车联网树状多链结构设计

1 引言

物理位置区块链为区块链增加了地理位置属性和区域信息查询方法，但通过区域状态缓存的方式实现查询效率的提升，所有节点存储的区块链仍为链式区块链结构，即全网一致，并未涉及吞吐量或可扩展性方面的研究。

已有一些针对改变区块链结构的研究，但是没有结合地理分区特性的多链结构。为了充分利用车载网地理分区特性，提高区块链存储访问效率，设计按照geohash划分的具备区域物理位置状态特性的树状多链结构，实现不同地理分区内的节点保存不同的链上数据，从而实现减少数据存储量、提高吞吐量和提高区域信息查询效率。

车联网中的节点具备移动性，在树状多链结构中有跨区域移动的行为。车辆网中的移动节点对应树状多链的普通账户。在树状多链中，普通账户具备账户余额和物理位置两个属性，跨区域移动过程中，通过账户位置变化表示移动性，还要关注跨区域后的账户余额一致性。有一些针对跨链资产转移的工作，但是要么借助外部智能合约，要么借助XXXX来实现，没有在区块链内部实现的方法。设计跨区域资产转移方法，在树状多链内部实现不同账户在不同区域的子链间的资产转移。

2 相关工作

（1）提高吞吐量或区块链结构变化的相关工作

（2）跨链资产转移相关工作

（3）我们的工作是按照geohash编码的地理区域构建树状多链结构，实现在子链间的跨区域资产转移。

3 树状多链结构设计

3.1 结构概述

提出一种按照geohash的层级划分结构来建立树状结构区块链，结构示意图如图fig:geohashchain所示。

