高技术通讯 2017 年 第 27 卷 第 11 – 12 期:875 ~ 888

doi:10.3772/j.issn.1002-0470.2017.11 – 12.001

区块链全局账本数据的拆分技术研究①

于 雷②*** 金 岩**

(*中国科学院大学 北京 100049)

(**中国科学院计算技术研究所计算机应用研究中心 北京 100190)

摘 要 分析了区块链用于交易网络的技术特点,指出在目前的区块链技术架构中,交易数据和新区块数据的泛洪式全网广播及全局区块链数据在所有共识节点全复制存储,成为区块链系统规模扩展的瓶颈。考虑到区块链网络存在交易频率局部性这一特征,提出了将区块链全网共识划分为若干区域子网共识的方法,并解决了网络划分前后的"双花"问题、节点的跨区移动和跨区支付问题,使得网络 I/O 负载和区块链数据存储负载在全网均匀划分。该方法是在区块链原有核心协议基础上进行的优化和改进,因此,并不会引入额外的安全问题。最后,利用数学方法理论分析了划分区块链网络前后的系统整体负载变化情况,证明了该方法在资源消耗方面具有明显的优势。

关键词 区块链,数据分区,拆分技术,双花问题,跨区交易,扩展性

0 引 言

近年,以比特币为代表的数字货币实践得到广泛关注,数字货币的底层技术平台是区块链(blockchain)技术,区块链的核心协议可以概括为以下几个技术术语的组合:P2P 网络、基于非对称秘钥机制的签名验证、全网共同遵守的当前时间段交易信息共识、基于单向 Hash 算法的交易历史链式数据结构,Nakamoto[1]对此进行了详细的描述。可以将区块链技术的本质视为分布式数据库,该数据库保存历史交易数据,这个数据库被所有节点通过分布式一致协议共享[2]。区块链技术的核心价值包括去中心化,分布式共识、非对称秘钥的签名和加密、时间戳,在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作,从而为解决中心化机构普遍存在的高成本、信用垄断、可靠性依赖等问题提供了解决方案。具体的区块链的定义可描述如下:区块链是一种按照时间顺序将数据区块用类似链表的方式组成的数据结构,并以分布式共识和密码学方式保证区块链的数据全局一致、不可篡改和不可伪造的分布式去中心化账本,能够安全存储简单的、有先后关系的、能在系统内进行验证的数据[3]。区块链的出现解决了数字货币的两大问题:双重支付问题以及拜占庭将军问题[4-9]。区块链技术在金融、保险、支付、公证等领域有广阔的应用前景。本研究根据现实中的交易网络具有明显的局部特征,提出了一种将全局区块链网络划分成若干区域区块链子网的方法,该方法通过拆分全局区块链数据,解决了区块链全局账本不断膨胀造成的存储瓶颈问题,依据交易方之间的局部性特征,减少了区块链网络节点的存储需求、算力需求和区块链网络带宽需求。该方法没有改变区块链的核心协议,没有引入新的安全问题。

1 区块链的基本结构

一般而言,区块链应用可以分为两类:

① 国家自然科学基金(No.61202413)资助项目。

② 男,1981 年生,博士生;研究方向:区块链,大数据;联系人,E-mail:yulei@ncic.ac.cn

(收稿日期:2017-06-26)

（1）公有链（public blockchains）：所有节点都可以参与共识、竞争记账权。任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，数据公开。其特点是中立、开放、交易速度慢、需要“挖矿”或类似共识机制，常用 P2P 网络，抗审查性高。

（2）许可链（permissioned blockchains）：只有被许可的节点才能共识、竞争记账权并创建区块，包含私有链、联盟链、企业链等所有非公有链。数据可以公开或不公开。其特点是交易速度快、不需要“挖矿”类的全网共识、交易成本低（交易只需几个许可节点验证即可），可审查，会占据商业应用领域的主流。

当前，区块链技术并没有形成行业标准，基本的区块链的数据结构如图 1 所示。

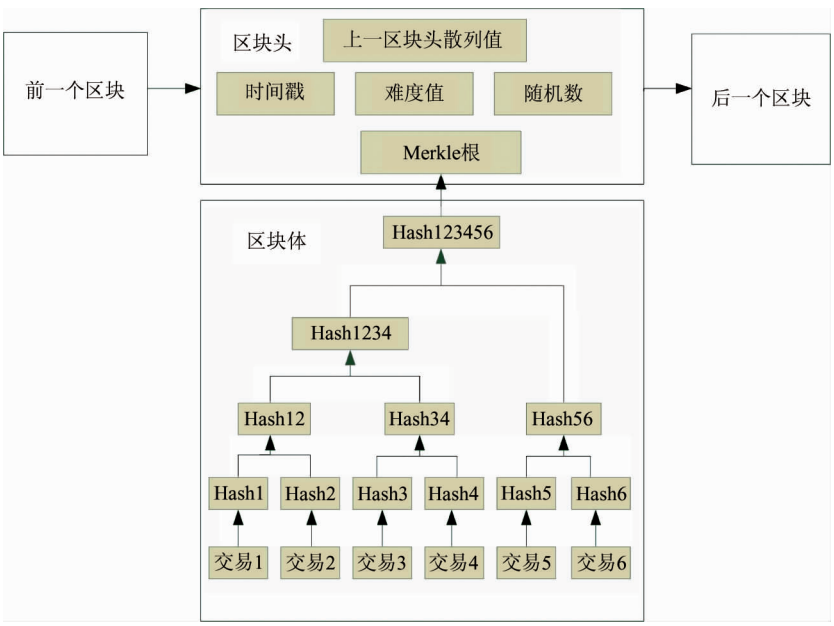

图 1　区块链的基本数据结构

区块链协议中的链式结构、交易信息的 Merkle 树和共识机制，保证了历史交易数据极难被篡改，其中的交易数据为本段时间内的交易单信息，其中的交易单的逻辑结构如图 2 所示。

