区块链扩容技术

北京交通大学
计算机与信息技术学院
信息安全系

李超 (li.chao@bjtu.edu.cn)
段莉 (duanli@bjtu.edu.cn)

目录 | CONTENT

区块链拥堵与扩容技术

拥堵的区块链

- 区块链技术使得任何用户可以在**不需要第三方信任机构**的情况下建立信任关系。
- 这样的信任关系源于用户对整个系统的信任，而无需信任单个节点，这样的技术特性将对组织间协作关系、各领域商业模式带来极大变革，然而当前的区块链系统普遍存在严重的性能可扩展性瓶颈：**交易吞吐量不足**。

拥堵的区块链

- 当前比特币（Bitcoin，BTC）区块链系统每 10 min 左右产生一个区块，理论上只能支持 **7 笔 /s** 的交易确认。
- 以太坊区块链最高支持**15笔 /s** 的交易确认，这样的系统性能距离 Visa 卡几万、支付宝几十万的吞吐量相差甚远。
- 因此，区块链系统性能在面对绝大部分业务场景（尤以高频交易为甚）都难以满足实际应用需求。

区块链性能限制

- 区块链的分布式技术架构能够保证数据不易篡改，便于创造可信执行环境，也因分布式共识机制使得区块链系统实现数据一致性所用时间大大增加，而这正是影响区块链网络性能的**技术瓶颈所在**。
- 分布式共识是经典的技术难题，学术界和业界都已有较多的研究成果，如 Paxos、PBFT等，问题的核心在于如何解决在分布式网络中数据状态变更能够得到**一致的、多方承认的、确定的、不可推翻的结果**。

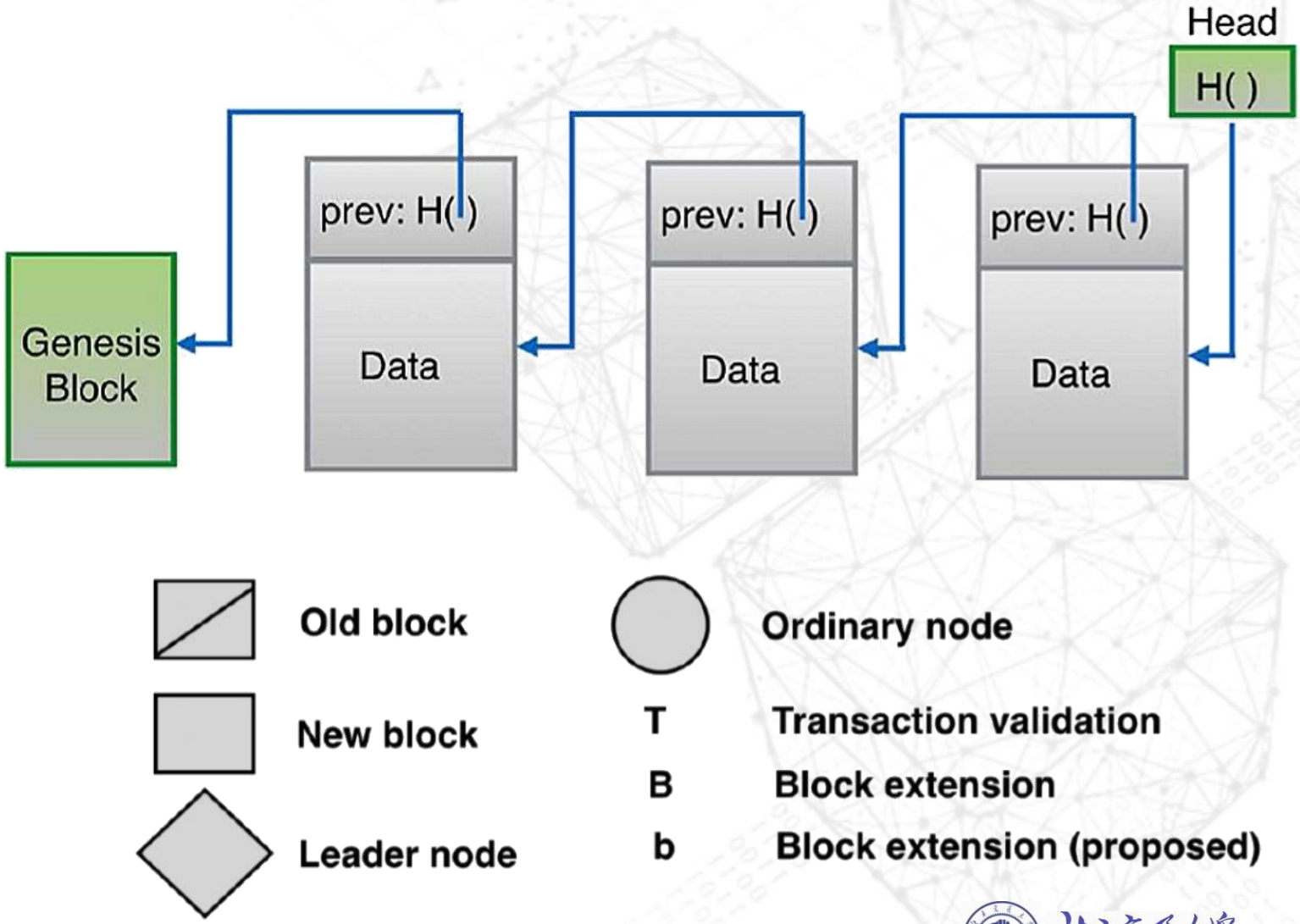
区块链性能限制

- 传统分布式系统中一直存在 CAP理论，系统最多只能满足**数据一致性、可用性和网络分区**容忍 3 个 特性中的 2 个。
- 区块链继承了分布式系统架构，同样存在类似的三元悖论，即**性能扩展、去中心化和安全性**这 3 个特性不能同时得到满足，现有区块链系统就是选择牺牲性能，以保证交易记录的多方可信与安全存储。

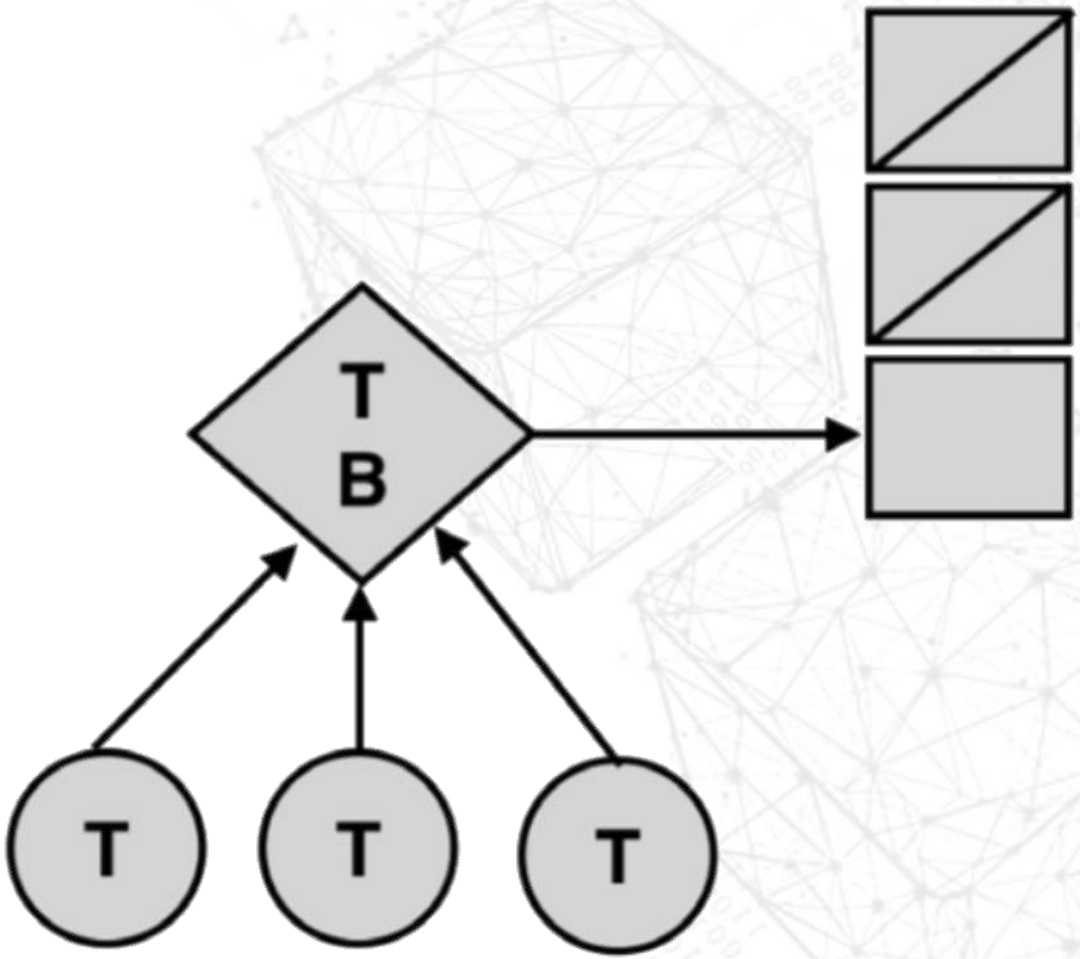
区块链性能限制

- 对区块链系统进行性能扩展时，需要综合考量**去中心化和安全性**。
- 传统分布式系统通过增加节点数量来提升系统吞吐量的方法不但不能提高区块链系统处理数据交互的速度，反而会**降低**共识效率，导致系统性能进一步下降。
- 所以，需要开展针对区块链系统的性能提升研究，即**区块链扩容技术**。

