GIAC

全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

基于侧链存储的主链扩容技术方案

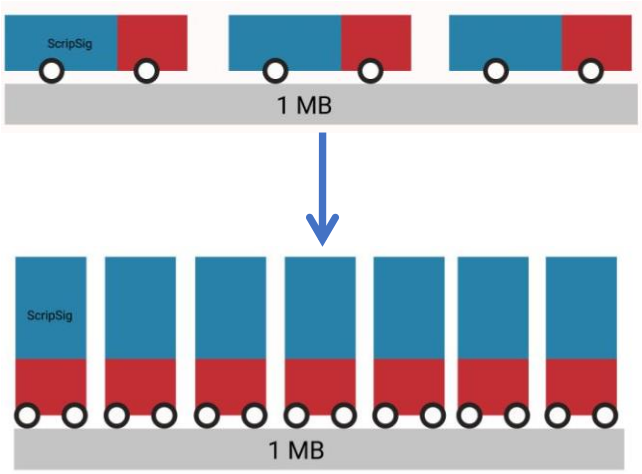
陈有才　公信宝　GXS Labs Director

1.为什么要扩容？

比特币刚诞生时，区块大小最大可达32MB。为了保证资源不浪费、预防DDoS攻击，中本聪决定临时将比特币区块大小限制为1M。即每秒大约只能处理6-7个交易。

随着比特币交易量不断增长，比特币网络渐渐难以迅速地进行转账交易确认，比特币网络出现拥堵。

1.1隔离见证（Segwit）



每笔交易里面，我们能否去掉一些数据，比如交易签名？例如：调整账本结构。

其优势在于：改变了账本结构，又没有导致硬分叉，一定程度上增加了单个区块可容纳的转账笔数，提高了转账效率，也能确保网络的完全去中心化。

该方案已于2017年8月在比特币网络上被采用。

1.2增加区块大小

TPS	单个块大小	块手续费	全年块大小
1	0.3MB	0.12BTC	15GB
3	0.9MB	0.36BTC	47GB
10	3MB	1.2BTC	150GB
100	30MB	12BTC	1.5TB
1000	300MB	120BTC	15TB
10000	3GB	1200BTC	150TB
100000	30GB	12000BTC	1500TB

直接增加区块大小能直接提高单个区块转账数量，从而提高转账效率。
提高转账数量的同时，提高了区块手续费，也提高了全年出块的存储空间。

1.3POS

PoW

PoS

以以太坊为例，优化共识算法，通过软件实现扩容：
在PoS中不需要挖矿，只需要锁定矿工一部分的ETH，就能成为验证者（validator）。如果验证正确，矿工就获得相应代币奖励，如果验证错误，矿工就失去锁定的ETH。

目前以太坊处于PoW和PoS的混合机制。

软件对区块链扩容的意义很大，如ETH，因为算力与持有的ETH相关，持有越多的Token，能产生区块的机会越大，获得的奖励也越多。因此矿工会拼命增加区块大小以承载更多转账信息，从而提高转账速度。

1.4分片技术（sharding)

