基于 SimpleChain Beta 的跨链交互与持续稳态思考

闪电网络与雷电网络的设计已经将扩展性问题的解决引导向了主链之外的第二层，将不同需求的网络和主链网络分层，成了解决扩展性问题的一大趋势

文 | 俞学劢

比特币作为第一个区块链应用与运行到目前为止最被信任的公链，其扩展性问题却持续被作为焦点贯穿着整个链的发展周期。类似的问题，在以太坊上依然存在。

在主链扩展难以破局的过程中，一方面出现了将主链区块链数据验证和计算的责任仅交由一小组高性能节点来完成的解决方式，比特股、EoS 等的 DPoS 机制即通过这种方式来实现。这类解决方案通过模拟现实中的议会制选举高性能节点，而难免引起了利益集团与中心化趋势的疑议。除此之外，也有通过链下交易来解决这类问题的尝试，其中比特币的闪电网络和以太坊的雷电网络是较为典型的两个实例。

由于比特币 UTXO 的区块链模型和以太坊基于账户余额模型的区别，在链下交易通道的具体协议设计上就有了闪电网络和雷电网络的差异。但不管如何，闪电网络与雷电网络的设计已经将扩展性问题的解决引导向了主链之外的第二层，将不同需求的网络和主链网络分层，成了解决扩展性问题的一大趋势。

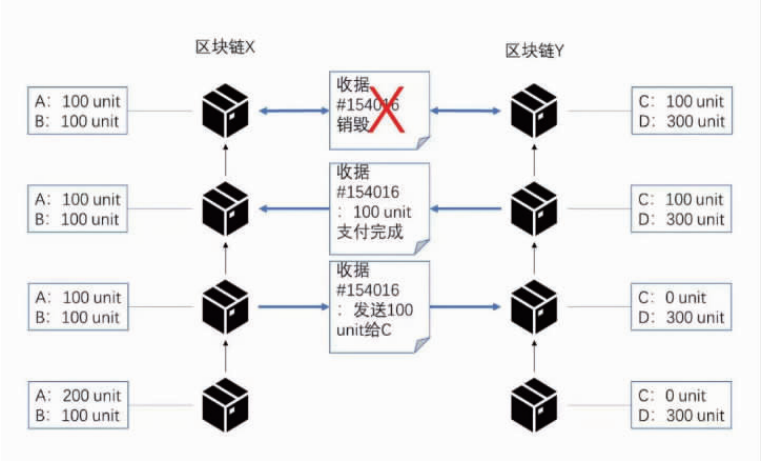
主子链设计与分片概念

分片源于数据库设计中的概念，通过分类备份和冗余来增加整体数据库的处理效率和容错性。分布式数据库中通过建立不同的分片机制满足业务系统的不同要求。区块链中针对性能扩展所提出的第二层（Layer 2）解决方案也借用了这一概念，通过将不同业务对区块链的不同需求进行分类，并各自分布在不同的子链当中，从而解决全链共识的性能瓶颈。

分布式数据库中通过建立不同的分片机制满足业务系统的不同要求。区块链中针对性能扩展所提出的第二层（Layer 2）解决方案也借用了这一概念，通过将不同业务对区块链的不同需求进行分类，并各自分布在不同的子链当中，从而解决全链共识的性能瓶颈。

然而，区块链与分布式数据库中较大的区别在于，分布式数据库的增删改查以及计算来自业务系统或者中心化的数据管理系统，分布式数据库各节点仅负责响应数据管理员（DBA）；而区块链的业务逻辑也来自各节点即包含业务逻辑、计算，也包含了至少账本层面数据的管理，也就是每个节点都可以是 DBA，或者理解为根本没有 DBA，因此在设计上则更为复杂。

由于分布式数据库的交易逻辑为中心化控制，因此其分片可以被看作是单纯的存储分片。区块链的分片则主要分为相对简单的交易分片：即仍然保持全网络节点在数据上的全同步，仅通过分片来让不同节点运行不同的运算逻辑；和更为困难的状态分片：即同时包含了对交易与存储的分区。狭义上来理解，最直观的状态分片其实就是各种分叉，不同分叉链上各自处理自己的交易、存储自己的账本数据，验证历史区块有效性的时候可以选择一直回溯到分叉发生前的区块，通过快照来确认历史交易。但这种类型的分片由于没有后续跨片交互的机制设计，因此并没有提



▲ 图 1 基于收据的跨链交易确认(Ethereum wiki)