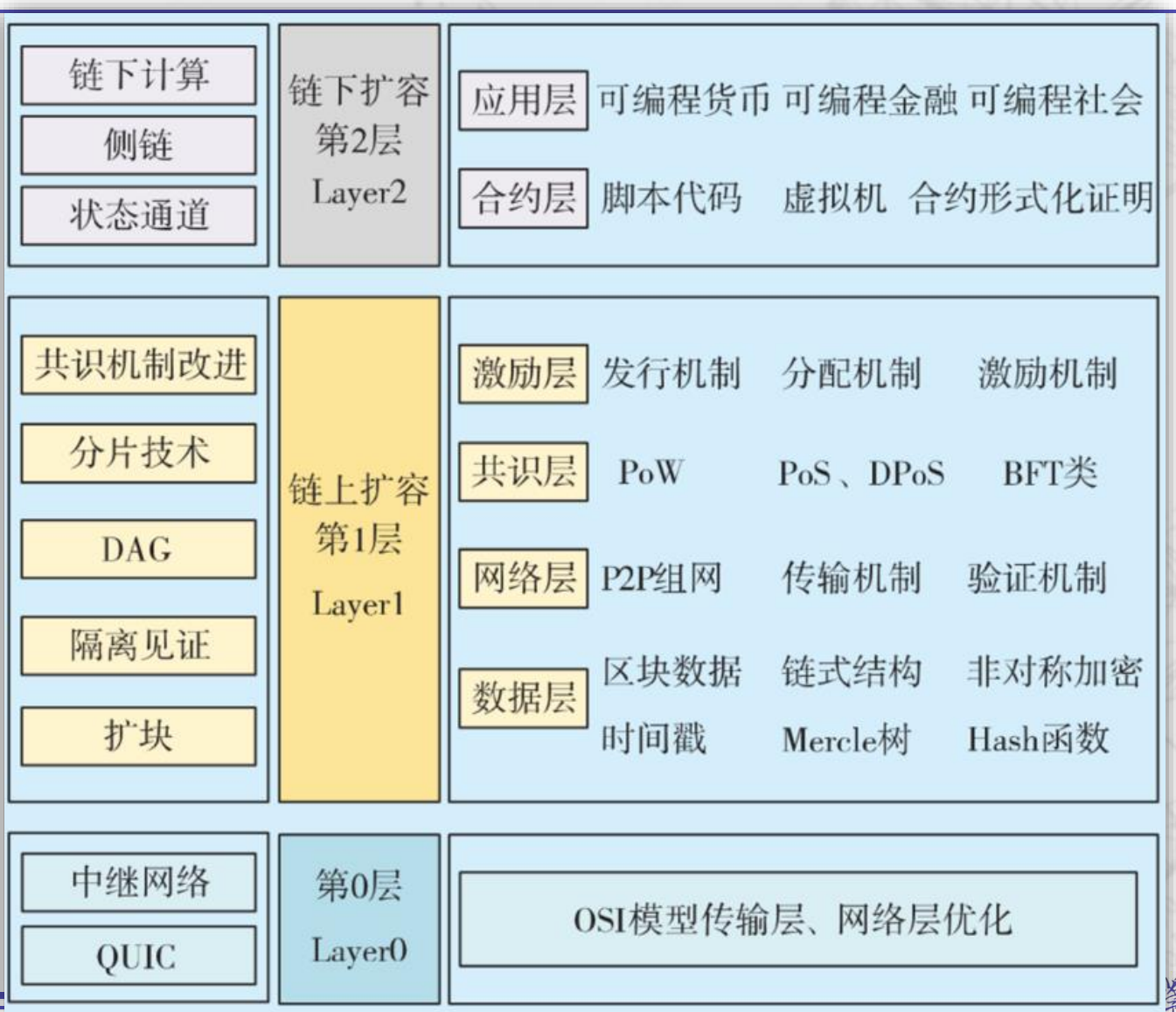
比特币区块链模型化


Head
H( )
prev: H( )
prev: H( )
prev: H( )
Genesis Block
Data
Data
Data
Old block
New block
Leader node
Ordinary node
T
Transaction validation
B
Block extension
b
Block extension (proposed)

比特币区块链模型化



区块链扩容技术分层概览



链上扩容

链上扩充5种，链下扩容3种。

链上和链下扩充的区别：
1.链上 动房子
2.链下 动房子的前后左右

链上扩容

- 链上扩容方案是针对区块链自身的基本协议、 体系结构进行修改优化，达到扩容效果，提升系统性能。
- 链上扩容主要有数据层扩容、网络层扩容、共识层扩容方案。

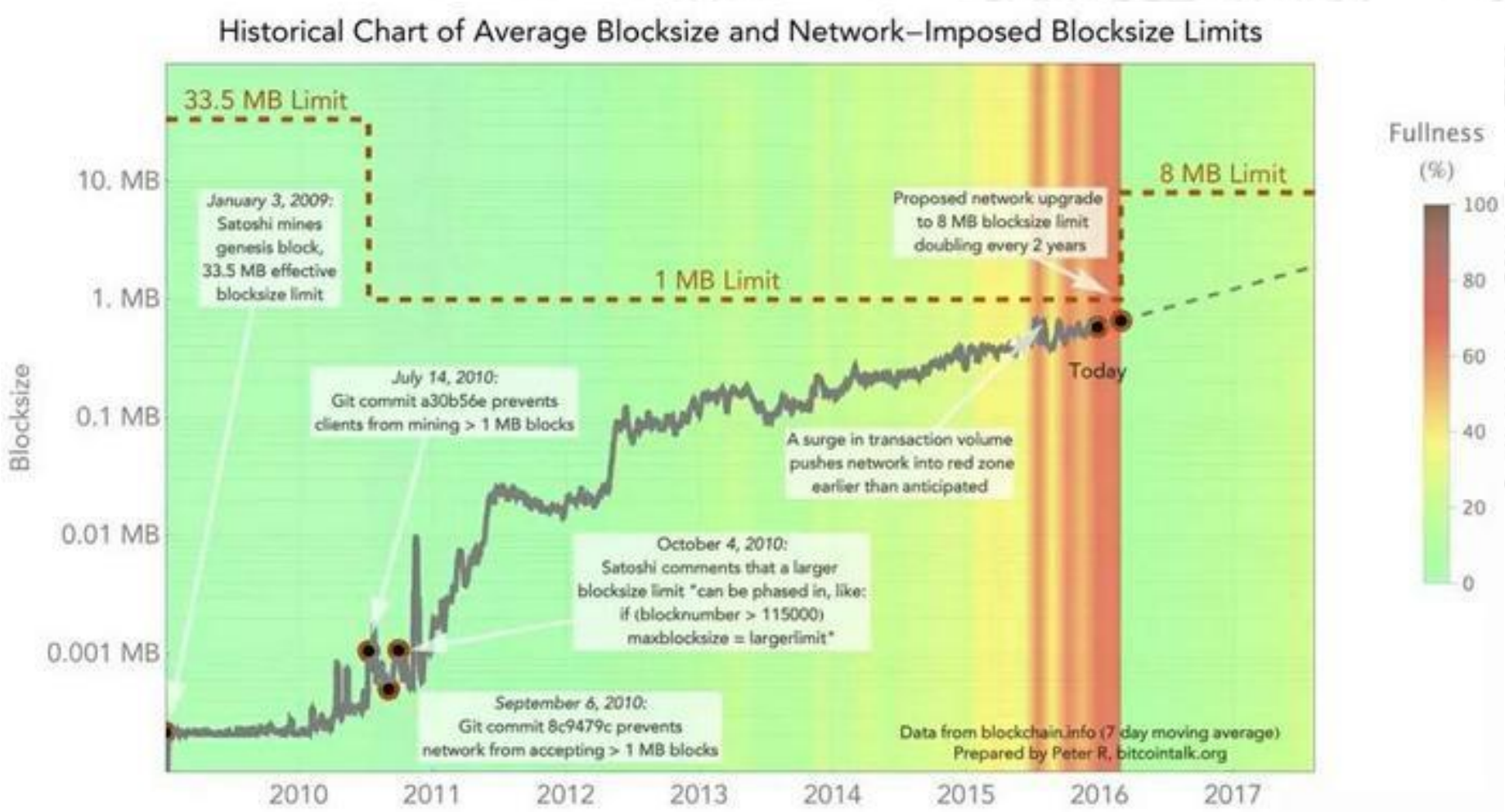
数据层扩容

- 数据层扩容主要是**对数据区块进行修改**，**增加区块容纳交易的数量**，根据修改方式的不同，目前主要有三种技术路线：
  - 扩块
  - **隔离见证**
  - 有向无环图（Directed Acyclic Graph，DAG）