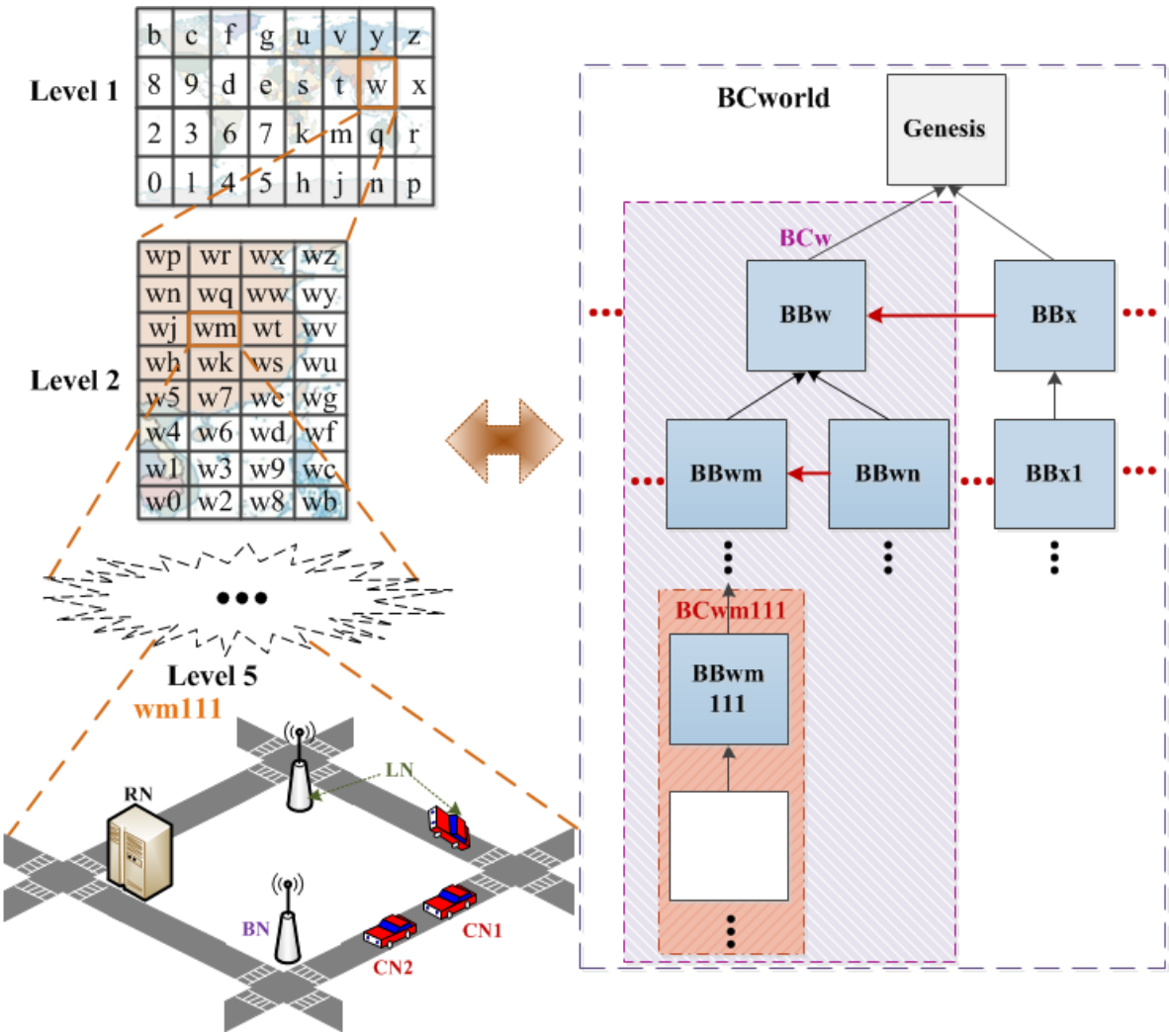

图 fig:treemultichain

Geohash是一种以一维字符串编码地理空间的方式，非常适用于海量物理位置相关信息的索引。按照geohash编码方式划分树状结构，根据不同长度的geohash编码表示父链与子链关系。所有的区块链都有相同的创世块Gensis,然后根据geohash范围划分不同的区域子链。根据区块在树状区块链结构中的作用不同，区块分为创世块（Genesis Block），分支区块(Branch Block)和普通区块（Common Block）三类。树状结构每增加一层分支，都会按照geohash编码方式增加32个平行子链。分支区块由于具备指向同层级前一个分支区块的平行链指针使得原有单链结构成为树状多链结构。

根据树状多链存储内容的不同分为全区块链（Full Chain），分支区块链(Branch Chain)和叶子区块链(Leaf Chain)。全区块链保存包括创世块在内的所有分支区块和普通区块。如BCworld。分支区块链保存以指定分支区块为父区块的所有分支区块和普通区块，以及以该分支区块为终点的包括创世块在内的所有父分支区块。如BCw。叶子区块链保存以指定分支区块为父区块的所有普通区块，以及以该分支区块为终点的包括创世块在内的所有父分支区块。如BCwm111。叶子区块链和分支区块链的区别在于叶子区块链的指定分支区块为最底层分支区块，它的子区块只有普通区块。树状多链结构需要构建父链并维护多链间信息同步，这是本文研究的重点。