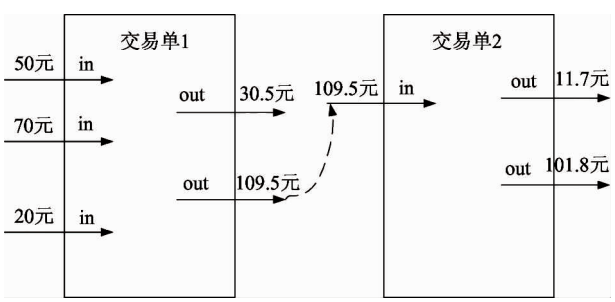

图 2　区块体中交易单的逻辑结构

从创世区块开始，区块链历史账本数据中，包含了数字资产的首尾相接转账交易单构成的交易链条，上一个交易单的输出（out）成为当前交易单的输入（in），当前交易单的 out，又可以作为下一个交易单的 in，每个交易单的具体数据结构如下：

```
{
    Hash:[代表本交易单的哈希值],
    in: //收入来源项内容
    {
        prev _ out: //前置交易信息
        {
            Hash:[代表前置交易的哈希值],
            n:[代表输出项 out 的索引值]
        },
        scriptSig: < sig > < pubKey > //拥有者的签名和公钥
    },
```

```
    out: //支出去向项内容
    {
        value:[付款金额],
        address: [代表收款方地址的哈希值]
        scriptPubKey: 脚本内容
            验证使用者的公钥地址与当前指向的公钥地址哈希值匹配(基于非对称秘钥机制);
            验证使用者的数字签名与使用者的公钥匹配(基于非对称秘钥机制);
    },
}
```

首尾相接的交易单数据(包含交易发送方的数字签名)经过脚本内容的验证为合法后,被不同时间戳的区块进行记录,构成首尾相接的区块链的数据主体。区块链网络的节点通过共识过程,竞争交易单的记账权,避免“双花”问题,避免历史交易数据被轻易篡改。

基于去中心化的点对点交易需求以及系统可靠性方面的考虑,区块链技术普遍基于 P2P 网络,网络中的每个节点以扁平式拓扑结构相互连通和交互,不存在任何中心化的特殊节点、不存在层级结构,每个节点均会承担网络路由、验证交易单、验证区块数据、传播区块数据、发现新节点等功能。按照节点存储数据量的不同,网络中的节点可以分为全数据节点和轻量级节点。前者保存从创世区块到当前最新区块为止的完整区块链账本,并通过实时参与全网共识过程,进行竞争记账来动态更新主链。全数据节点(或称全节点)的优势在于不依赖任何其他节点而能够独立地实现任意区块数据的校验、查询和更新,劣势则是维护全节点的空间成本较高。以比特币为例,截止到 2017 年 6 月,创世区块至当前区块的数据量已经超过 100GB。与之相比,轻量级节点则仅保存一部分区块链中的区块头数据,并通过“简易支付验证方式”向其相邻节点请求所需的数据来完成交易单数据的校验。

区块链作为新兴技术,还有很多问题亟待完善,区块链协议面临着扩展性的障碍[10-13]。区块链的扩展性问题大致分为两个方面:交易吞吐量和交易确认延迟的扩展性障碍,区块链全局账本数据存储瓶颈造成的扩展性障碍。同时,这两个方面的扩展性问题又是相互矛盾的联系在一起的。以比特币的区块链应用为例,比特币区块大小限制在 1MB,每 10min 形成一个新区块,每年的数据增长的最大为 52GB,此时能提供的交易吞吐率是6.7笔/s[14],如果要增加比特币的交易吞吐量,可以增加区块大小,但是会使得存储扩展性问题更趋严重,以达到支付宝或 VISA 的水平为参考(10000 笔/s),这将造成每年的数据增长量为 7TB,这种情况下,运行区块链全数据节点将变得异常困难,这将与区块链希望尽可能多的节点运行全数据节点的要求相悖;也可以通过减少区块生成间隔的方式增加交易吞吐量,同时也减少了交易的确认时间,但是这种方式会降低整个区块链网络的稳定性、降低数据防篡改能力,同样会线性增加区块链的全节点存储需求。无论如何,区块链账本数据量会随时间越来越大,尤其是以区块链中的公有链为代表,区块链全局账本数据需要在公有链的尽可能多的节点进行全复制存储。

以比特币为代表的公有链类型,有个假设的前提即为在整个区块链的 P2P 网络中,任意两点之间发生交易的概率是一致的。以此为前提,全网所有节点(全节点)共享存储一个相同的分布式账本数据,全网所有新的交易信息都在此唯一账本后追加,新交易信息通过共识机制形成的新区块被全网节点接受后,链接到此唯一账本中,在每个节点存储完整的账本副本,如此反复。这样形成的全网共享的唯一账本构成了全网任意节点之间交易的基础信息。

2　相关研究

区块链技术的发展,从第一代比特币到第二代以太坊,都面临严峻的可扩展性问题。扩展性与去中心化特性之间形成了现实的矛盾。比特币社区提出了将 UTXO 数据结构分区存储的建议[15],在《以太坊白皮书》中也提到了可无限扩张的方案,但是都未真正实现。除此之外,有些方案干脆放弃区块链的定义来解决可扩展性问题,例如 Bigchain-DB[10]、VaultOS[11]、RSCoin[12],它们解决了交易吞吐量、交易确认延迟和区块链数据存储两方面的扩展性问题,但是他们放弃了区块链的本质定义。这些都是类似区块链的系统,它们改变了传统区块链