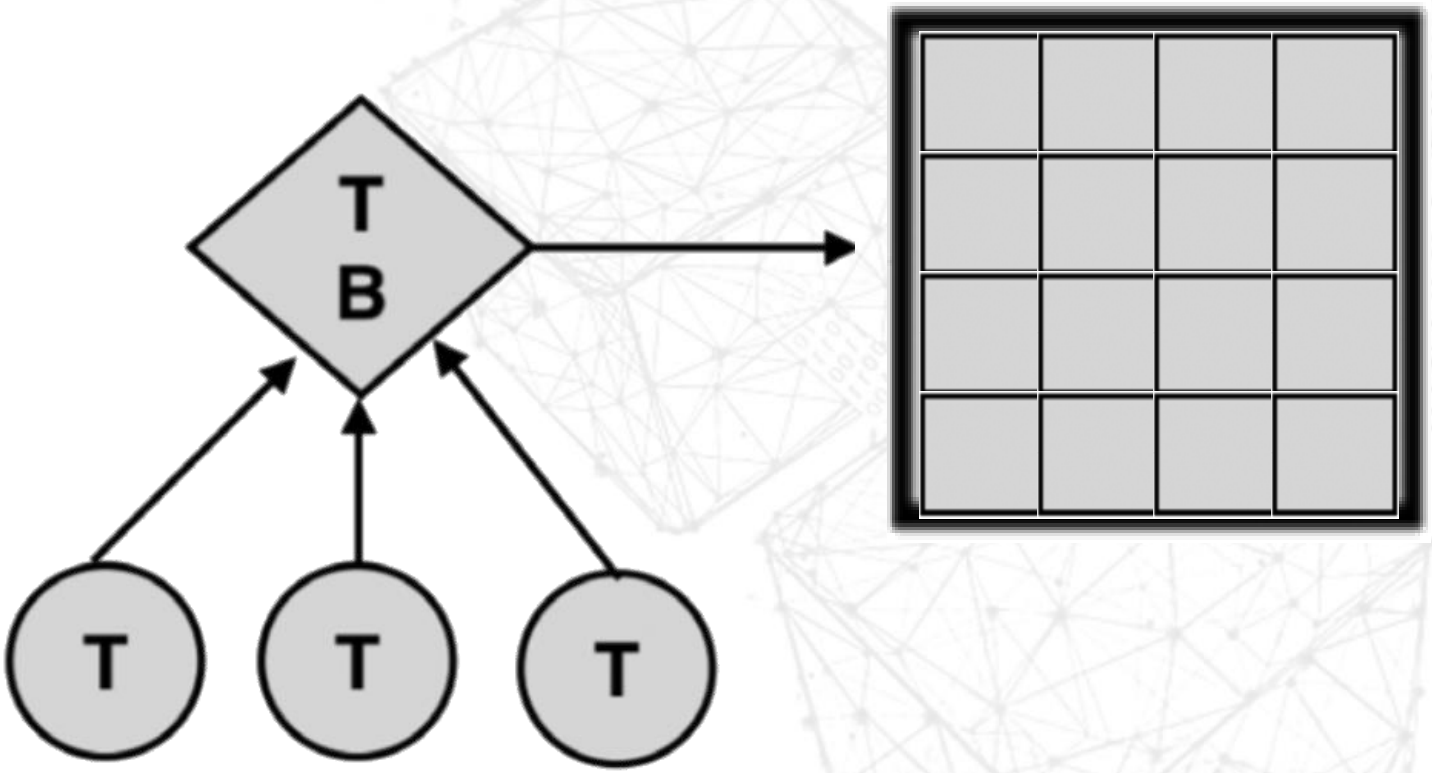
扩块

- 扩块即**扩大区块的容量**，从而增加数据区块能够打包的交易数量，提升吞吐量。
  - 例如，从比特币分叉出来的比特现金（Bitcoin Cash， BCH）就从原来的1 MB区块，先后扩至 8 MB、32 MB。
- 增加区块大小的这种方法**最简单、直接、易实现**，但是区块的大小**不能无节制随意扩大**
  - 区块容量增加对节点处理能力要求也相应提高，容易导致**算力中心化**问题；
  - 同时也会增大区块在网络中传输的**延迟**，更容易受到外部攻击。

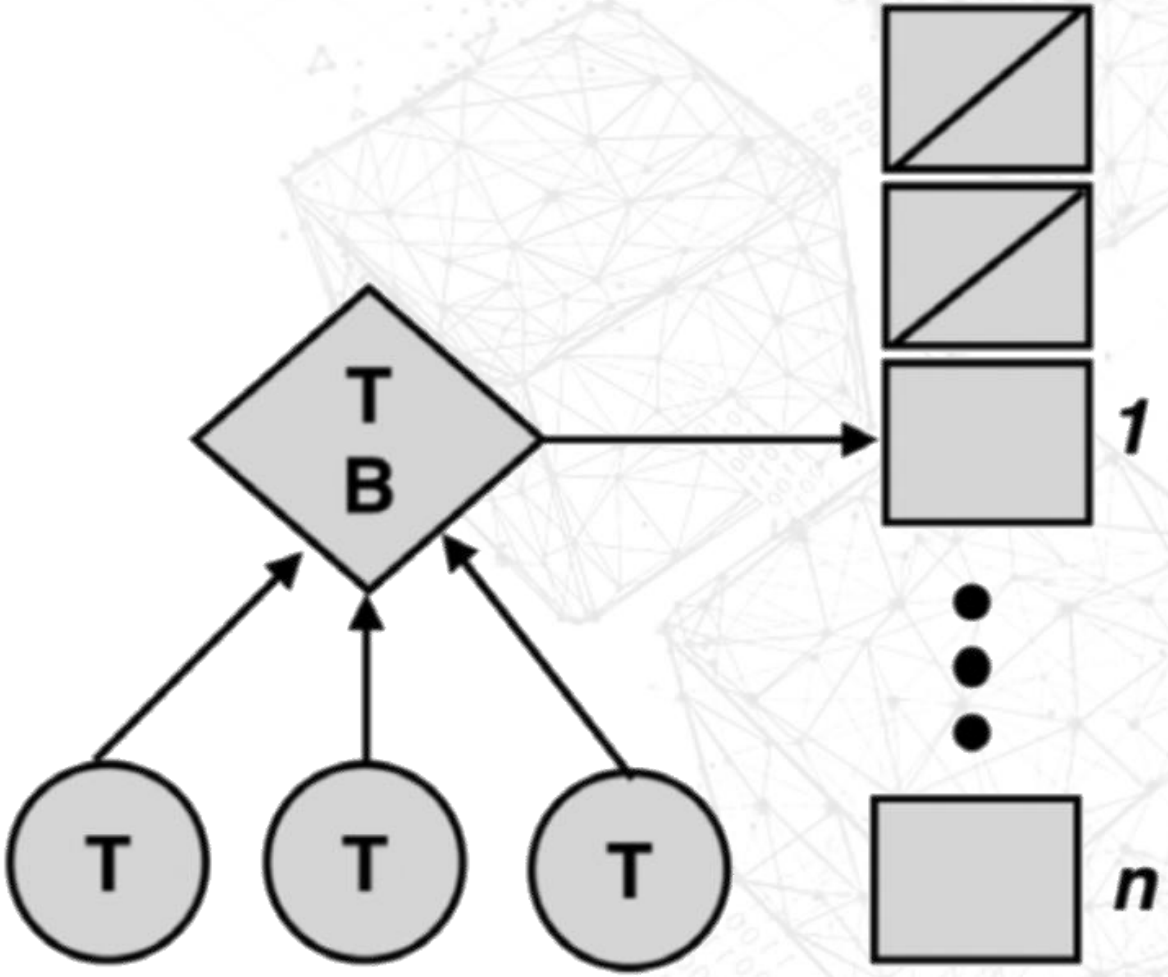
交易率变化、区块容量变化



扩块



扩成块数量



隔离见证

- 隔离见证主要思想是将原本存放在区块中的**交易签名提取**出来，放到外部
- 这样交易区块内部就能存放更多的交易记录，间接达到扩容目的

隔离见证

- 数据区块包括数字签名和其他交易信息，其中**数字签名便占用了区块大部分空间**
- 数字签名仅仅在验证阶段需要，将数字签名“**隔离**”出区块，节省数据区块空间，提升单个区块所能容纳的交易数量，变相扩大区块大小
- 隔离见证最初不是针对区块扩容而提出，而是针对交易签名篡改攻击而提出的比特币区块链结构改进方案，但间接达到了扩容的效果

隔离见证

```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe
9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL]
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c
04f4938de5cc17b4a10fa336a8d752adf",
    "sequence": 4294967295
  }
]
```

```
"vout": [
   {
     "value": 0.10000000,
     "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY
OP_CHECKSIG"
   }
 ]
```

隔离见证

- 隔离见证（segwit）是一次比特币共识规则和网络协议的升级，其提议和实施基于BIP-9 软分叉方案。

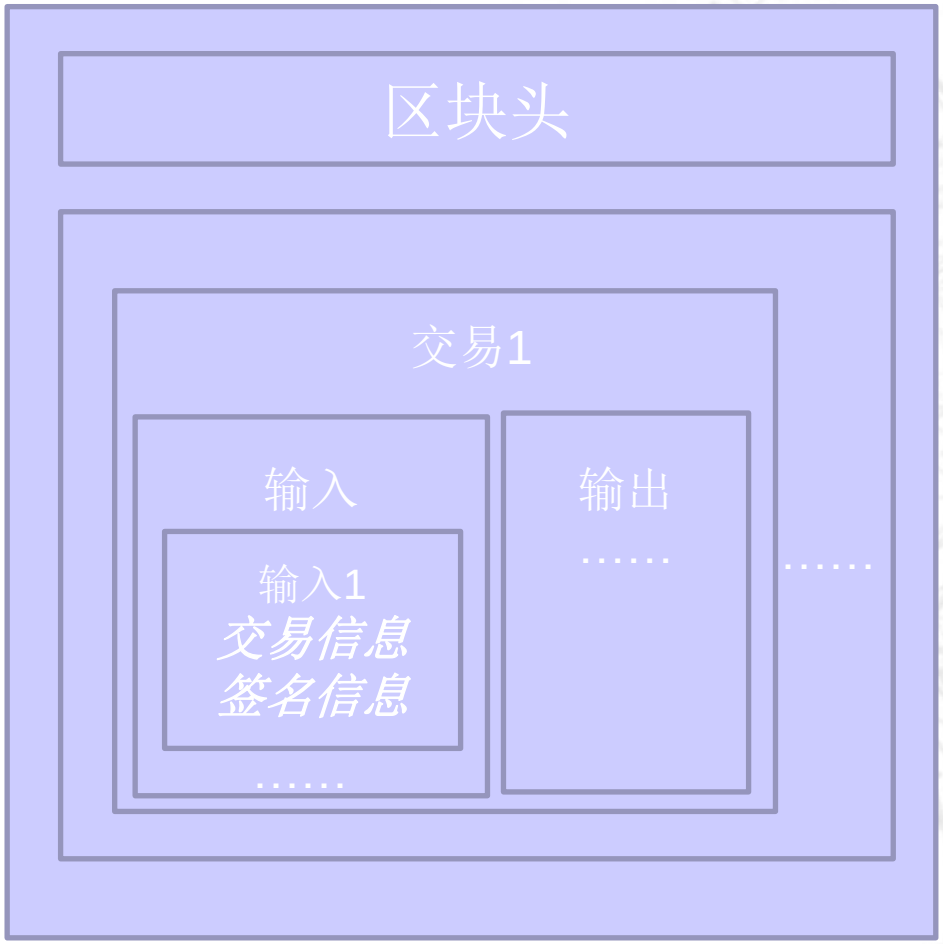
- 在密码学中，术语“见证”（witness）被用于形容一个加密难题的解决方案。在比特币中，“见证”**满足了**一种被放置在未使用的交易输出（UTXO）上的加密条件。