3.2 区块结构

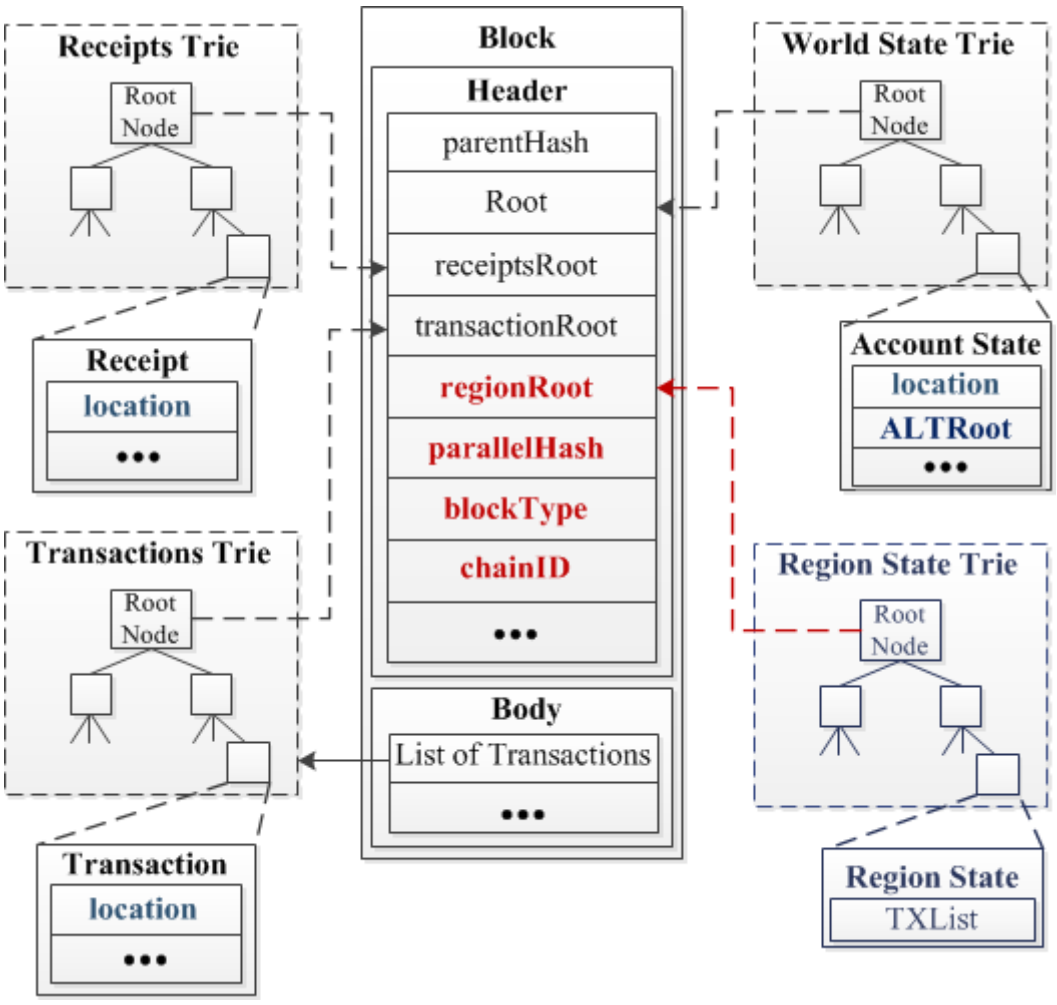

图 fig:block

图 fig:block为树状区块链的区块结构示意图。根据不同类型区块的功能需求，区块中添加如下属性：

blockType:区块类型属性。树状多链由创世块、分支区块和普通区块三种不同类型的区块组成，为了实现按照区块类型存储区块，需要在区块中添加区块类型属性。

chainID:区块链ID属性。单链结构中的区块由于具有线性关系，只需要区块序号即可区分不同的区块。但在树状区块链中，由于各个子链独立生成区块，其区块编号在各子链内部不冲突，但在多链之间存在序号冲突，因此需要添加区块链ID以区分来自不同区块链的区块。

parallelHash:平行链指针。为了使分支区块能够维护其在树状区块链结构中的结构关系，除了要有父链指针指向上层区块外，还需要有维护兄弟关系的指针。平行链指针为指向和当前分支区块链具备相同父区块、geohash编码位数相同，在当前区块之前产生的分支区块的指针。每一个分支区块中最多有一个平行链指针，分支区块根据平行链指针顺序可以查询到同层子链产生的先后顺序。

不同类型区块属性表如表tab:blockattribute所示。

表tab:blockattribute 区块属性表

区块类型	父链指针	blockType	chainID	parallelHash
创世块genesis block(GB)	no	yes	no	no
分支区块Branch Block(BB)	yes	yes	yes	yes
普通区块Common Block(CB)	yes	yes	yes	no

创世块为树状区块链的第一个区块，父链指针为空，平行链哈希也为空。由于处于树状区块链的最上层，因此上层区域状态为空。

普通区块用来在叶子区块链中记录所在区域的账户、交易和收据，方便节点同步数据时按区域同步，具备父链指针，同时其区块中存储有作为区域状态信息的上层区域状态树根列表，用来维护数据一致性。同一叶子区块链内部的普通区块采用单链方式链接，因此没有平行链指针。