的架构,一般来说安全性比较差。这些已经偏离传统区块链的定义系统,能否被市场接受还有待观察。除此之外,已有很多相关的研究和讨论提供了解决区块链应用的交易吞吐量、交易确认延迟的问题[16-21]。Bitcoin-NG[22]在类似比特币系统的区块链应用中,一定程度上解决了交易延迟和交易吞吐量的扩展性限制。Bitcoin-NG 将区块的生成过程划分为两个过程,分别是 leader 的选举过程和交易的序列化过程,解决了两个问题:(1)区块大小在交易吞吐量和区块在网络的传播速度之间的矛盾;(2)区块生成间隔在系统稳定性(或称安全性)和交易延迟之间的矛盾。从而,提高了比特币类型区块链应用的交易吞吐量,缩短了交易延迟,但是,Bitcoin-NG 没有解决区块链数据快速膨胀给全节点造成的存储瓶颈问题,从而使得区块链应用的扩展性依然受制于节点的全区块链账本存储能力。容许区块链框架(permissioned blockchain framework,PBF)[23]提出了将区块链的 P2P 网络进行分区的方法,通过随机地将 P2P 网络划分为若干子网,避免非诚实的节点在少数子网的聚集,在每个子网内部的节点收录子网内产生的交易单信息,并通过子网内部的一致性的共识机制创建子块,另有两个“特别委员会”节点集,第一个“特别委员会”验证每个子块包含的交易信息的合法性,第二个“特别委员会”将各个子网的子块写入全局区块,最后链入全局区块链的末尾。PBF 同样提高了交易吞吐量、缩短了交易确认的延迟,同时,没有牺牲系统稳定性(或称安全性)。但是 PBF 依然存在全局区块链的多复制存储瓶颈问题,并没有拆分全局区块链数据到各个子网中。文献[24]提出了区块链数据快速膨胀的问题的解决方法:不管区块链网络规模有多大,通过删除历史交易单数据,可以将区块链的“全局区块链账本”数据保持在固定的大小,这种数据删除的方法降低了低资源用户的准入门槛,使得很多移动终端用户可以参与到区块链的全局共识中,从而提高了区块链网络的稳定性和可靠性,文中通过 B 语言深入分析了该方法与传统区块链协议之间的安全性差异,证明了删除历史交易单的方法在解决存储瓶颈问题的同时,没有带来新的安全问题。但是,在去中心化的数字货币应用中,没有中心发行方的数字货币的信用,建立在区块链账本数据的交易历史可追溯之上,从“造币”交易到最近一次的转账交易都可追溯,形成了数字货币的信用基础,通过删除交易历史数据来减少区块链数据存储需求,破坏了去中心化的数字货币信用基础。

3 区块链全网划分为若干区块链子网

3.1 划分子网的过程与划分方式

现实中,某些交易场景下,全网任意节点之间发生交易概率并不相同,具有明显的局部性特征,即区块链的 P2P 全网之中,某些地域内(如地市内)节点之间发生交易的概率大大高于与地域之外节点发生交易的概率,或某些团体内(如汽车行业供应链企业之间)的节点之间发生交易的概率大大高于与团体之外节点发生交易的概率,利用这样的交易概率局部性,可以实现全网账本数据的拆分,同时将交易信息的记账负载进行拆分。当然,这样的拆分不能影响到全网任意节点之间都可进行交易的功能。

首先,依据交易的频繁程度,将区块链的 P2P 全网划分为若干个交易区域子网,网络划分的示意图如图 3 所示。

本文以基于地域局部性特征为例,说明网络的具体划分方法和过程。基于团体交易局部性特征的网络划分方法与此类似,不再赘述。

首先,需要将区块链全网覆盖的地域范围进行细粒度的分区,区域分区的粒度等于可预见的区块链网络可实际划分的最小粒度,给每个分区赋予一个全局唯一的编号值。划分区域的方式可以借用现实的行政地域划分方法,以区块链交易网络覆盖全中国为例。可以预计,全网划分子网覆盖一个县域就已经足够小了,因此可将全国的每个县分配一个唯一编号值,以县域作为划分子网的最小粒度。每个区块链的节点记录自身所在的地域属性值(地域划分的最小粒度的属性值,例如某个县域值),且每个区域的节点应该保存全网所有的区域编号信息。网络的具体划分过程叙述如下。

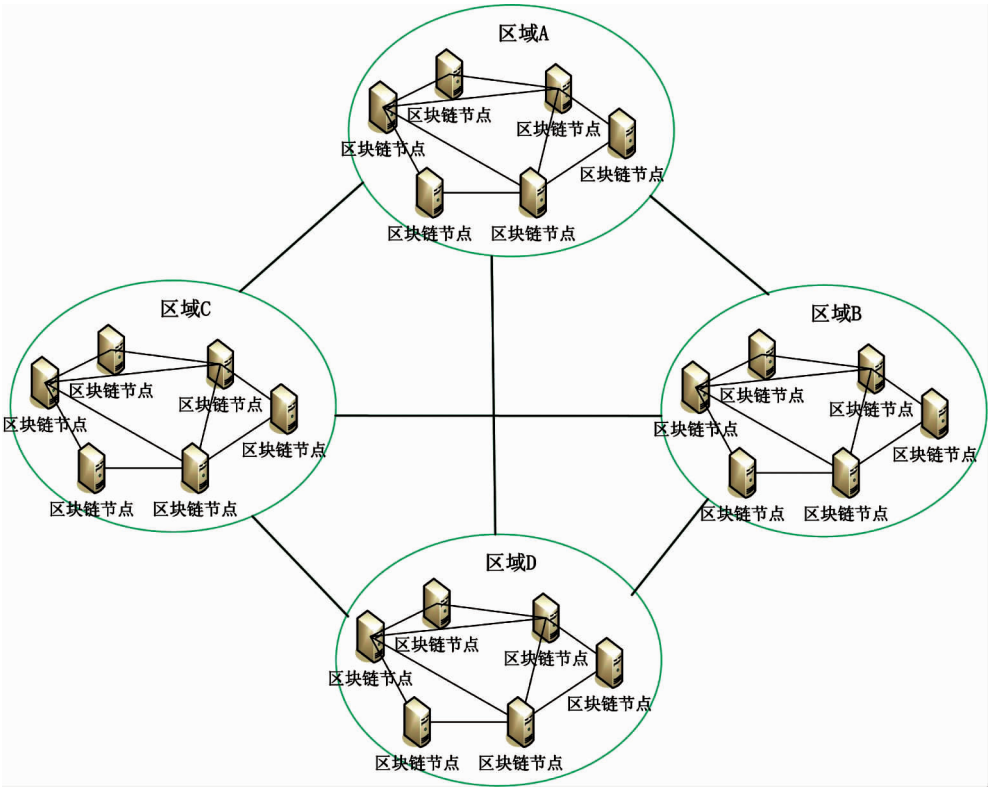

图 3　区块链的 P2P 网络划分示意图

(1) 初始状态。从创世区块开始,全网所有节点只被分成一个交易区域,全网所有节点参与全区域的共识机制,共同维护一个相同的区块链账本数据,随着节点交易数据的累计,全局区块链的区块数不断增长。