- 在比特币语境中，**一个数字签名就是一种类型的“见证”**。但“见证”是一个更为广泛的任意解决方案，能够满足加诸于一个UTXO的条件，使UTXO解锁后可被花费。术语“见证”一词是一个更普遍用于**“解锁脚本”（或scriptSig）**的术语。

隔离见证

- 在引入“隔离见证”之前，每一个交易输入后面都跟着用来对其解锁的见证数据，见证数据作为输入的一部分被内嵌其中。
- 术语“隔离见证”（segregated witness），或简称为“segwit”，简单理解就是将某个特定输出的签名分离开，或将某个特定输入的脚本进行解锁。用最简单的形式来理解就是**“分离解锁脚本”（separate scriptSig）**，或**“分离签名”（separate signature）**。
- 因此，隔离见证就是比特币的一种结构性调整，旨在将见证数据部分从一笔交易的scriptSig（解锁脚本）字段移出至一个伴随交易的单独的见证数据结构。客户端请求交易数据时可以选择要或不要该部分伴随的见证数据。

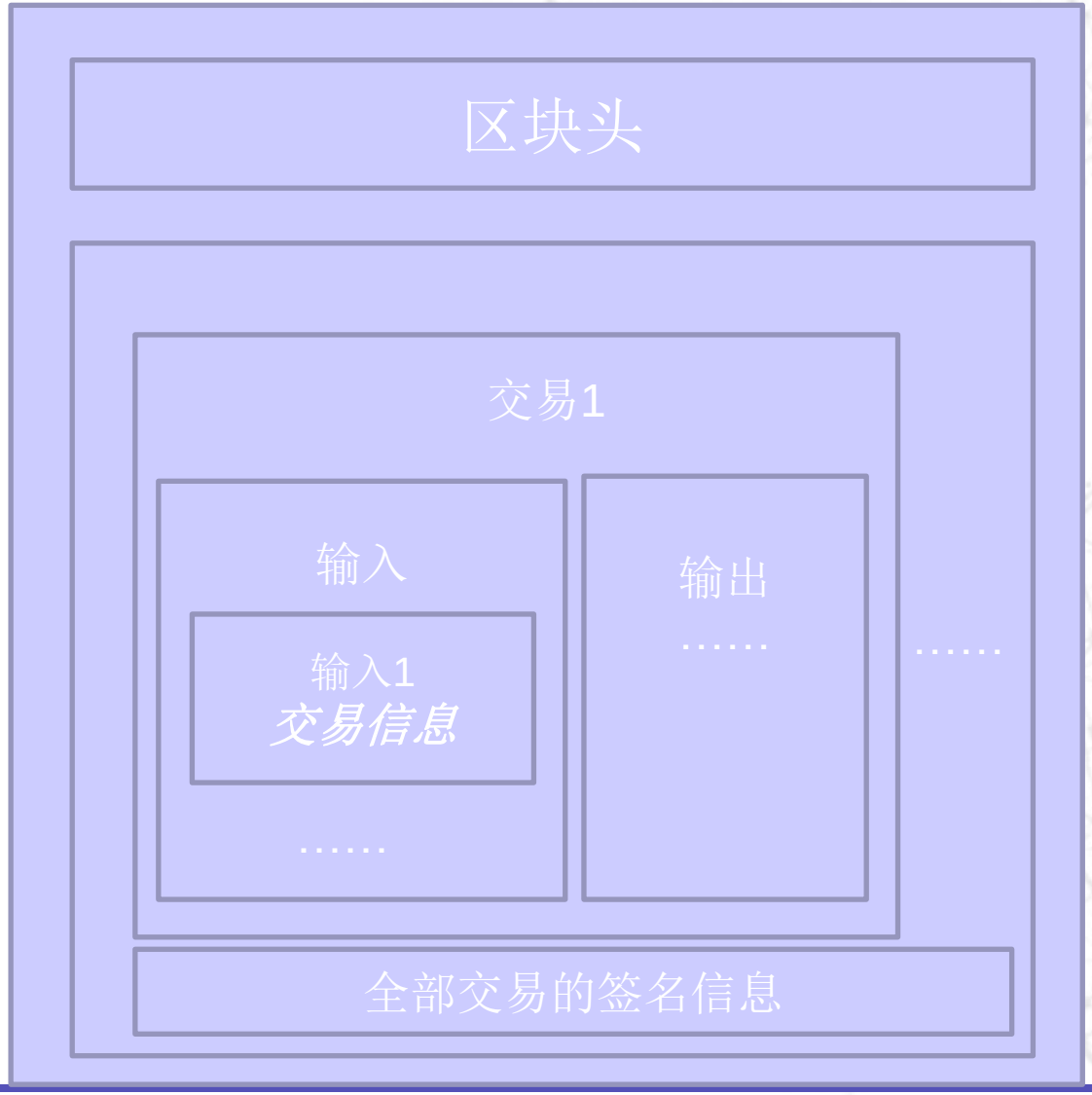
隔离见证



比特币区块结构

每笔交易平均 250 字节，签名信息的数据约为 150 字节，其余部分 100 字节。

隔离见证



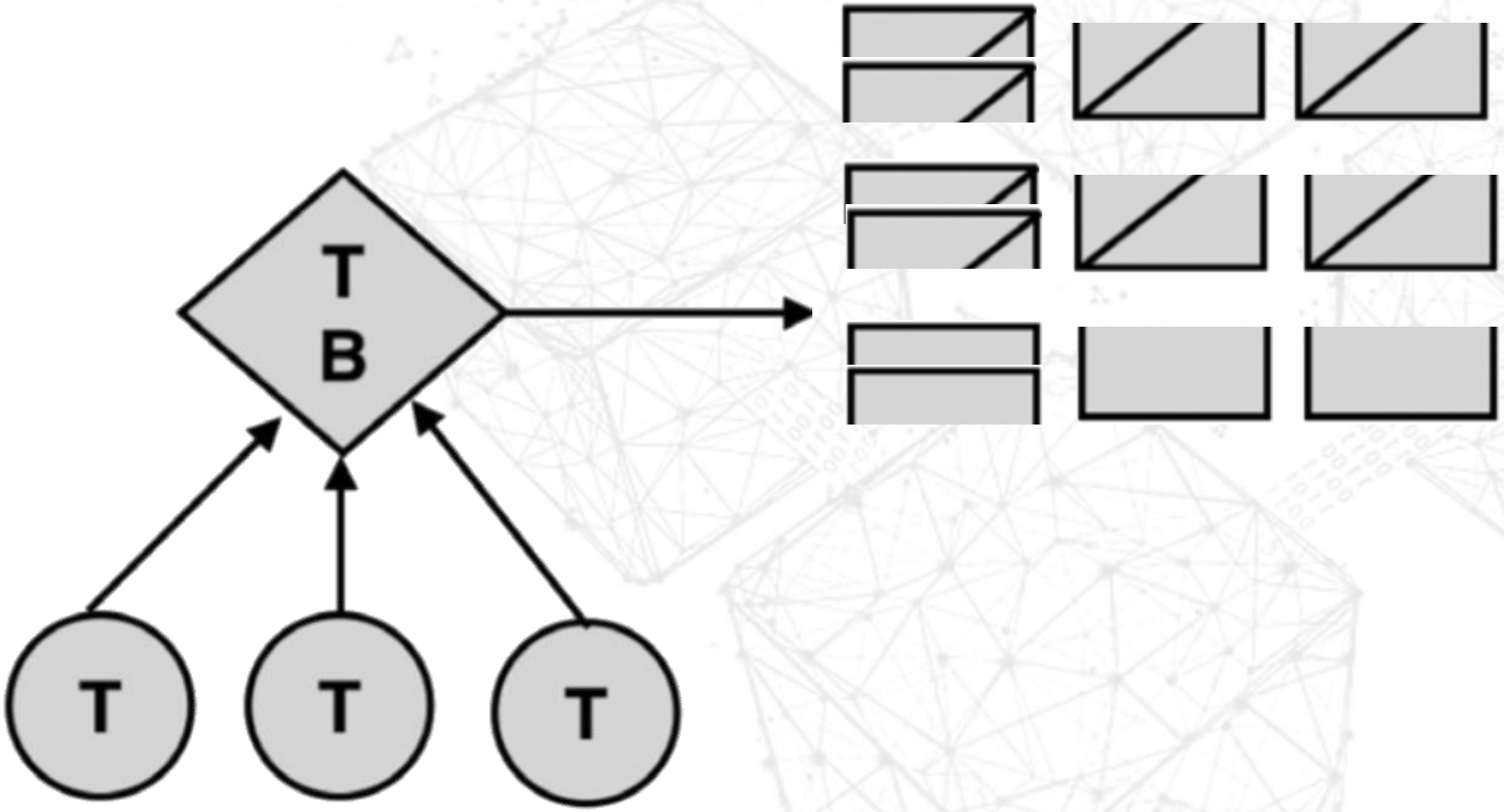
隔离见证后
比特币区块结构

- 验证交易时签名信息同样会被验证。
- 签名信息依然在区块中。

1M限制突破

- 那么这时候你可能会疑问，比特币不是规定区块大小是1M嘛，你这样做只是改变了下数据结构，把见证信息挪了个地方，然后又加了新的交易信息，那肯定超过1M。
- 超过1MB大小的区块，对于老节点来说不是非标准交易，而是非法交易。为了解决这一问题，SegWit将**欺骗老节点**的伎俩发挥到了极致。它将整个Witness的部分放在原来整个block的外面。对于老节点来说它并不知道它接收的整个block后面还有一个witness的结构。
- 这样就解决了1M限制的问题。也就是**主区块仍然是1M，而见证信息放到了3M的见证区块里**。
- 所以你看，隔离见证**其实并没有直接扩展区块的大小**，只是通过一种分离部分数据，然后改变交易数据计算方式，而达成的**变相扩容方案**。