分支区块作为指定分支的第一个区块，存在指向上层的父链指针和指向同层前一个分支区块的平行链指针。根据geohash编码方式，在geohash区块链树中，每增加一个层级，就会增加32个分支区块。但是各个分支区块不会全部同时产生，且只有已经存在的分支区块才能将其指针记录在新产生的分支区块中。对于同层级第一个分支区块，构建时还没有同层级的其他分支区块，因此平行链指针为空。

3.3 结构设计

3.3.1 节点角色设定

根据geohash划分方式，每增加一级子链，就会同时增加32个子区域，同时增加32个分支节点。这时会出现两种情况：第一，每次划分增加32个节点使得整体节点数量过于庞大。第二，32个分支节点不是同时出现。我们采用节点角色设定的方式解决这两个问题。

节点角色：结构节点（包括根节点、分支节点和叶子节点）和普通节点。

角色设定：进入树状区块链的车联网节点需要首先设定节点角色。树状区块链构建时，需要遵循自顶向下的构建顺序，依次构建根节点，分支节点和普通节点。如图fig:treestruct所示。在树状区块链中，至少有一个服务器作为根节点负责保存整个树状区块链的全部信息，这时就是单链结构，如图中的single chain。如果一个全区块链只需要划分为同层级的两个区域时，这时只需要构建一个全区块链和两个叶子区块链的两层树状结构，每个叶子区块链至少有一个路侧节点或者车辆节点作为叶子节点。如图中的two chains所示。除了上述两种特殊情况外，树状区块链在构建时需要同时具备结构节点和功能节点。如图中multi-chains所示。不同的角色设定使得树状区块链仍然能够适用于单链的情况。

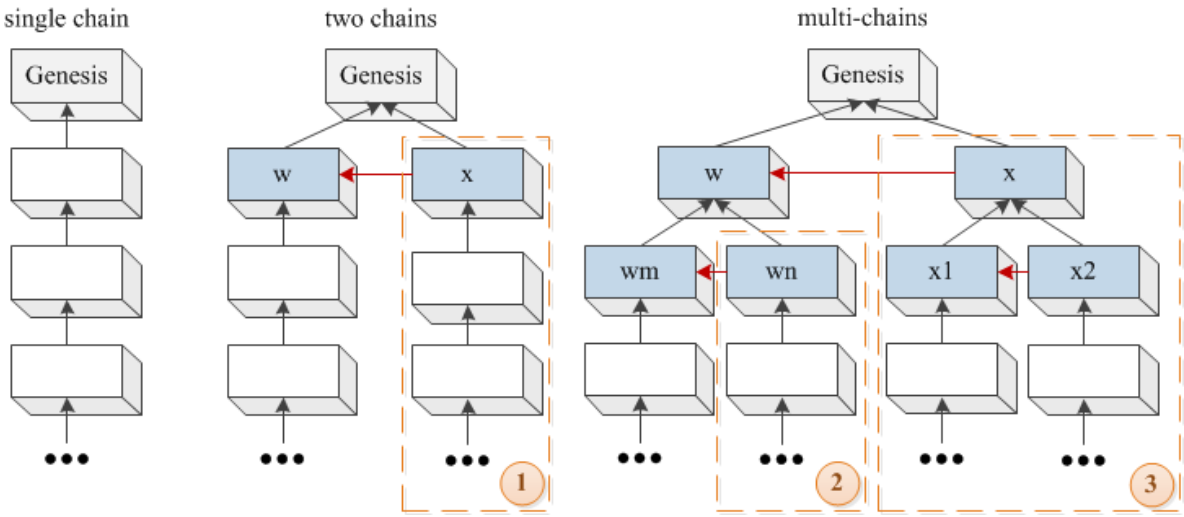

图 fig:treestruct

3.3.2 层次结构设定

层级设置完毕才可以有交易。

树状区块链在构建时需要设定好基本区域和层级。如图fig:treestruct中单链结构没有区域和层级，双链结构只能构建区域范围为1位geohash编码的分支区块，而多链结构中则可构建区域范围从1位geohash编码开始的所有分支区块。一旦结构区块设定完成，区块链的基本层级结构也设定完成，不能改变。初始同层级区域不指定编码顺序，可根据需要设定。我们研究的区域范围为北京地区，则从geohash编码为w的区域开始。