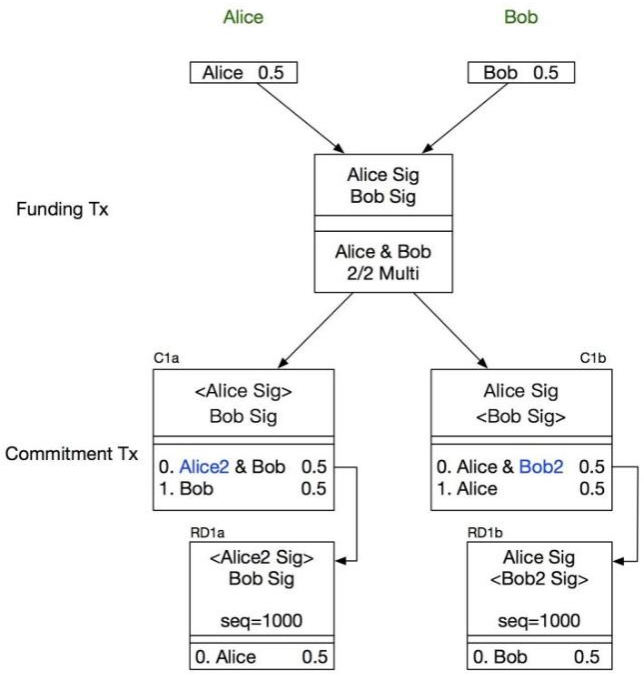
分片技术是基于数据库分片传统概念的扩容技术。

由于网络中的每一个完全参与的节点都必须要验证每一笔交易，并且这些节点必须和它的其他节点保持一致，这是区块链技术的组成部分，它通过创建分布式的账本来保证区块链的安全。我们想象一下：区块链就像一条繁忙的高速公路，这条高速公路的收费站只有一个收费口。这种布局的结果将是导致交通堵塞，因为人们将排着长队等待通过这唯一的收费站。实现一个基于分片技术的区块链就像在高速公路上增加15或20个收费口。它将极大地提高汽车通过收费站的速度。分片技术中，每一节点只与自己所处分片的节点交互，因此，分片技术将带来巨大的差异，并显著提高区块链的交易速度。

分片的方式：网络分片、交易分片、状态分片等。

侧链是“外部嫁接”，分片是“内部分割”。

1.5链下状态通道技术



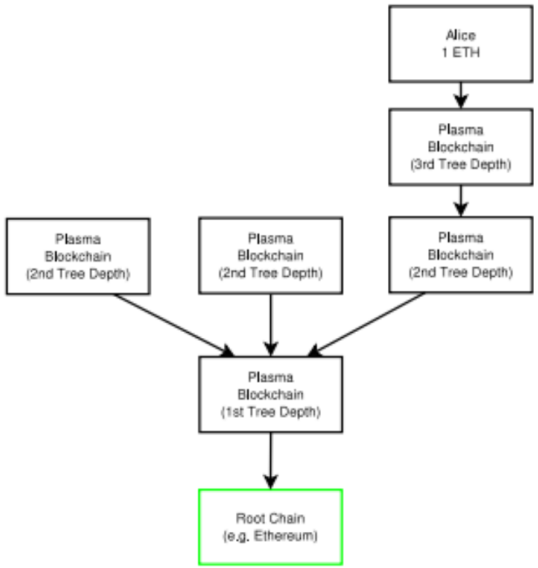
RSMC

最典型的就是闪电网络，利用状态通道，实现快速的小额支付。扩容逻辑是将小额高频的交易在链下计算，链上记录最终的结果。

1.RSMC（revocable sequence maturity contract）可撤销的按序到期合约
2.HTLC（hashed time lock contract）哈希时间锁
3.闪电网络

RSMC：
1、双方各拿出0.5BTC，构建Funding Tx，输出为爱丽丝和鲍伯的2/2多重签名。此时， Funding Tx未签名，更不广播。
2、爱丽丝构造Commitment Tx：C1a和RD1a，并交给鲍伯签名。C1a的第一个输出为多重签名地址，爱丽丝的另一把私钥爱丽丝2和鲍伯的2/2多重签名，第二个输出为鲍伯 0.5BTC。
3、RD1a为C1a第一个输出的花费交易，输出给爱丽丝0.5BTC，但此类型交易带有sequence，作用是阻止当前交易进块，只有前向交易有sequence个确认时才能进块。
4、鲍伯构造Commitment Tx：C1b和RD1b，并交给爱丽丝签名。结构与C1a、RD1a是对称关系。
5、鲍伯对C1a和RD1a进行签名，并将签名给爱丽丝；同理，爱丽丝对C1b和RD1b签名，完成后给鲍伯。此时，由于并未对Funding Tx进行签名，任何一方均无法作恶，任何一方也不会有任何损失。
6、双方均完成对commitment Tx的签名并交换后，各自再对Funding Tx进行签名，并交换。此时，Funding Tx是完整的交易，广播之。

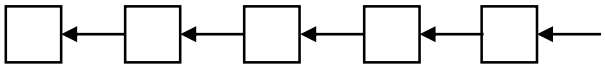
1.6Plasma



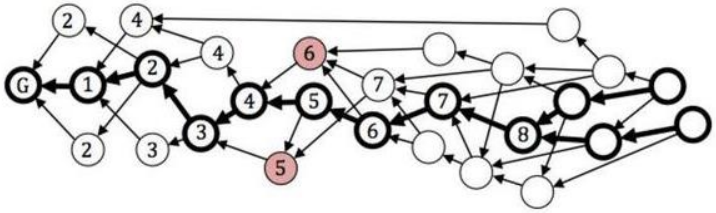
通过大量的“子区块链”来减少存储在区块链上的数据量，并使用“欺诈证明”的技术将“子区块链”和主区块链连接在一起，从而实现扩容。