隔离见证

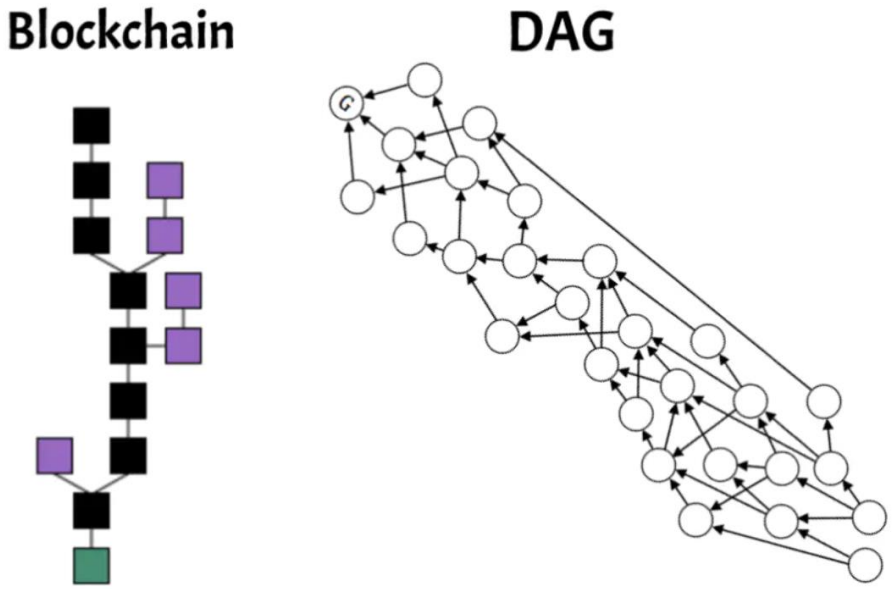


有向无环图（DAG）

看看红字

- 有向无环图（DAG）是一种使用拓扑排序的有向图形数据结构，**改变了区块链的块链式线性存储结构**
- 在 DAG 中，**每一笔新的交易都可以单独作为一个“区块”提交“共识”**
- DAG 的共识机制也不再是传统的广播数据验证，而是根据规则传递前一区块的 hash 值，数据的记录存储可以是**并行**的，打破了块链式串行存储结构，从而提升区块链网络的吞吐量

DAG



- 传统区块来讲，我们总是**以“区块”为单位**，一个区块里往往包含了多笔交易信息。而在DAG中，没有区块的概念，而是**以“单元”为单位，每个单元记录的是单个用户的交易，组成的单元不是区块，而是一笔笔的交易**，这样一来，可以省去打包出块的时间。
- 简单来说，区块链和DAG有向无环图最大的区别就是：区块链是一个接一个的区块来存储和验证交易的分布式账本，而**DAG则是把每笔交易都看成一个区块，每一笔交易都可以链接到多个先前的交易来进行验证**。

DAG

- 对于DAG来讲，**每个新加入的单元，不仅只加入到最长链的一个单元，还要加入到之前所有的单元**。
- 举个例子：假设Alice发布了一个新的交易，此时DAG结构已经有2个有效的交易单元，那么Alice的交易单元会主动同时链接到前面的2个之中，去验证并确认，直到链接到创世单元，而且，上一个单元的哈希会包含到自己的单元里面。
- 换句话说， Alice**要想进行一笔交易，就必须要验证前面的交易**，具体验证几个交易，根据不同的规则来进行。这种验证手段，使得DAG可以异步并发的写入很多交易，并最终构成一种拓扑的树状结构，极大地提高扩展性。

DAG

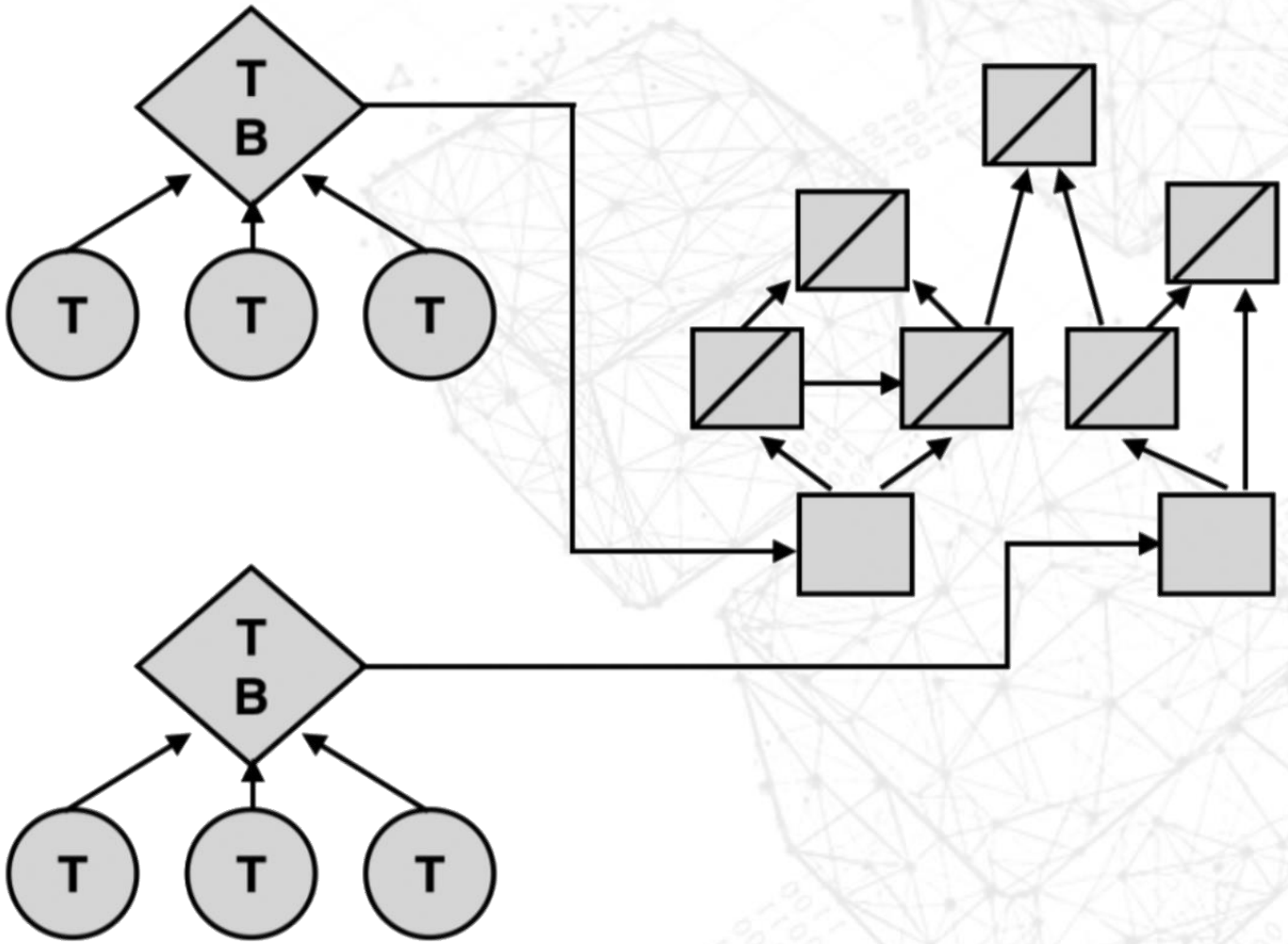
- 区块链组成单元是Block（区块），DAG**组成单元是TX（交易）**。
- 区块链是单线程，DAG是**多线程**。
- 区块链所有交易记录记在同一个区块中，DAG**每笔交易单独记录在每笔交易中**。
- 区块链需要矿工，**DAG不需要矿工**。

IOTA

- DAG的代表项目，最知名的无疑就是 IOTA。可以说，正是因为IOTA这个币种在2017年下半年冲进市值排行第四位，才使人们真正认识到了它的底层技术：DAG有向无环图。

- IOTA在DAG有向无环图的基础上提出了**“缠结”概念**，在IOTA里面，没有区块的概念，共识的最小单位是交易。**每一个交易都会引用过去的两条交易记录哈希，这样前一交易会证明过去两条交易的合法性，间接证明之前所有交易的合法性。**这样一来， 就**不再需要传统区块链中的矿工**这样少量节点来验证交易、打包区块，从而提升效率，节省交易费用。

有向无环图



网络层扩容方案：分片

- 当前网络层扩容方案的思想主要是以太坊提出的**分片（sharding）**技术
- 借鉴传统数据库的分片技术思想，**在网络层将区块链网络节点进行分片，每个分片网络各自进行共识，并行处理交易**，以此提升区块链系统吞吐量
- 根据分片对象的不同，可分为**网络分片**、**交易分片**和**状态分片**，其中网络分片是交易分片和状态分片的**前提和基础**