为了简单起见，这里不讨论树状区块链结构的动态调整（子链增加和合并），只讨论树状结构的扩展。所谓树状结构扩展，是指在基本区域和层级设定好的基础上，对已有结构叶子块链结构的平行链扩充，即增加与当前叶子区块链同一层级的其他平行链。当车联网中车辆节点需要移出当前所有叶子区块链的区域时，需要建立覆盖新区域的叶子区块链结构时，则要完成平行链扩充。

图fig:treestruct中的双链结构和多链结构可以完成平行链扩充，而对于单链结构，由于区块链中不具备基本层级结构，无法完成结构扩充。在图中的双链结构中，由于当前叶子区块链的地理区域范围为1位geohash编码，因此只能增加1位geohash编码区域的平行区块链，如图中步骤1。在多链结构中，可以建立叶子区块链的平行链，如图中步骤2，建立geohash编码为wn的叶子区块链；或者构建某个分支区块链的平行链，如图中步骤3，首先建立分支区块链w的平行链中geohash编码为x的分支区块，然后再建立两个geohash编码分别为$x1$和$x2$的分支区块，从而构建两个叶子区块链。

层次结构初始化过程：

1. 树状区块链的层次结构初始化过程按照区域范围由大到小的顺序建立，即先建立大区域的层级，再建立小区域层级。eg:先建立分支区块w，再建立分支区块wx。
2. 下层的分支节点需要首先获得上层分支节点的分支区块信息后，再建立自身区域的分支区块。
3. 叶子节点为可以构建分支区块的最底层节点，在获取所有上层分支区块信息后，建立自身区域的分支区块即叶子区块，然后将叶子区块反馈给上层节点。
4. 叶子节点在具备叶子区块后，可以完成普通区块打包过程。
5. 叶子节点只打包发生在该区域内的交易。位置为w1的交易超出叶子节点区域范围wx，则需要给交易发送方反馈超范围消息，然后记录账户跨链消息，并将该跨链消息发送给父链的分支节点。
    1. 如果分支节点中存在编码为w1的分支区域，说明该存在该分支，完成账户跨链工作即可。
    2. 如果所有上层分支节点中都没有找到该分支区域，说明还未建立对应分支区域，则需要等待分支区域建立完成后，再完成跨链工作。
    3. 在等待对应分支区域建立过程中，账户的来源链叶子节点需要缓存跨链交易，并要求跨链账户等待目标链建立。
6. 假设各个区域的物理设备（分支节点）随时可用，不存在找不到合适设备作为结构性节点的情况。

3.4 分支节点区域状态缓存

树状多链中各个叶子区块链相互独立，其内部的区域状态互不影响。然而整个树状区块链是完整区域状态的汇总，在上层分支区块链中，分支节点对所有子链的区域状态具备汇总功能。

分支节点的本地缓存与叶子节点不同，分支节点缓存汇总后的区域状态树。分支节点缓存的区域状态树由所有直接子链的汇总信息构建而成，为数据一致性和不可篡改性提供保证。汇总过程中遵循两个排列规则：（1）时间顺序规则。多个子链的区域状态列表数据首先按照时间先后顺序排序；（2）区域geohash编码顺序规则。当同一个时间有多个区域状态时，则按照区域的geohash编码顺序再次排序。分支节点的区域状态树不需要再存入数据库中。汇总以叶子区块链有新交易开始，逐层向上修改各层分支节点中缓存的区域状态树。

分支节点汇总区域状态缓存过程以收到子链区块同步信息开始，不限定一次汇总的区块或区域数目。若同时有多个子链有待汇总信息时，只需要完成一次区域状态汇总过程，从而提高效率。

分支节点汇总区域状态还为区域状态查询提供方便。当需要查询某个区域内的区域信息时，只需要向对应分支节点请求查询即可。

（应该加一个图）

4 跨区域资产转移

树状多链通过账户位置变化表示移动性，通过账户发送的位置交易来改变账户位置。当车联网移动节点从一个子链区域移动入另一个子链区域时，除了位置发生变化，还需要在子链间维持账户余额的一致性。