Plasma是“一种复杂的闪电网络”，使用一种特殊的方式将本是平行的两层网络结合在一起。

1.7DAG（有向无环图）



Blockchain



DAG

DAG（Drected acyclic gragh)并不是传统的“区块+链表”的结构，没有区块的概念。

DAG的特点是把数据单元的写入操作异步化，大量的钱包客户端可以自主异步地把交易数据写入DAG，从而可以支持极大的并发量和极高的速度。

第一，数据不像比特币和以太坊一样强同步，而是弱同步，允许节点在同一时刻数据不一样，数据可以有一些微小的差别。第二，可以通过数据单元之间的引用来完成交易的确认，就是后面发生的单元去引用前面的单元，这样不需要我们把数据传给矿工，整个过程都是由自己去完成的，这个过程很快。

但DAG面临的双花问题会非常复杂。

2.链上存储的扩容：创世区块的思考

字节	字段	描述
4	版本	这笔交易参照的规则
1-9	输入计数器	包含的交易输入数量
32	交易哈希	不引用任何一个交易，值全部为0
4	交易输出索引	固定为0xFFFFFFFF
1-9	Coinbase数据长度	coinbase数据长度
不定	Coinbase数据	在V2版本的区块中，除了需要以区块高度开始外，其它数据可以任意填写，用于extra nonce和挖矿标签
4	顺序号	值全部为1，0xFFFFFFFF
1-9	输出计数器	包含的交易输出数量
8	总量	用聪表示的比特币值
1-9	锁定脚本大小	用字节表示的后面的锁定脚本长度
不定	锁定脚本	一个定义了支付输出所需条件的脚本
4	锁定时间	一个区块号或UNIX时间戳

coinbase交易

2009年1月3日，比特币的创始人中本聪在创世区块里留下一句永不可修改的话：

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks（2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘）。”

2.1外部数据引入？

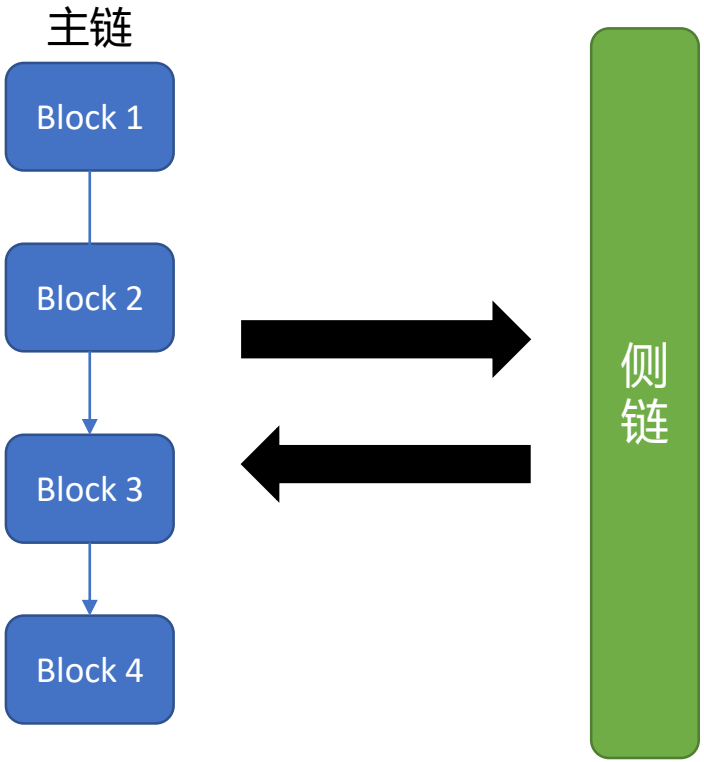
智能合约（英语：Smart contract ）是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