填空题

网络分片

- 网络分片是最基础的一种分片方式，就是将整个区块链网络划分成多个子网络，也就是一个分片。
- 网络中的所有分片并行处理网络中不同的交易。

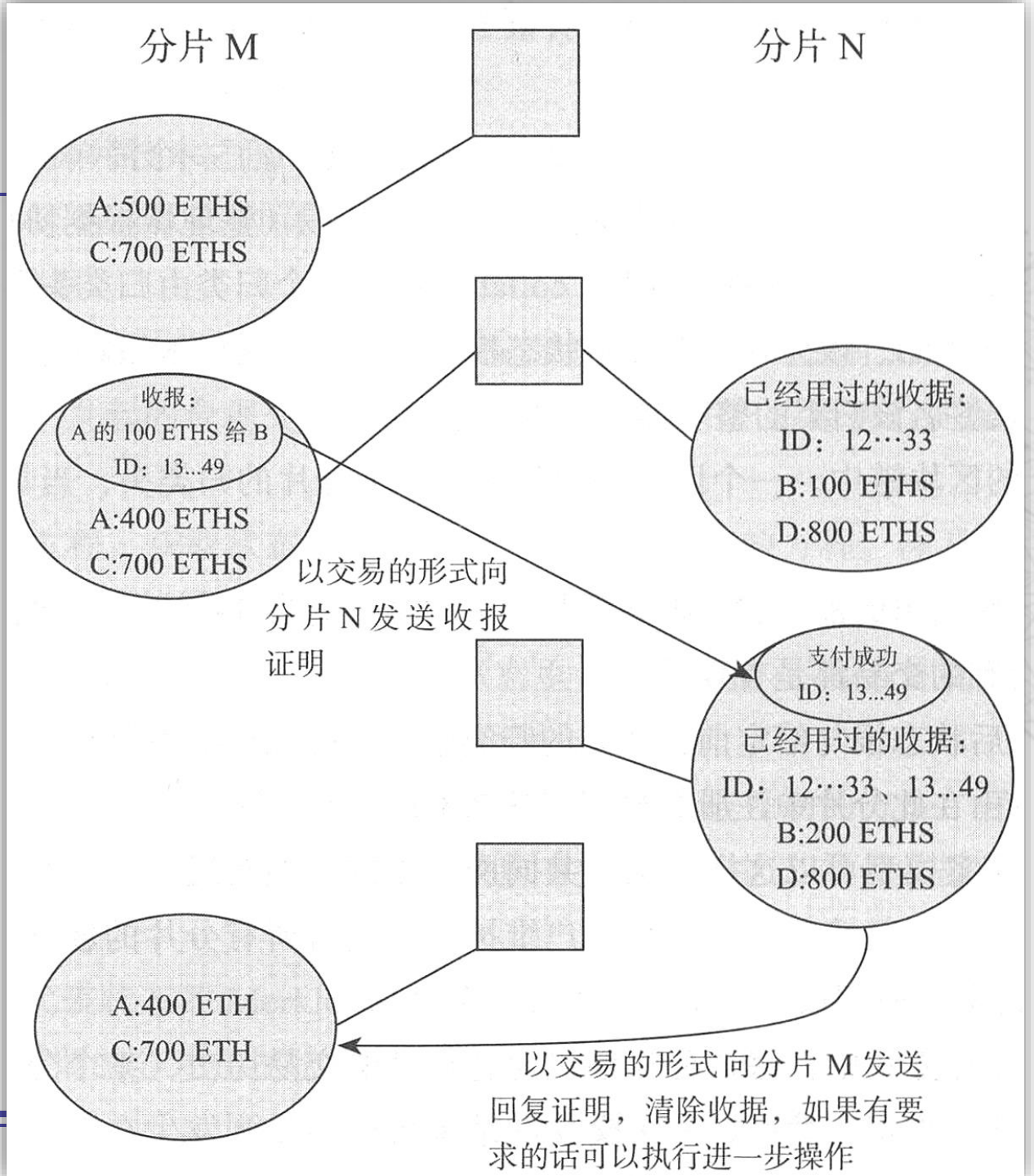
交易分片

- 在网络分片的基础上，将**全网交易划分到不同的网络分片中进行分区域共识**
- 每个分片网络可以同时进行共识、验证交易数据
- 系统由串行事务处理改为并行事务处理机制，以提升区块链网络的整体性能。

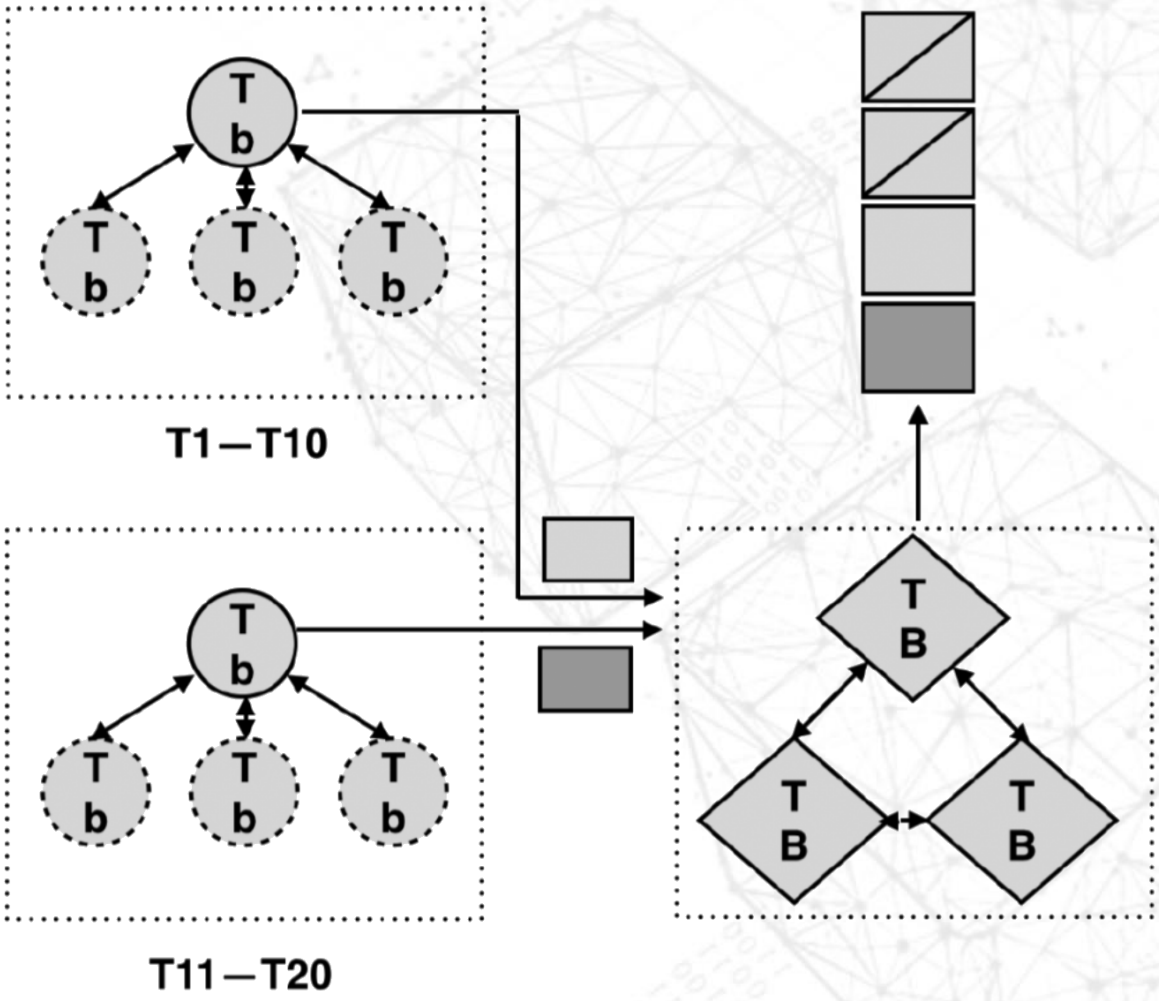
状态分片

- 状态分片同样建立在网络分片的技术上
- 区别是**每个网络分片不再存储账本的全部信息，只存储特定状态的部分账本信息**，减少了系统处理事务时数据调用、传输和存储的开销，以提升系统效率
- 相比于交易分片只能有限提升区块链性能，状态分片能从本质上解决区块链性能扩展问题
- 但是还存在较高的技术壁垒，实现难度大，此外分片技术将完整的系统生态加以划分治理，也会带来一定的安全风险

跨片：收据


分片 M
分片 N
A:500 ETHS
C:700 ETHS
收报：
A 的 100 ETHS 给 B
ID：13...49
A:400 ETHS
C:700 ETHS
已经用过的收据：
ID：12…33
B:100 ETHS
D:800 ETHS
以交易的形式向分片 N 发送收报证明
支付成功
ID：13...49
已经用过的收据：
ID：12…33、13...49
B:200 ETHS
D:800 ETHS
A:400 ETH
C:700 ETH
以交易的形式向分片 M 发送回复证明，清除收据，如果有要求的话可以执行进一步操作