升太多实际价值。

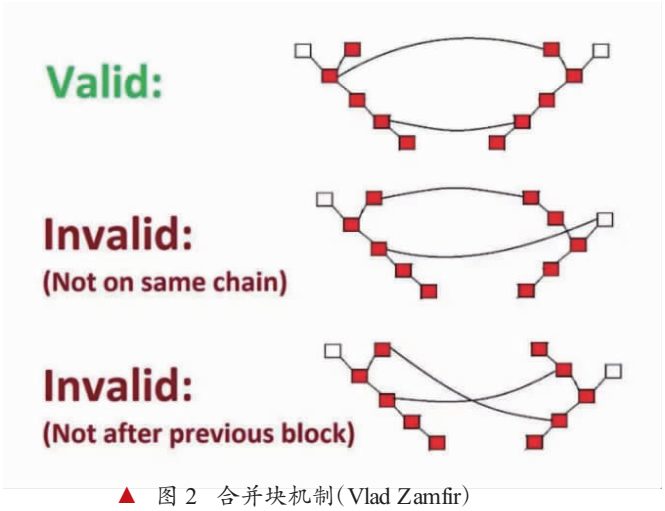
那么状态分片的跨片交易需要解决的就是如何去相互验证不同分片内交易的有效性了。分片内部交易的有效性由分片内的节点通过共识机制确保,也因此在 SimpleChain(上链)的设计当中,不同的分片内也同样拥有着区块链的运行机制,因此跨片交易问题在 SimpleChain(上链)当中就被理解为跨链交易的问题,而分片则被定义为子链。

跨链交易的形成

由于跨子链交易来自两个账本数据不一致的区块链用户之间,因此通过构造一个不作为状态存储在账本中的"对象",可以实现类似于 SPV(简单支付验证)的机制,即通过互相之间所同步的区块头来完成梅克尔证明,验证这个构造出来的"对象"所传递信息的有效性。在这里,可以把这个"对象"称为收据。

在图 1 中,表示的是一个从区块链 X 中的用户 A 向在区块链 Y 中的用户 C 发送 100 个单位的资产的过程。

为了确保上面这个机制的持续有效,还需要考虑跨链交易中的终局性



▲ 图 2 合并块机制(Vlad Zamfir)

问题,或者叫做分叉选择机制。区块链 Y 所验证的区块链 X 交易必须来自区块链 X 有效链的块中的交易,而不是来源于一个孤块或者孤链。Vlad Zamfir 提出过一个合并块的设计,也就是两条链在需要发起跨链交易时,两个在不同链上的块合并为同一个区块,各自的链都基于这个合并块去延长之后的块数据。但实际上合并块意味着两条链的账本同步,因此其实并不能解决两个分片或者两个链之间的相互独立性问题。但是跨链交易中,如何寻找正确的对方链的块去完成收据的梅克尔证明,是可以从 Vlad Zamfir 的思路中找到答案的。

Vlad Zamfir 将两条需要实现跨链的链进行等级排序,分为"父链"和"子链","子链"需要在与"父链"高度相同,或高于"父链"高度所产生的区块与"父链"进行区块合并,或者在场景中是在"父链"上进行区块跨链验证。这样能够确保两个链在各自延长的过程中,跨链部分数据能够持续保持一致。

但是,在上述的解决方案中存在需要两个区块链同步出块的前提,因为如果"父链"X 的交易迟迟不能确认,或者没有延长,或者"子链"Y 没有及时收到 X 的延长情况,抑或"子链"与"父链"存在间断性同步,则"子链"Y 的后续交易有效性也都会受到相应的影响。

在以太坊 2.0 的设计中,信标链被赋予了这个职能。信标链可以被认为是以太坊 2.0 设计中所有分片链的主链,这条主链通过 Casper 共识机制来选举并在每一轮中随机产生分片验证者,用于协调分片之间的交易正确性。但是在属于 PoS 的 Casper 共识机制中,由于没有了难度要求、nonce、块哈希这些原本在 PoW 中能够执行无状态 SPV 证明的工具,因此要验证分片链的有效性需要回溯到可信区块,再重新计算可信区块后的区块状态一致到当前区块,才能完成验证,导致验证者增加了工作量。因此在 SimpleChain 当中,为了减少验证者的工作量,类似信标链的角色通过 PoW 的主链来完成。

