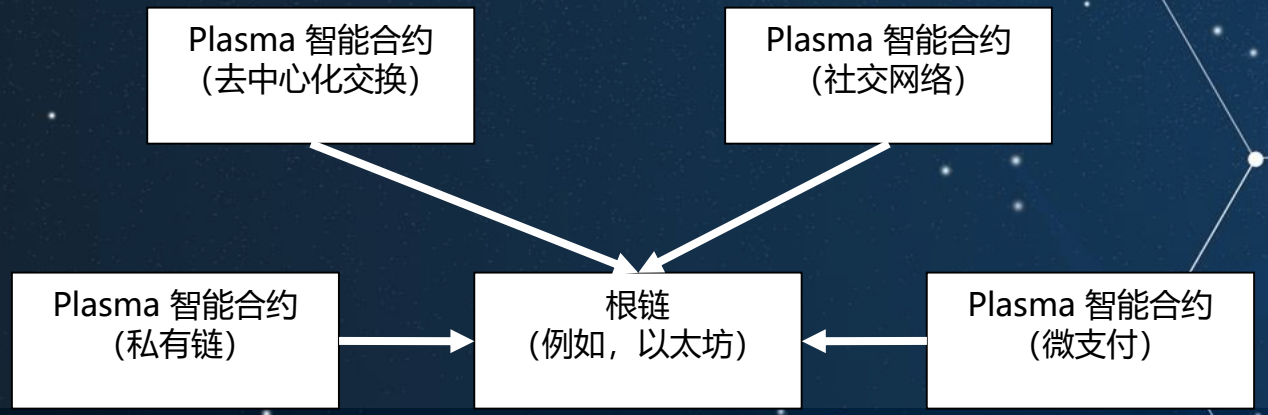
侧链-Plasma：可扩展的自主智能合约

- 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；
- Plasma是运行在根链（ETH主链）上的一系列智能合约。Plasma区块链为树状结构，每个分支为一条子链，一般情况下只将子链区块头的哈希值提交到根链，用于验证区块有效性。当有欺诈证明被提交到根链，区块会回滚并且惩罚区块创建者。由于根链只需要处理子链的少量提交，根链的交易负荷有效降低。

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



链下计算

- 链下计算最初针对ETH提出，由于ETH存在区块GasLimit，计算量较大的交易消耗gas较多将导致拥堵（比如单个区块只能打包一笔交易）甚至无法执行（单笔交易消耗gas超过区块GasLimit）。链下计算的思路是将复杂的交易放到链下执行，执行结果提交回链上，减轻链上处理压力。
- 以太坊声称要做计算机，EOS要做全球操作系统，但无论是做计算机还是做操作系统都得正视计算这个问题，链上计算的开销是非常大的，链上每一个EVM的合约计算都需要全球计算机算一遍。