跨片：多层



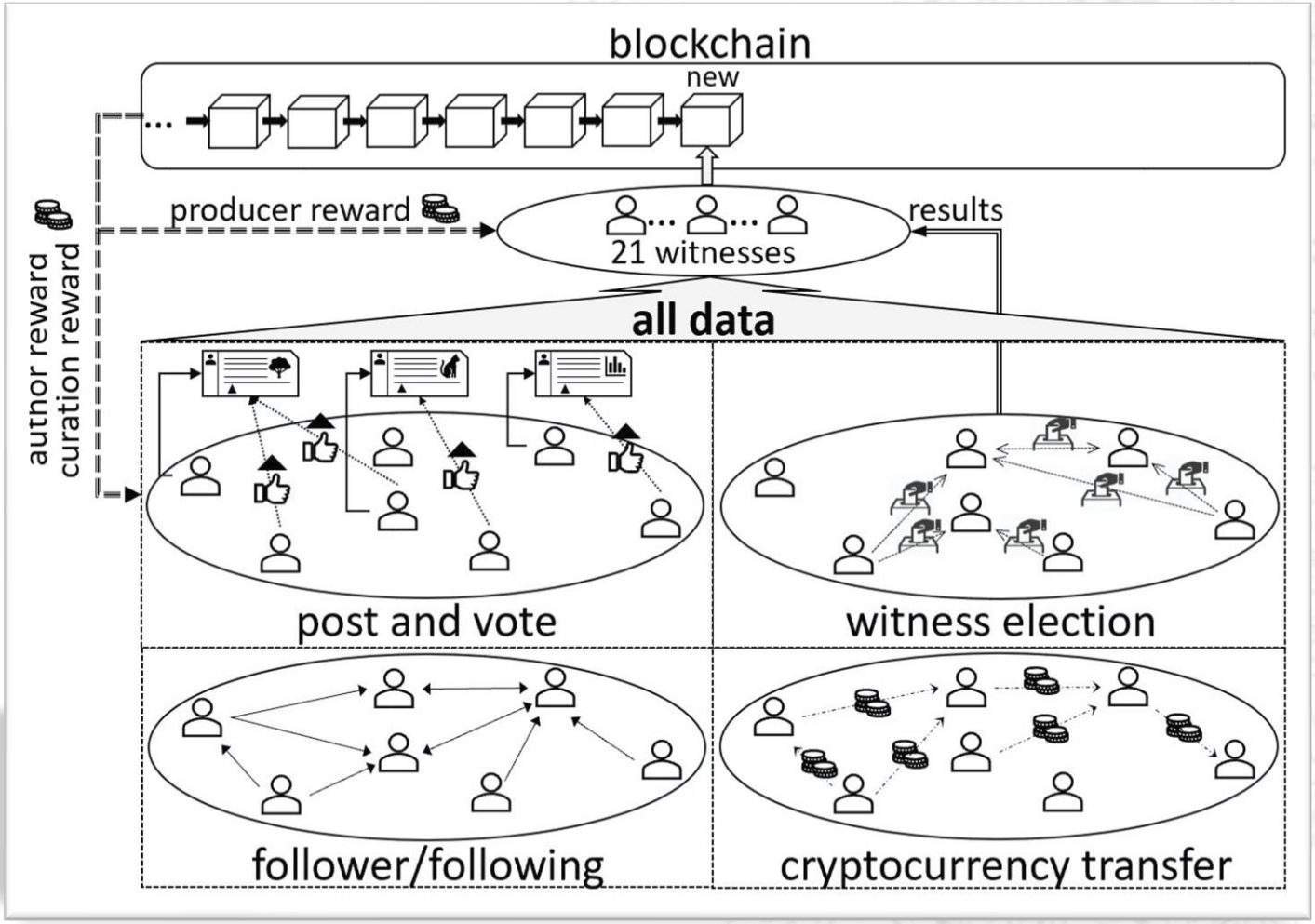
共识层扩容方案：共识机制改进

- 共识层扩容方案主要是**修改共识机制**，PoW共识机制需要节点计算规定难度的哈希值
- 为了减少计算过程的大量时间浪费，提出了**PoS、DPoS、PBFT**，以及混合共识机制等多种共识算法来减少系统达成共识所用的时间，以此提高系统性能

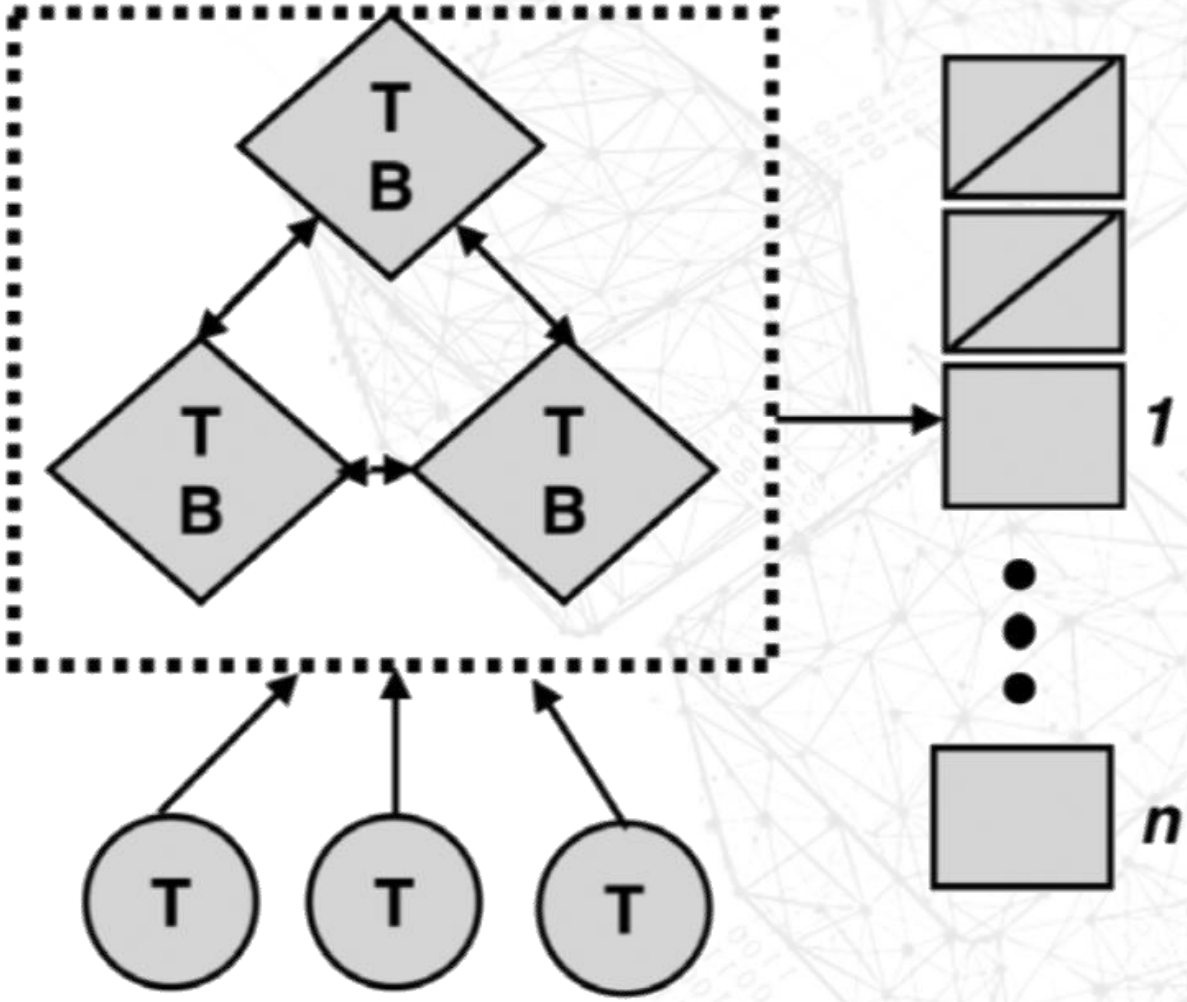
为什么能够扩容。

- 但是到目前为止，尚未出现能够解决区块链分布式系统三元悖论的共识算法，分布式系统的共识机制在很长一段时间内都将是区块链系统的研究难点与热点

DPoS


blockchain
new
producer reward
21 witnesses
results
autnor reward
curation reward
all data
post and vote
witness election
follower/following
cryptocurrency transfer

共识机制改进



链下扩容

链下扩容

- 链下扩容的主要思想是**将部分数据转移到链下进行计算处理，将最终的结果返回至链上进行存储记录**。
- 根据转移方式的不同，目前主要有3种技术路线：
  - 状态通道
  - 侧链
  - 链下计算

状态通道

- 状态通道的转移方式主要是**链下通道交互、链上清算**
- 开辟联通交易双方的通道，锁定区块链部分状态，将交易中间过程和相关的大量数据计算与事务处理放在通道内处理，只把最终的状态提交到链上进行开辟通道前状态记录更新
- 通道内数据交互不需要经过链上共识，以节省时间达到提高系统效率的目的