区块链上的智能合约需要外部参数的引入。

因此，我们能否对“Coinbase”进行扩容，让它能对应一些外部数据？

更进一步，我们如何实现更加复杂的智能合约？

2.2侧链存储方案

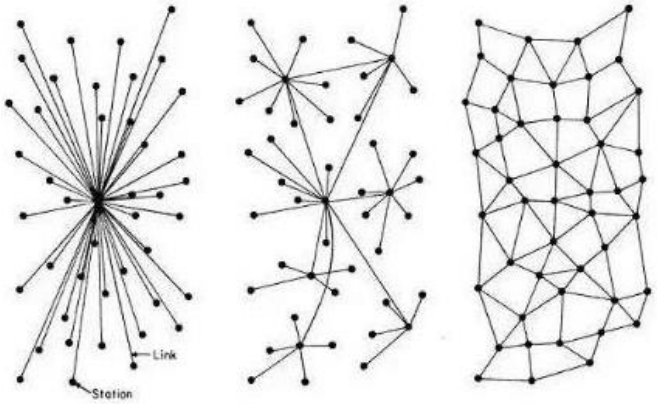


1.侧链作为存储空间，将外部数据引入系统内

2.建立主链与侧链的关联

3.通过主链交易，实现侧链数据的调用

2.3侧链-IPFS

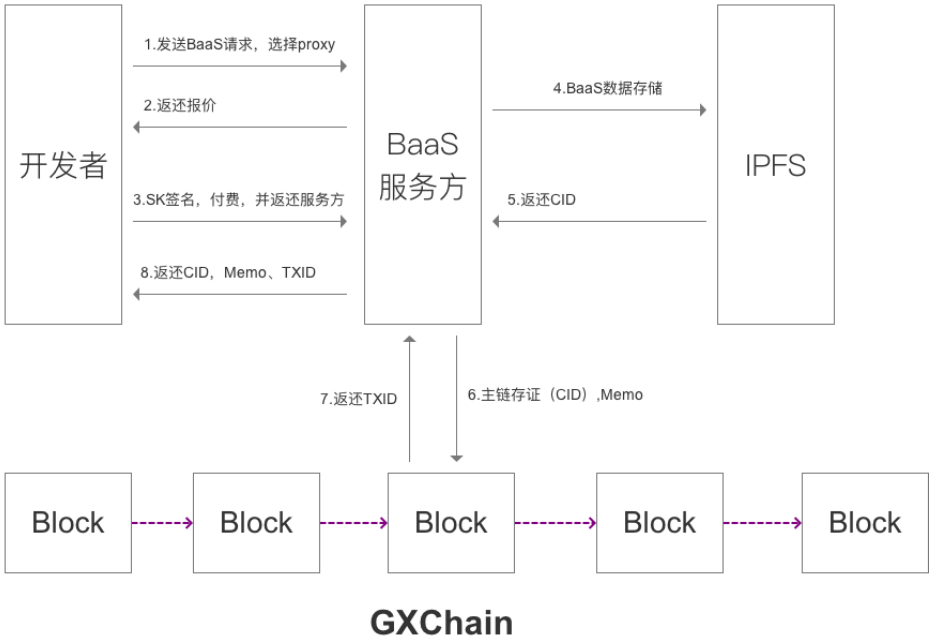


IPFS（The InterPlanetary File System）星际文件存储系统是一种点到点的分布式文件系统，它连接的计算设备都拥有相同的文件管理模式。被认为是“下一代的HTTP协议”。

HTTP存在超中心化的问题，下面分析一下IPFS如何解决这些问题。IPFS从根本上改变了查找的方式，这是它最重要的特征。使用HTTP查找的是位置，而使用IPFS我们查找的是内容。

IPFS的做法则是不再关心中心服务器的位置，也不考虑文件的名字和路径，只关注文件中可能出现的内容。我把刚才的文件放到IPFS节点，它会得到一个新名字QmXGTaGWTT1uUtfSb2sBAvArMEVLK4rQEcQg5bv7wwdzwU，它是一个由文件内容计算出的加密哈希值。哈希值直接反映文件的内容，哪怕只修改1比特，哈希值也会完全不同。当IPFS被请求一个文件哈希时，它会使用一个分布式哈希表找到文件所在的节点，取回文件并验证文件数据。

2.4公信宝的BaaS-可实现基于IPFS的侧链存储



开发者
基于GXChain的各类应用开发

BaaS服务方
将数据写入侧链的记账节点

IPFS
星际文件存储，GXChain的侧链，用于存储数据本体

GXChain
公信宝的底层主链

2.5GXChain的架构

2.6公信宝=“大数据+区块链”

2.7公信宝的开发环境

公信宝为开发者提供更优质的开发环境

	在公信宝公链上开发 Dapp	在其它公链上开发 Dapp
数字身份	KYC 后的唯一通用数字身份 (G-ID)	仅有数字钱包账户
用户数据	多维度的链上用户数据标签	—
平台流量	布洛克城百万级用户流量	—
存储服务	BaaS 支持大量数据存储和验证	需要自行扩展
智能合约	可编程可计算的运行环境	可编程可计算的运行环境

2.8公信宝的孵化案例

Lucia

利得

Unitopia

币得

预言家

公益类
出行类
知识培训类

AND MORE

GIAC 全球互联网架构大会
GLOBAL INTERNET ARCHITECTURE CONFERENCE

谢谢！

公信宝公众号

商务联系邮箱：bd@gxb.io
个人邮箱：chenxiao@gxb.io
个人微信：a36079354