（资产跨区域转移过程画一个图）

（1）准备过程

1. 账户注册。移动节点首先需要在第一个子链中完成账户注册和密码设定，并保存好账户的keystore。账户为全网账户，各个子链记录账户在当前链的状态和交易。
2. 账户位置判断。车辆账户主动发送包含位置的交易，在打包交易时，矿工节点会判断交易发送的位置信息。若位置在本区块链地理范围内，则可接受该交易；若超出范围，则拒绝该交易，并返回账户位置超出范围提示。

   （画一个账户位置判断过程图）
3. 账户复制。当账户位置超出原有区块链范围，移至新子链时，需要将账户的keystore文件复制到对应子链的文件夹下，在新子链中仍然使用来源链的账户ID和密码。

（2）跨区域资产转移过程

由于账户余额只在当前区块链中存在，而在新链中没有余额可用，则需要通过跨链资产转移将账户余额从来源链转入目标链；同时为了维护账户的活跃度唯一，只有在活跃链中账户余额不为0，其他子链中账户余额都为0。设计资产转移交易，该交易区别于普通交易和合约交易，专门为跨链资产转移设计。资产转移交易分为资产转出交易和资产转入交易两部分。

设计资产管理账户（Asset Management Account，简称AMA），负责管理跨链移动账户的资产转移。每个分支节点都有公开的资产管理账户，叶子节点维护所有上层父链分支节点的资产管理账户列表。由于账户唯一性要求，对复制到新链的账户需要在资产转入进行身份验证。跨链资产转移过程由内部资产转移合约实现。

1. 跨链资产转移请求交易TX_request。跨链账户在新链中没有余额可用，需要完成跨链资产转移。而资产来源链即活跃链需要通过向分支节点查询账户状态获取。因此需要账户主动向父链的资产管理账户发起跨链资产转移请求交易，交易内容为（from:CN1,to:AMA）。
2. 活跃链查询。叶子节点有当前活跃账户信息，分支节点有汇总后的活跃账户信息。父链在收到TX_request交易后，会查询账户CN1的活跃链位置，如果当前父链范围内不存在待查询账户的活跃链，则逐层向上层父链请求，直到返回活跃链位置，此父链即为资产转移前后的共同父链。对于初始账户，查询到最上层父链仍没有查询到活跃链，则返回查询失败，说明账户为第一次出现在整个多链中。
3. 资产转出交易TX_out。车辆账户在来源链中向父链的资产管理账户发送资产转出交易，交易内容为(from:CN1,to:AMA_out,value:CN1.balance,location:AMA_out_location,hashed:CN1_hashvalue)，其中转移的value为车辆账户的全部余额，交易位置为资产管理账户所在位置。TX_out打包成功后，分支节点BN1保存Out Data列表，记录资产转出信息out_data：TX_out_hash为资产转出交易哈希值，block_num为资产转出交易所在区块编号，tx_trie_root为资产转出交易所在区块的交易树根哈希，acc_value记录转出的账户余额。
4. 资产转入交易TX_in。在目标链中用父链资产管理账户向车辆账户发送资产转入交易，交易内容为（from:AMA_in,to:CN1,value:acc_value,location:AMA_in_location,hashed:CN1_hashvalue,exdata:rlp(out_data))。其中，资产转出信息out_data作为附加信息记录在资产转入交易中。返回资产转入成功信息in_data（TX_in_hash为资产转入交易哈希值，block_num为资产转入交易所在区块编号，tx_trie_root为资产转入交易所在区块的交易树根哈希）给分支节点，资产转移过程结束。由于资产转入交易是在资产转出交易打包入区块后才完成的，保证了资产转移的交易顺序和整个跨链资产转移过程的原子性；同时，资产转入交易中记录资产转出交易相关的转出信息，实现资产转移交易的可验证和可追踪性。虽然增加了父链资产管理功能，但资产转移工作是由账户自己发起的，转移的资产数目已知，且资产转出交易可验证，保证了跨链资产转移的安全性。
5. 资产转移状态记录TX_result。分支节点会为每个资产转出记录设定有效时间valid time，如果在有效时间内收到资产转入成功信息in_data，则将对应资产转移信息的result标记为sucess，同时in_data作为交易的附加数据写回来源链中；如果在有效时间内没有收到资产转入成功信息，则将