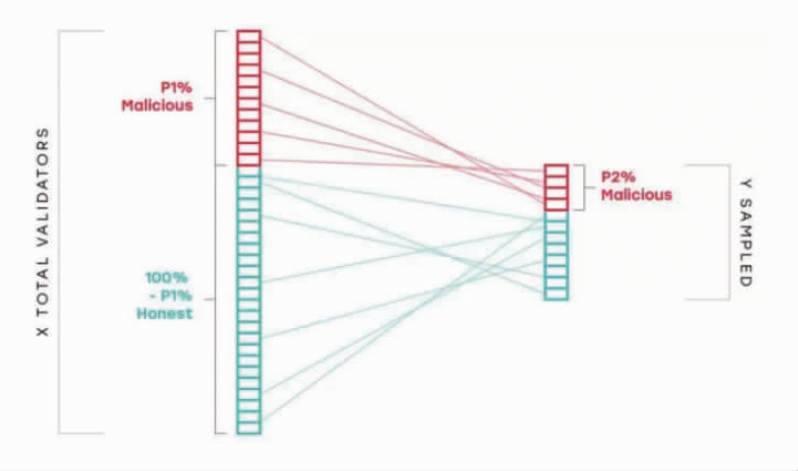
主链当中存在锚定矿工的角色,所谓锚定矿工承担三个功能角色:一是负责在某子链发起跨链交易时验证该子链状态的有效性;二是负责在主链中写入子链交易并广播获得确认;

三是将意在主链确认的跨链交易结果分别写入交易发起子链与交易接收子链的区块中。锚定矿工在验证、广播和传递跨链交易时，既作为子链矿工也作为主链矿工存在。然而在主链上的矿工数量会比子链中的矿工数量多，因此在子链中伪造交易传递到主链的成本将大大低于在主链伪造交易写入子链。因此需要一种更为合理的锚定矿工选举机制。

锚定矿工不针对于某个子链长期存在，但需要长时间作为主链矿工存在。由于 PoW 的主链能够允许无状态 SPV 证明，因此在 SimpleChain 中将锚定矿工的选举通过随机的形式来完成。

由于锚定矿工来自 PoW 主链矿工，因此通过从小到大排列主链矿工所计算出的工作量证明计算结果，进行锚定矿工筛选。由于数值越小的工作量证明计算结果获得的概率越低，因此在锚定矿工预选列表中的排名越高，超出该次锚定矿工数量上限排名的矿工则在当前轮的交易验证中不参与签。锚定矿工选举过程的 PoW 排序与主链延长的 PoW 同步进行，即主链矿工不仅将使用工作量证明计算结果获得主链 SIPC 奖励，还将获得锚定矿工奖励。锚定矿工奖励来自子链跨链交易发起者所支付的 SIPC 矿工手续费。

信标链可以被认为是以太坊 2.0 设计中所有分片链的主链，这条主链通过 Casper 共识机制来选举并在每一轮中随机产生分片验证者，用于协调分片之间的交易正确性。



▲ 图 3 子链中作恶矿工的概率将会高于主链（Alexander Skidanov）

在保证主子链的一致性问题上，采用 n 个确认的机制。当发起一笔跨链交易时，子链内的区块应首先获得 n 个块高的确认，才能够通过锚定矿工的验证并广播至主链上。

主子链结构持续稳态的经济设计

SimpleChain 在白皮书 1.0 中提出了主链数字资源 SIPC 的微通胀机制，即随着子链的增加、子链活跃度的增加以及对跨链交易需求的增加，SIPC 的区块奖励会在原本的衰减曲线基础上产生微调。这种微调的结果就是当主链 SIPC 被作为一种资源，子链对其的需求量增加的时候，主链出块奖励将相应增加，以当前状态为例，主链出块奖励将可能从 20SIPC 增加到 21SIPC。

假设一个资料的启动运营池容量是 10SIPC，在跨链过程中，每次会分出其中的 0.1SIPC 给到跨链矿工作为跨链矿工的部分奖励，一次交易过后运营池容量减少为 9.9SIPC。此时，一般主链矿工收取到的交易手续费为 20+0.01，这 0.01 就是微通胀调节奖励。

运营池可以由任何 SimpleChain 用户选择再次注入 SIPC，也可由子链共识触发活跃度下限，更改跨链矿工奖励来使得跨链矿工获得的 s2 为负，即部分跨链手续费被存入子链运营池。此时，一般主链矿工收取的手续费中的微通胀调节奖励 k 将为 0 或转向负数。这种情况下表明子链走向衰退期，或子链与主链将逐渐通过减少互相激励而脱离关系。

不过，需要指出的是，上述模型中可能存在的技术风险包括主链区块当中对于包含跨链交易的交易量上限问题，以及过多锚定矿工造成的主链负担过重的问题。经济模型方面，也存在“损人不利己”攻击的可能，即通过创建衰减子链，影响主链矿工与用户利益的情况。

（作者单位：浙江数秦科技有限公司。本文由浙江省区块链技术应用协会供稿）