(2) 通过对历史区块链中交易数据的“学习”,逐渐形成交易节点之间的“热度矩阵”。学习过程:首先全网所有节点之间两两热度值初始设置为 0,此后,两个交易节点之间每发生一次交易行为,这两个节点之间的热度值加 1,经过一段时间,两两交易节点之间的热度值形成一个“热度矩阵”。

(3) 依据“交易热度矩阵”,在全局的交易节点群中,依据聚类方法(可灵活选择),对交易节点进行聚类过程,识别交易联系紧密的交易节点群。将这样的交易节点集群划分为多个交易节点子区块链网络,对子网中所有交易节点所在区域属性值求取并集,得出该子网的覆盖区域范围,并记录在每个子网节点中,即子网节点记录当前所在子网的共识范围地域编号列表。

(4) 每个区块链子网以当前全局区块链账本数据,作为拆分后的区域区块链账本数据的起点。从这个起点开始,每个节点只收录记账本区域(或称本子网)节点之间的交易单和本区域(或称本子网)节点跨区转账的交易单,通过本区域内(或称本子网内)的共识机制,将新区块加入本区域的区块链末尾。

(5) 随着新的交易节点加入某个区域的区块链网络,区域区块链网络规模不断扩大。通过“学习”子网内的历史交易数据,可以选择继续分裂当前的子网为更小的若干子区块链网络(每个子网覆盖的区域范围更小),分裂过程与(1)至(4)叙述的过程一致,分裂之后的子区块链网络以原区域的区块链网络账本数据作为起点。新子网内的节点开始收录记账子区域内的交易单数据和子区域的节点跨区产生的交易单数据,通过子区域共识将新交易单记入区块链末尾。

在区块链网络分裂开始前,全局区块链数据中,“所有未使用的交易输出 out”作为当前交易单转账交易的前置输入交易,必须随着网络进行分割。如前所述,每个子区块链网络节点记录了当前节点的

共识范围列表(见表 1),该列表记录了该节点参与的共识区域范围,或称记账范围,这个范围通过区域集合的形式描述。在每笔交易单的输出项 out 中添加区域编号(区域划分后的某个最小粒度值的编号,如某个县的编号),该编号记录该 out 项的输出指向区域,也就是说,给该笔转账的数字资产赋予了当前所在区域的属性(如在某个县)。

交易类型的交易单的数据结构示例如下:

{

Hash:[代表本交易单的哈希值],

in://收入来源项内容

{

prev_out://前置交易信息

{

Hash:[代表前置交易的哈希值],

n:[代表输出项 out 的索引值]

},

scriptSig:〈sig〉〈pubKey〉//拥有者的签名和公钥

},

out://支出去向项内容

{

value:[付款金额],

address:[代表收款方地址的哈希值]

locationNO:[输出指向的目的地编号,例如:10017]

scriptPubKey:脚本内容

验证使用者的公钥地址与当前指向的公钥地址哈希值匹配(基于非对称秘钥机制);

验证使用者的数字签名与使用者的公钥匹配(基于非对称秘钥机制);

},

}

共识节点接收到的交易单,其前置交易单的输出项 out 中的指向目的地 locationNO 在当前节点的共识范围列表汇总时,才被当前节点接受并验证。

初始状态,全网所有节点收录交易单的范围都是全集,即每个交易节点向其它所有共识记账节点广播交易单信息,区块链网络中每个参与共识的节点,其共识区域范围列表都为全集(All)(见图 4)。

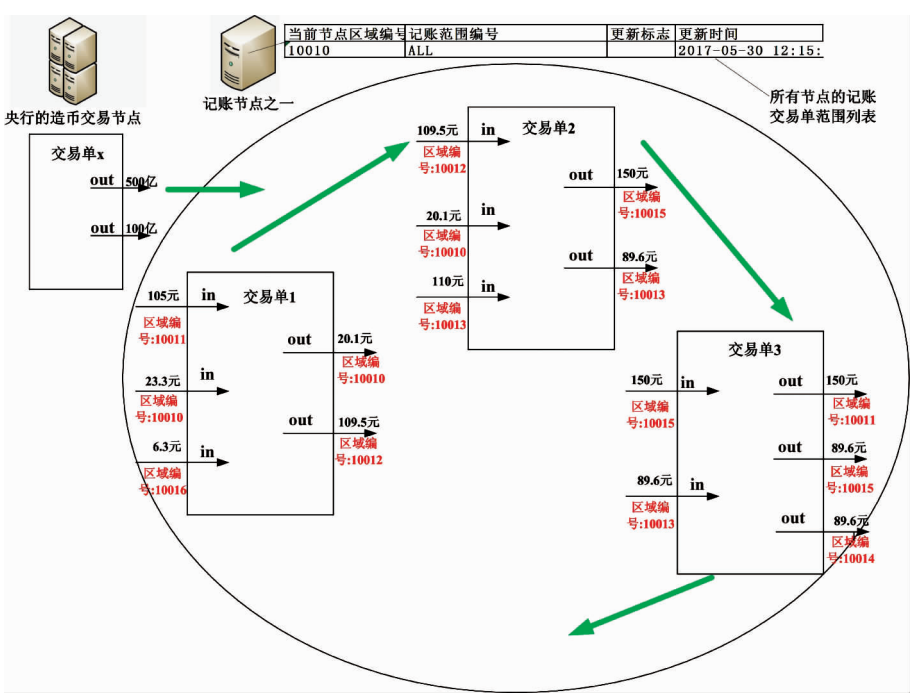

图 4　初始状态所有节点的共识范围为 All,全网节点维护共享的统一账本

由于交易负载不断增长,网络管理模块通过历史交易单的查询获得交易双方之间的局部性信息,网络开始分裂过程。分裂管理模块向所有节点发送全网消息,消息内容包括以区域编号为单位的分区方式信息,交易节点依据新的网络分区方式,更新自身的共识范围列表(见表1)。

表1　记账节点存储的共识范围列表

当前节点区域编号	共识范围编号	更新标志	更新时间
10010	All	0	2017-06-26 01:30:00
10010	10017,10011,10015,12013,14401	1	2017-06-30 12:15:37