对应result标记为fail，同时发送资产回退交易，交易内容为（from:AMA_out,to:CN1,value:CN1.balance,exdata:rlp(in_data)），将未成功结果写回来源链。

（3）资产转移内部合约

由于父链节点完成移动账户在来源链和目标链两个子链间的跨链资产转移，整个过程由移动账户在目标链上发起资产转移请求开始，开始时来源链未知，因此跨链资产转移是内部合约的形式完成的，资产转移列表作为合约内部记录存在，内部合约由父节点访问，同时监控来源和目标两个子链。如表tab:assettransfer所示即为父链节点处的资产转移列表。

表 tab:assettransfer

编号	账户ID	TX_request	来源链	目标链	开始时间	TX_out	out_data	Tx_in	in_data	result
1	acc1	request1	out_c1	in_c1	time1	tout1	odata1	tin1	idata1	sucess
2	acc2	request2	out_c2	in_c2	time2	tout2	odata2	---	---	fail

其中，来源链为Tx_trans_chain。目标链为Tx_request_chain。开始时间为Tx_request_time。trans_value和req_value用于资产转移身份验证。result有两个，当Tx_in_time<=Tx_request_time+valid_time时，资产转移成功；否则，在valid_time内未收到Tx_in，则资产转移失败。

资产转移列表一条记录完成后，根据该条记录的结果，完成结果反馈。反馈结果有两种：

1. 转入交易在valid_time成功：资产转移状态标记为sucess，分支账户向来源链发送转出成功交易Tx_out_success。
2. 转入交易在valid_time未成功：资产转移状态标记为fail；分支账户向来源链发送转出失败交易，转出金额退回转出账户Tx_out_fail；分支账户向目标链发送转入失败交易，转入交易取消，Tx_in_fail。

（4）讨论

1. 身份一致。在查询到活跃链后，为了保证跨链资产转移的安全性，只能向目标链中相同账户ID转入资产，从而保证身份一致性。
2. 原有区块链的交易要求全网连通，而在现在的多链环境下只在有跨链需求时才要求跨链分支范围内网络连通，链内交易不要求全网连通，从而降低对网络连通程度的要求。
3. 资产管理账户的安全性保证。资产管理账户为分支节点具有的特殊类型账户，由于分支节点的身份具有全网可见性，通过账户与物理位置（分支节点位置固定）和物理实体（例如，车联网中的路侧节点作为分支节点）相结合的方式实现绑定，从而保证账户的安全性。同时，由于该类型账户的物理特性，可通过实际物理资产的抵押来保证账户安全性。
    1. 绑定机制。资产管理账户与分支节点的物理资产绑定，从而保证特殊账户的安全性。
    2. 授权机制。树状多链自顶向下逐层建立，下层链通过上层链授权建立，上层父链对子链有管理作用，各层区块链数据是逐层汇总从而构建为树状区块链，是逻辑单链结构。分支节点记录所有子链建立的信息。同时，账户通过授权获得角色（分支账户，移动账户），分支节点记录账户角色信息。
    3. 跨链资产转移合约。属于区块链内置合约，用于分支节点完成跨链资产转移工作。在逻辑单链结构中，由跨链资产转移合约维护的跨链交易仍然属于链内交易。分支节点可以访问跨链资产转移合约，记录子链资产转移信息，维护跨链资产转移交易的原子性和资产来源链和目标链的一致性，可验证性。跨链资产转移合约由目标链的资产转移请求触发。

5 实验与评价

1. 数据量对比：分别对比2个子链和4个子链区域情况下，原始区块链、物理位置区块链和树状多链的子链数据量对比
2. 吞吐量对比：分别对比2个子链和4个子链区域情况下，原始区块链、物理位置区块链和树状多链的吞吐量对比
3. 区域交易查询时间对比：分别对比2个子链和4个子链区域情况下，原始区块链、物理位置区块链和树状多链的相同区域的区域交易查询时间对比
4. 跨区域资产转移可用性实验？说明成功了？再统计一下成功的时间？
5. 出租车调度一起相结合的实验

6 结论