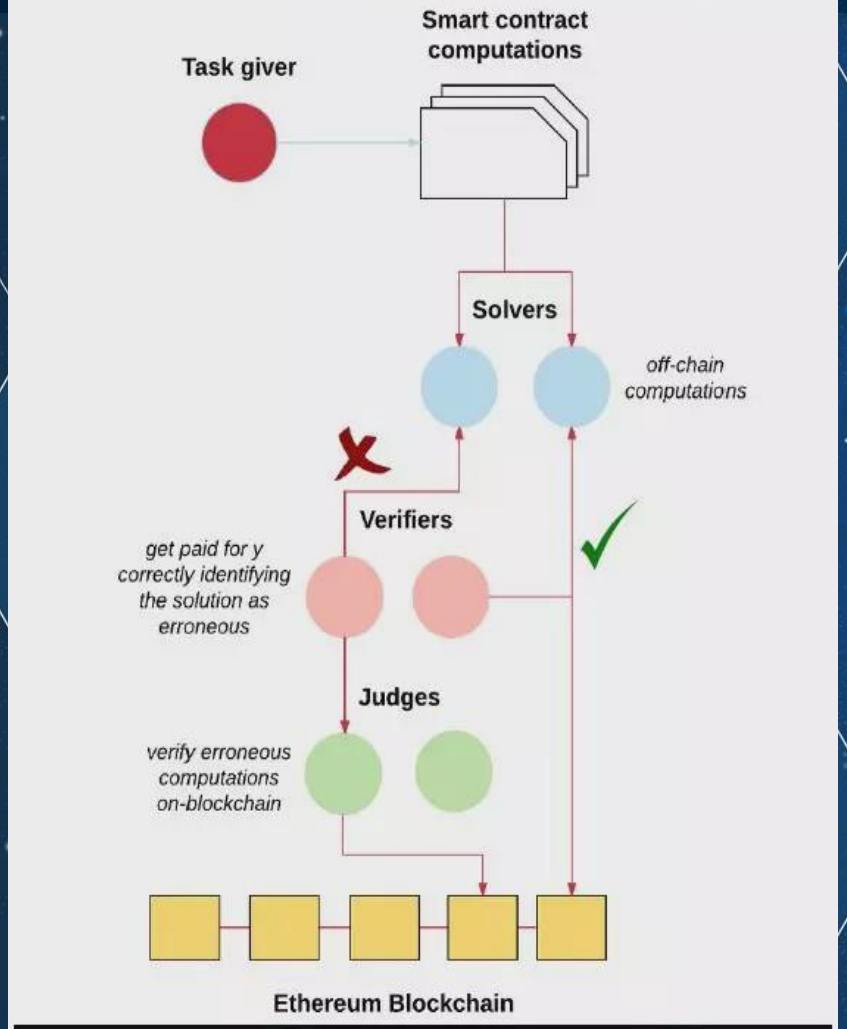
链下计算

- 第一种是在可信的执行的环境TEE（Trusted Execution Environment）中，把这个计算算出来，然后传到链上去，再加上可信环境的一个证明。这个证明不是计算结果的对和错，而是证明这个计算是在安全的环境里运行的。可信的执行环境在工业界相对来说还是比较成熟，苹果和安卓手机的指纹的秘钥信息都是存在TrustZone里面的。
- 优点：
  - 隐私性很强，因为所有东西都是在黑箱子里面的。
  - 性能也非常的高，单个机器执行即可，因为我信任的不是这台机器，而是这个 Trust Zone。
  - 功能非常的灵活。
- 缺点：
  - 黑箱计算引入了未知的风险。
  - 依赖于硬件限制了它的扩展性，因为不可能每个人都有一个符合硬件要求的设备来运行这套系统。
  - 系统的安全性是依赖于厂商的，厂商是可以在Trustware里面做任何的事情，这个也引入了风险。
- 所以这种依赖于安全执行环境的Layer 2方案一般是由联盟链或者是企业内部的链来使用的。

链下计算

- 另一种以Truebit为例，Truebit由求解游戏和验证游戏构成。
- 求解游戏中，求解者执行智能合约的计算，同时提交押金和问题结果，如果正确，返还押金并获得奖励，如果求解者欺诈，押金将被没收。
- 是否存在欺诈通过验证游戏解决。验证者在链下对求解者的工作进行检查，如果没有验证者发出质疑，系统将会接受结果，如果出现质疑，由裁判在链上裁定质疑，链上裁定的工作量与链下执行任务的工作量相比微不足道。如果确实存在欺诈，则没收欺诈者的押金，如果不存在欺诈，质疑者将为误报消耗的资源支付一定的费用。

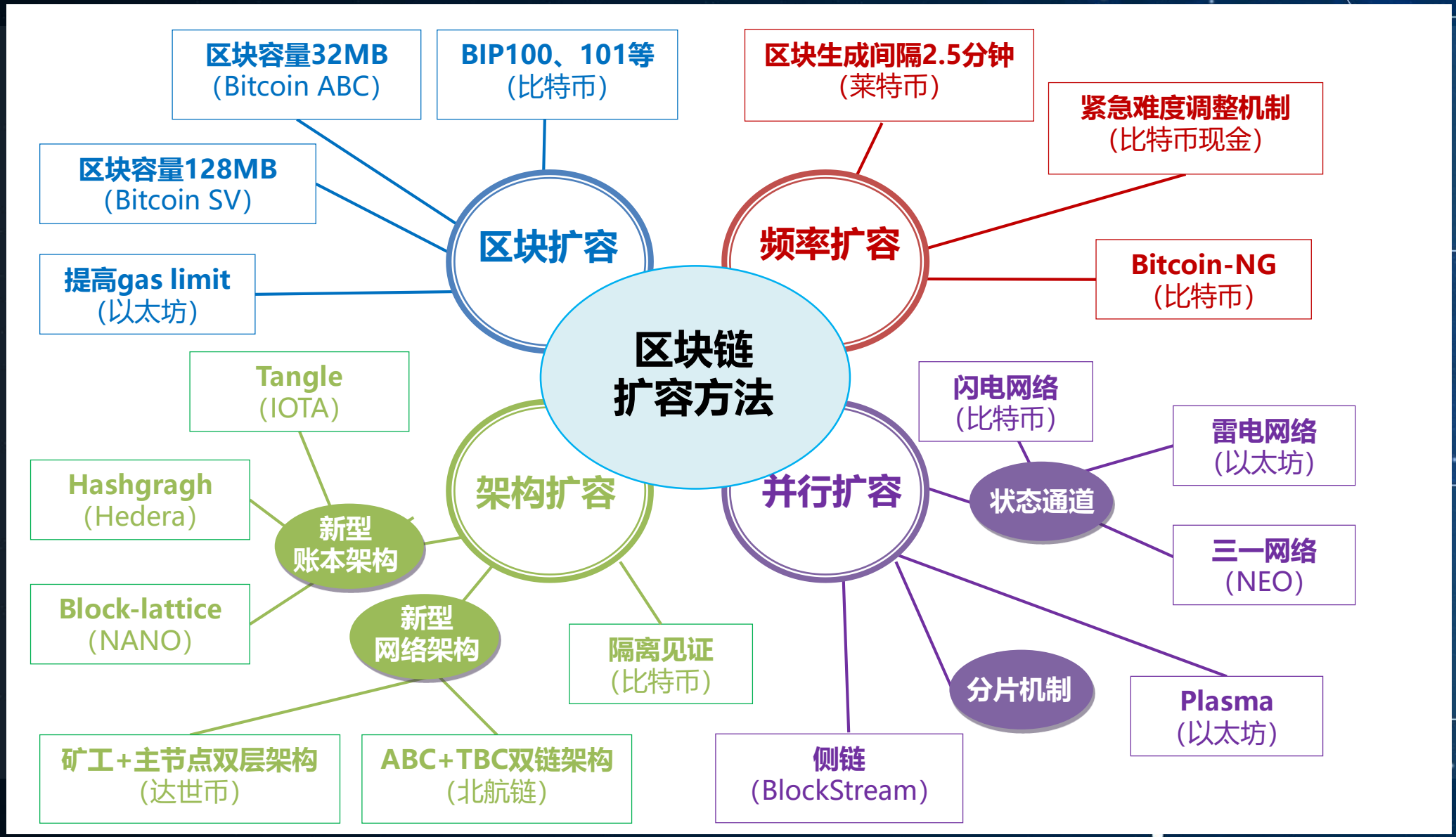
图表17：Truebit 链下计算示意图



资料来源：Off-Chain Computation Solutions for Ethereum Developers，通证通研究院

区块链扩容-区块链存储扩容

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!