图5中的中心网络管理模块和区域网络管理模块,分别负责管理全网和划分之后的区域网络状态,具体的功能如下。

(1)学习当前网络内的交易节点局部性信息。

(2)向管理的网络节点发送网络状态改变消息(可通过公开消息Hash摘要的方式保证消息的完整性)。

(3)监测当前管理的网络状态信息,保证这些状态信息在当前网络中同步。

网络拆分之后,每个子网节点参与共识记账过程时,只能收录这样的交易单:

(1)前置交易项来自“所有未使用的交易输出”。

(2)前置交易单的输出项指向的地域编号在本节点的共识地域编号列表范围内。

以上两个条件必须同时满足,以避免“所有未使用的交易输出”在全网划分后,被多个子网的交易单同时使用,即避免网络划分前后的“双花”问题。

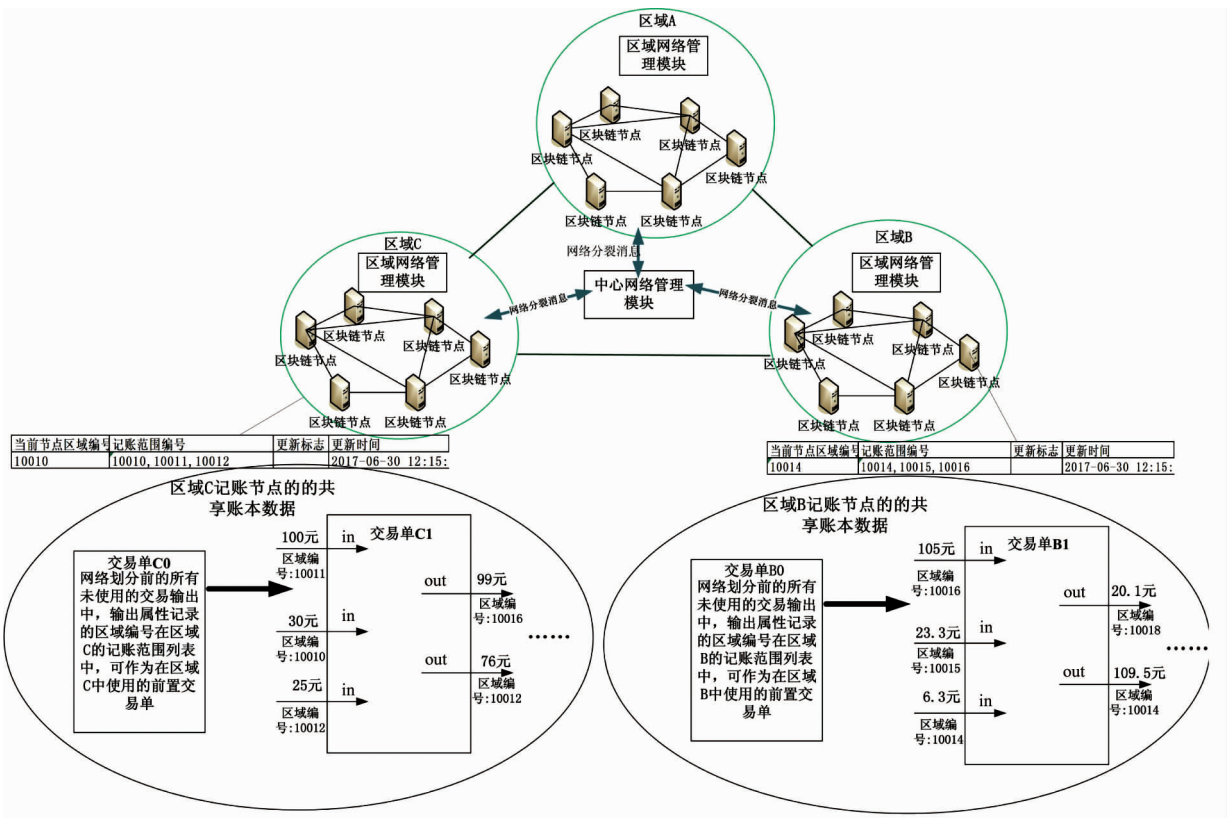

图5　划分多个区域后,所有未使用的交易输出同时被划分

网络划分为多个子网,在基于交易热度划分的基础上,需要额外保证各个子网的并集覆盖全网,同时各个子网之间无节点交叉。在网络划分过程中,处在两个子网划分边缘的交易热度较低的节点,无论选择进入哪个子网,都不会影响子网划分的正确性,这是因为子网内交易热度低的节点对所在子网的区块链数据负载和网络 I/O 负载的变化不会产生很大影响,因此可以将处在多个划分子网边缘的交易热度较低的节点,随机地选择划分到某个子网内,这不会影响到划分子网意义的正确性——拆分全局账本数据、拆分全局交易负载。

3.2　交易记账过程

在全网划分为若干区域子网之后,每个区域子网不再参与全局共识(也已经不存在全局共识),每个区域子网的交易节点只保留本区域交易节点之间的交易单信息。在本区域节点内,通过区域内的共识机制竞争记账(POS 或 POW 共识机制),本区域的节点以划分前的区块链全局账本数据为起点,在其后链接新的区域区块,区域内的新区块只收录区域内的交易单,也就是说,本区域区块体只记录本区域交易节点之间交易单数据。在区域交易单的属性信息中,应该加入本区域的全局唯一编号信息,用于标示该交易单的属地区域。

此后,当个人在子网发起转账交易时,在区域区块链账本数据中,个人在“(分割之后的)所有未使用的交易输出集合”中,找到公钥地址属于本人可用的交易单输出,获知自己的“余额”信息并据此构造新的交易单。如图 6 所示。