状态通道

- 使用状态通道的一般流程为：
  - 锁定状态
  - 开辟通道
  - 通道内数据交互
  - 关闭通道
  - 提交更新状态
  - 链上清算

给个流程，看看顺序对不对。

- 在通道内的数据交互与状态更新是不需要进行区块链共识的，因此能够提高区块链系统吞吐量

雷电网络

通道

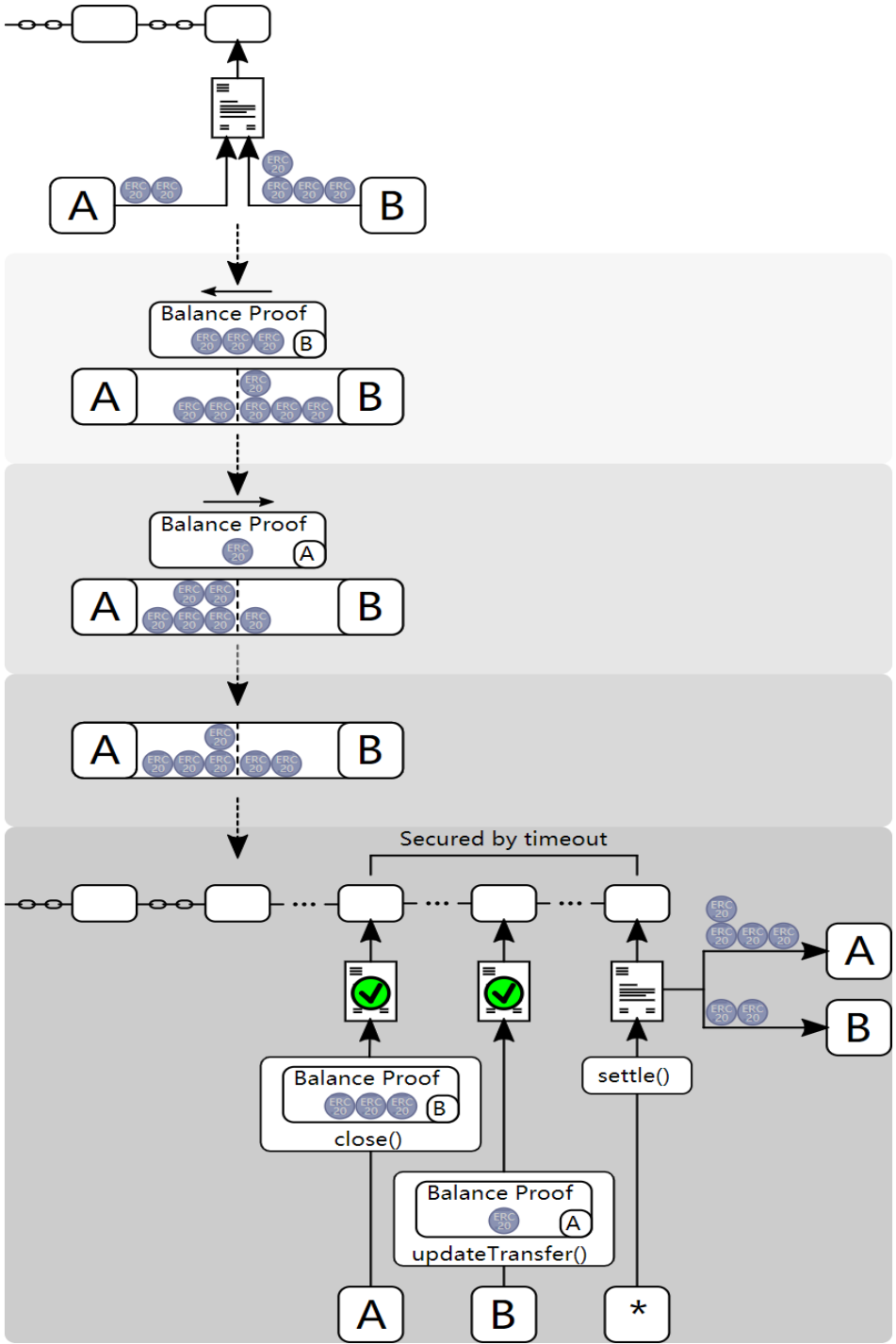
- 对于经常需要相互转账的 A 和 B 来说，A 可以在链上部署一个智能合约然后 A 和 B 向合约中转入一定数额的以太币
- 当A向B转账时，该交易无须全网广播，而是双方保留彼此签名的转账消息，无法伪造和抵赖
- A和B可以通过此方法频繁交易
- 当交易结束，想写入以太坊主链的时候，A或B只需把签名的转账消息提交到合约中最终的以太币余额会按照线下转账记录来分配

雷电网络

例子

- A和B建立通道时在合约中锁定6个Token (A2B4)
- 当B转账给 A3个Token的时候，B将这个新的对该通道中的资金的余额分配方案(A5B1)，用自己的私钥签名，并将签名后的消息（余额证明）发送给对方A
- 当A确认收到这条消息后，这笔转账就完成了
- 同理，当A需要向B转账时，只要把自己签名的余额证明发送给B就可以了

雷电网络


A
B
Balance Proof
B
A
B
Balance Proof
A
A
B
A
B
Secured by timeout
A
B
Balance Proof
close()
settle()
Balance Proof
A
updateTransfer()
A
B
*

雷电网络

优点

- 雷电网络通道中的转账全部发生在链下，在整个通道的生命周期中，只有常数次交易被广播到以太坊网络中（创建智能合约、双方注入资金、一方请求关闭通道、一方在关闭前更新余额信息、任意用户确认通道关闭）
- 雷电网络通道中的转账**无需等待**以太坊的区块确认延迟也不会给以太坊网络造成任何的负担，转账时**不需要支付**以太坊网络中的 Gas，网络上的其他用户也无法看到每次转账的细节而只能看到通道撤销时最后的资金分配情况。 从而解决了双方转账的场景中的大部分速度、费用和隐私的问题

状态通道

- 状态通道的参与者仅限业务相关方，避免了数据**隐私**泄露给不相关的节点
- 状态通道提供了较好的**安全**性，并且可做到随时关闭通道和更新状态，尤其适用于固定双方数据高频交互的场景
- 但是该种扩容方案要求交易**双方实时在线**，需引入第三方进行监督，因此带来了中心化风险

侧链

- 侧链协议最早源于比特币区块链，目的是让**比特币安全地在比特币主链和其他区块链间互相转移**，在后来的应用中，侧链的概念也被扩展至其他区块链
- 侧链是一个**独立的区块链**，通过主链资产的**双向锚定**进行数据交互，侧链依赖于主链，但是独立于主链处理事物
- 侧链相对主链缺少完备的生态体系，**容易成为攻击者的目标**，给主链带来可用性和安全性风险

侧链

- 建立主侧链锚定的一般流程为：
  - 锁定主链资产
  - 释放到侧链
  - 解锁资产
  - 侧链交易
  - 锁定侧链资产
  - 返回主链
  - 解锁主链资产

侧链、主链的衔接点：

侧链

- 根据主侧链间资产锁定与解锁管理方式的不同，目前有3种技术路线：
  - 托管模式（单一与联盟）
  - 简单支付验证（Simplified Payment of Verification，SPV）模式
  - 驱动链（Drivechain）模式
- 当前已经部署运行的侧链包括基于比特币网络的侧链 Lightning Network（闪电网络）、Rootstock 的 Liquid，以及以太坊的侧链 Plasma和国内采用侧链协议的Asch等。

托管模式

- 单一托管模式是**选取主链上的单一中间方作为资产锁定与解锁的管理者**
- 联盟托管模式则是**选取多个托管方组成联**盟，采用多重签名的方式对侧链进行资产管理
- 这种方式实现简单，不需要改变比特币的基础协议，但是增加了人为参与的**中心化风险**

简单支付验证模式

- 简单支付验证模式是侧链白皮书中**最初设计的双向锚定方式**
- 将主链资产锁定到一个地址中，生成 SPV 证明，该证明用于主侧链间信息的相互验证，即 **SPV 证明作为托管方**，管理主侧链资产
- 但是，采用 SPV 证明进行资产锁定的同时，也即是对主链进行了临时的软分叉操作，解锁时，主链软分叉结束，又对侧链进行了软分叉，给主侧链带来了**安全风险**

驱动链模式

- 驱动链模式是将**矿工作为托管方**验证主侧链间的数据交互
- 其**利用受利益驱动的矿工**作为公正的托管方，监管主侧链资产的锁定与解锁需求
- 该模式同 SPV 模式一样，带来软分叉的**安全风险**

链下计算

- 链下计算扩容方案的主要思想是将原本置于链上处理的各类计算、事务，放到链下处理，而链上仅作数据验证，以此间接提升区块链处理数据的速度
- 链下计算实现方案主要包括3 种方式：
  - 链下可信执行环境 （Trusted Execution Environment，TEE）计算
  - 链下安全多方计算
  - 链下激励驱动

链下 TEE 计算

- 将链下的计算放在 TEE 中进行
- TEE 提供**基于硬件的计算机密性和安全**
- Intel 芯片的 **SGX** 与 ARM 芯片的 **TrustZone** 都可以用于链下TEE 计算

链下安全多方计算

- 链下计算通过安全多方计算的方式实现数据可用不可见的应用方式
- 类似 TEE 提供硬件芯片的加密安全，多方安全计算提供**基于软件算法的加密**
- 具体而言，链下安全多方计算首先**锁定**链上的公共状态，然后将数据**分发**到链下进行安全多方计算，最后将各计算结果**组合并返回**链上进行验证

链下激励驱动

- 激励驱动型链下计算是采用激励机制，用于激励处理计算任务的求解者和检验求解者计算结果正确性的验证者
- 计算**正确的参与者可获得奖励，反之受到惩罚**

区块链扩容技术对比

总结的很全面，看一看

扩容层次	扩容方案	原理简述	优势	劣势
链下扩容	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	隐私性和实时性好，理论上可无限扩展	技术难度高，安全隐患多
	侧链	锚定主链资产，建立性能更高效的侧链	独立性好，灵活性高	创建侧链成本及维护成本高，易成为攻击目标，技术难度高
	链下计算	将复杂的计算放到链下，将计算结果返回链上验证记录	链下可用传统安全高效方法做复杂计算，间接提升性能	技术难度高，适用范围有限
链上扩容	扩块	通过扩大区块容量，增加数据区块能够打包的交易数量，间接提升系统吞吐量	技术简单易实现，实施周期短，短期效果明显	区块容量增大会增加区块在网络中的传播时延，容易产生分叉
	隔离见证	将数字签名信息移除区块，增加区块容纳交易数量	提升链上交易安全，易实现，降低交易费用	不是针对性能优化提出，扩容效果有限
	DAG 技术	块链式结构改为 DAG 网状并发式结构，实时验证交易	节点越多，交易验证速度越快，理论上无上限	安全性和一致性未得到充分验证，适用范围有限
	分片技术	将网络分片，每个分片独立并发处理全网交易	并行处理事务，节省系统资源	技术难度高，实施周期长
	共识机制改进	PoS、DPoS、PBFT 等改进算法、混合共识算法	降低能耗，提升共识效率	存在技术壁垒，较难实现
第 0 层扩容	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	不影响区块链自身架构	扩容效果有限，适用受限
	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	不影响区块链自身架构	技术难度高，扩容效果有限，适用受限

总结

1 区块链拥堵与扩容技术

2 链上扩容

3 链下扩容