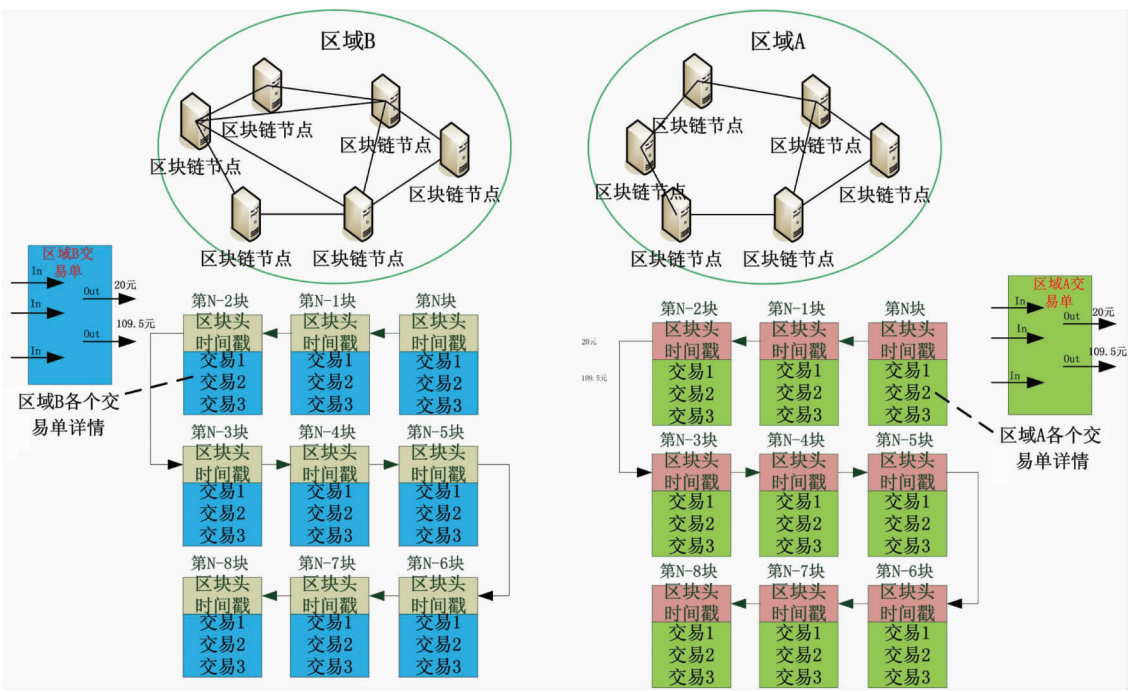

图 6　区域交易单被区域区块链记入

不难发现,这样的区域共享区块链账本,不可避免地带来了两个问题:(1) 节点跨区移动的问题;(2) 跨区域节点之间转账交易的问题。

第(1)个问题的解决方案有两种。

(i) 节点多公钥地址的解决方案(见图 7)。

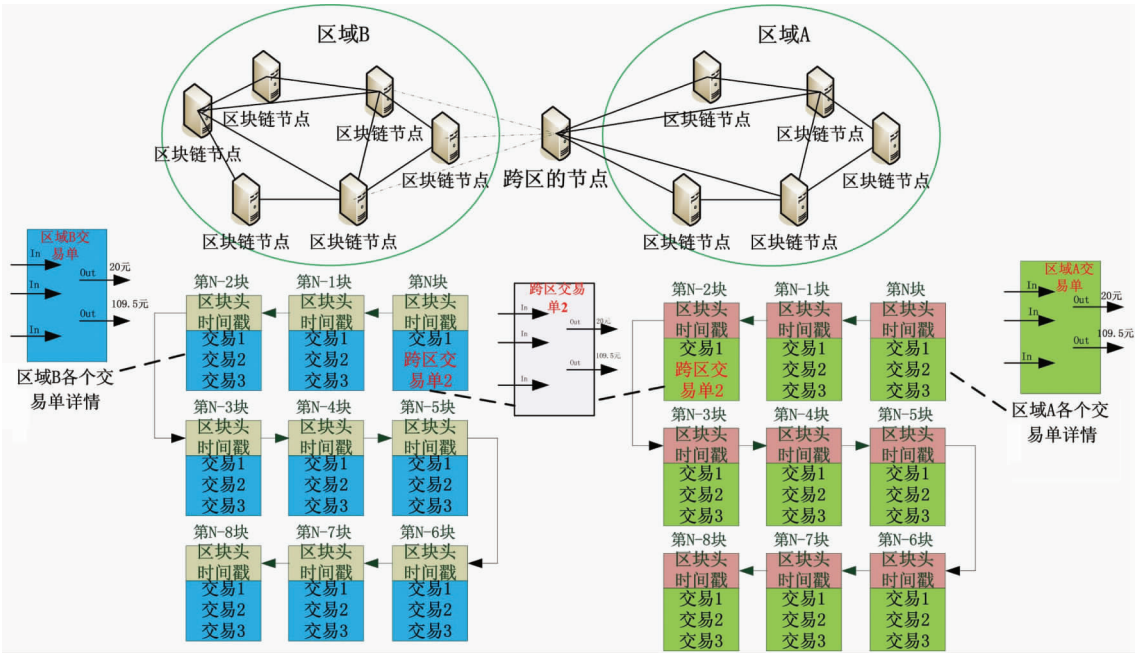

图 7　跨区交易单被两个区域的区块链共同记入

1）区块链交易节点 X 在原属地区域 A 有固定的公钥地址,通过区域 A 的交易节点之间的交易单历史数据,在区域 A 的分布式区块链账本的“所有未花费的输出”中,有属于节点 X 的若干可用的“交易输出”,即为数字资产。

2）区块链交易节点 X 进入区域 B 的区块链网络,节点 X 在该区域的分布式区块链账本中,暂时没有可用的“交易输出”,交易节点 X 发现自己跨区后,生成该区域的公私钥对,作为 X 在该区域 B 的公钥地址,然后向原区域 A 的区块链网络发出交易请求,生成一个跨区交易单(当前交易单的 out 属性记录的区域编号 locationNO 属于区域 B,其前置交易单的 out 属性中记录的区域编号 locationNO 属于区域 A),该交易单的交易请求将交易节点 X 在原区域 A 的可用“交易输出”转账给节点 X 在区域 B 的新公钥地址上,该跨区交易单在区域 A 和区域 B“同时”被记入本地区块链的新区块中。

3）前述中,跨区交易单在区域 A 和区域 B“同时”被记入本地区块链账本,并非真正的同时,区域 B 在接收跨区交易单的时候,需要验证此交易单的合法性,但是区域 B 没有跨区交易单的前置交易单信息,无法完成验证。因此,需要区域 A 的区块链网络首先完成对跨区交易单的验证,并记入区域 A 的区块链的账本后,区域 B 区块链网络获得区域 A 已经将跨区交易单成功记账的消息后,才将跨区交易单记入区域 B 的区块链账本中。

4）区域 A 的对跨区交易单的验证过程与普通交易单的验证过程完全一致,其验证过程包括:(a)交易单的输入来源是否是区域 A 中的“所有未花费交易”;(b) 交易输入来源的公钥地址与节点 X 的公钥地址是否匹配;(c) 验证节点 X 数字签名。区域 A 的区块链网络完成此验证后,将交易单记入区域 A 的当前区块,并通过区域内的共识机制获得区域 A 的区块链网络确认。

5）区域 B 通过网络获知,区域 A 已经完成了对跨区交易单的确认,并且记入了区域 A 的区块链网络,可以借鉴比特币网络的“6 次确认”的机制,即区域 A 的区块链网络的跨区域交易单记入的区块之后,已经在区域 A 的区块链中链接了 6 个以上的新区块,此时,区域 B 的区块链网络确认跨区交易单被区域 A 接受并确认(无法篡改),区域 B 的区块链网络验证跨区交易单为合法交易单,并通过区域内的共识机制记入本区域 B 的区块链网络。至此,完成了节点 X 的跨区运动问题;

不难发现,这个过程既避免了子网区域内的“双花”问题,也避免了跨子网区域的“双花”问题。

因为,如果有两个区域,区域 B 和区域 C,节点 X 在区域 B 和区域 C,同时向原区域 A 发送跨区转账交易单,区域 A 在区域内的共识机制下,只有一个跨区交易单能被成功记入区域 A 的区块链账本数据中,也就是说区域 B 或区域 C 中,只有一个区域的区块链网络能获得跨区交易单被原区域成功记账通知,进而完成本区域的跨区交易单的共识记入区块链过程。

经过以上过程,实现了数字资产的跨区域转移,分区域拆分的区块链可以支持节点全网的任意转移。

(ii)节点单公钥地址解决方案(见图 8)

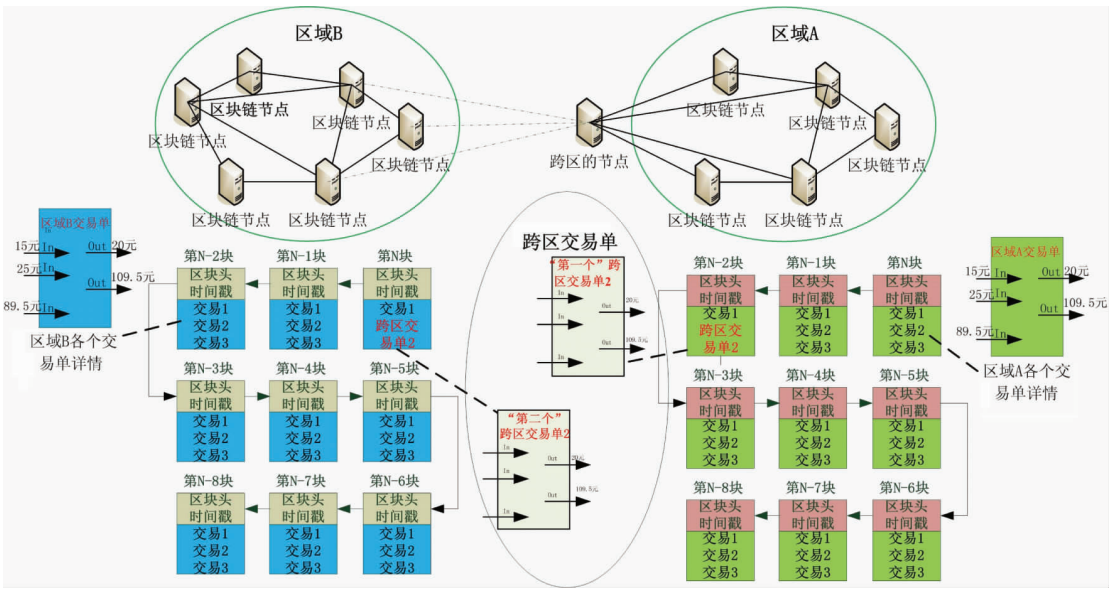

图 8　跨区交易形成的两个交易单在两个区域分别记入

1)节点 X 在全网有唯一固定公钥地址,通过交易节点之间的交易单的交易,在区域 A 的分布式账本"所有未花费的输出"数据库中有钱包 X 的若干可用数字资产。

2)节点 X 进入区域 B 的区块链网络,节点 X 在该暂时区域没有可用的数字资产,节点 X 发现自己跨区,然后向原区块链 A 区的记账节点发送两个相同的跨区交易单(当前交易单的 out 属性记录的区域编号 locationNO 属于区域 B,其前置交易单的 out 属性中记录的区域编号 locationNO 属于区域 A),跨区交易单将 A 区域的节点 X 的数字资产转账给 X 的原地址,该交易单首先在原区域 A 被记入当前区块;相同的跨区交易单被发送到区域 B,该交易单在区域 B 被记入当前区块。

3)前述中,两个跨区交易单在区域 A 和区域 B 被分别记入区域区块链中。区域 B 在接收跨区"第二个"交易单的时候,需要验证此交易单的合法性,但是区域 B 没有跨区交易单的前置交易单信息,无法完成验证。因此,需要区域 A 的区块链网络首先完成对"第一个"跨区交易单的验证,并记入区域 A 的区块链的账本后,区域 B 区块链网络获得区域 A 已经将跨区交易单成功记账的消息后,才将跨区交易单记入区域 B 的区块链账本中。

4)区域 A 的对跨区交易单的验证过程与普通交易单的验证过程完全一致,其验证过程包括:(a)交易单的输入来源是否是区域 A 中的"所有未花费交易";(b)交易输入来源的公钥地址与节点 X 的公钥地址是否匹配;(c)验证节点 X 数字签名。区域 A 的区块链网络完成此验证后,将交易单记入区域 A 的当前区块,并通过区域内的共识机制获得区域 A 的区块链网络确认。

5)区域 B 通过网络获知,区域 A 已经完成了对跨区交易单的确认,该交易单中的 out 输出属性信息记录的区域编号 locationNO 属于区域 B,该交

易单已记入了区域 A 的区块链网络,可以借鉴"6 次确认"的机制,即区域 A 的区块链网络的跨区域交易单记入的区块之后,又在其后链接了 6 个以上的新区块,此时,区域 B 的区块链网络确认跨区交易单被区域 A 接受并确认(无法篡改),区域 B 的即可验证该跨区交易单为合法,并通过区域内的共识机制记入本区域 B 的区块链网络。至此,完成节点 X 的跨区移动过程。

第(2)个问题,即跨区域节点之间的转账交易问题,其解决方案与第(1)个问题的第一种解决方案完全一致,在上述方案(第(1)个问题的第一种解决方案)中,节点 X 在区域 B 的新公钥地址视为区域 B 的一个节点 Y 即可,上述过程即变成了节点 X 在区域 A 向区域 B 的节点 Y 转账支付的过程,完成跨区交易单被两个区域的区块链子网络"同时"记账,也就完成了数字资产的在不同区域的转账支付过程,不再赘述。

4　区块链网络划分与"造币"机制

当前的区块链应用中,数字货币的应用为其中重要的一项,其中绝大多数的区块链数字货币应用中,都有"去中心化的造币机制",大致过程为某个节点通过某种算法支持的"挖矿"机制,竞争获得当前区块的生成权利,该区块包含了一个"造币"交易单,造币交易单的输出地址指向创建本区块的节点的公钥地址,该区块通过全网共识,被全网接受并链入全网共享的区块链账本数据中,这样,新的数字货币被创造出来并且获得全网的认可。但是,在本文中,区块链网络被逐渐划分为若干个子区块链网络,在每个子区块链网络内部,对新交易单及对应的新区块形成区域共识,这样的共识机制并没有延伸到区块链全网,因此,区域区块链网络共识的"造币"交易单将无法获得全网认可。

本文叙述的方法不适用于具有类似全局"造币"共识的经济激励机制的区块链应用,可适用于主权数字货币的区块链应用。这类应用不需要全局共识的"造币"交易作为激励,只需要特殊节点发起"造币"转账交易即可,这个特殊节点的身份类似于央行的角色,经过这样的类似央行的"造币"节点的数字签名的"造币"转账交易即为合法。

本文叙述的方法同时适用于区块链网络不再产生"造币"交易的区块链应用,例如,比特币网络在达到 2100 万的比特币总数之后,不再产生造币交易单,此后,可据此方式拆分区块链全局账本数据。

5　负载分析

5.1　算力负载分析

算力共识是公有链共识机制的基石,最典型的算力共识采用穷举法尝试随机值的方式,以"碰撞"极小范围的 Hash 值为目标。本文以算力共识为例,讨论网络划分前后的算力消耗变化。

首先,以保证网络划分前后,交易的记账及确认时间间隔不变为前提,即保证网络划分后,各个子网络生成区块的时间间隔与网络划分前全网生成区块的时间间隔一致,都为 $\triangle t$。为保证 $\triangle t$ 相同,网络划分后,需要将子网络内的目标 Hash 值的碰撞难度调低。在 $\triangle t$ 时间段内,无论是网络划分前,还是网络划分后,为竞争区块创建的权利,所有节点都在穷举随机值,试图碰撞到目标范围 Hash 值——全网共识的目标范围 Hash 值 H_1,或子网内共识的目标范围 Hash 值 H_2(如前所述,碰撞 H_1 的难度要高于碰撞 H_2),所有节点都在参与这个过程。穷举法算法的特点所致,无论目标 Hash 值的难度如何变化,每个节点每次的穷举尝试计算所消耗的算力资源都是一样的,因此,在保证网络划分前后 $\triangle t$ 不变的情况下,每个节点在 $\triangle t$ 时间段内穷举尝试的次数一致,所以,网络划分前后,全网消耗的算力资源是相同的。可见,区块链网络共识机制消耗大量算力的问题是由区块链的共识算法的选取决定的。

虽然网络划分前后,整体的算力消耗没有降低,但是在相同算力消耗的情况下,由于节省了大量的存储资源以及网络 I/O 资源,因此,在 $\triangle t$ 时间内,区块链系统在划分后的每个子网内都可达成"共识",这使得整个区块链系统在网络划分为多个子网之后,单位时间内可承载的交易单数量多于网络划分之前,即系统整体的费效比大大提高。

5.2 节点存储负载分析

假设以创世区块开始,到最后形成稳定的区块链区域子网,我们来分析一下区块数据增长量和记账负载的变化情况。

假设区块链全网节点数为 n, 每个节点单位时间产生 a 个交易单,每个交易单的数据量为 m, 如果全网共享一个账本数据,每个单位时间的数据增长量为 $L = a \times m \times n$。经过时间 T 后,全网的冗余数据量 R 为

$$R = n \times a \times m \times T \times (n - 1) \tag{1}$$

如果全网初始共享一个账本数据,通过一定时间 t 的历史交易数据学习,原全网节点拆分为 i 个区块链区域子网,拆分后,各个子网之间的跨网交易单数量与本区域内的交易单总数量中占比为 c,c 为 t 的函数,当 t 大于一定的数值后, c 值趋于稳定, t 和 c 之间可选的函数关系之一如下:

$$c = (1 + \frac{1}{t+1})^{t+1}/A,\ t \geqslant 0 \tag{2}$$

其中, A 为经验常数,代表了当前全局区块链网络中包含的交易局部性特征, A 值越大,局部性特征越强,反之,局部性特征越弱。

网络被划分为 i 个区块链子网后,假设每个子网的规模接近,设每个子网中,跨网交易单与区域区块链的总交易单的占比值相同,此后,单位时间内,全网每个节点的单位时间数据增长量为

$$L' = \frac{n}{i} \times a \times m + \frac{n}{i} \times a \times m \times c,\ 0 < c < 1 \tag{3}$$

通过上式可以看出,每个节点的单位时间区块数据增长量最大为未划分前的 $2n/i$ 倍,最小为未划分前的 n/i。

经过时间 T 后,全网的冗余数据量 R' 为

$$R' = n \times (n-1) \times a \times m \times t + 2n \times (\frac{n}{i} - 1) \times a \times m \times c \times (T - t) + n \times (\frac{n}{i} - 1) \times a \times m \times (T - t)$$

通过上式可知,全网划分成 i 个子网之后,全网冗余数据量取决于“学习”时间 t 、“学习”效果 c 以及交易具有的局部性特征 A。如果全网的交易行为具有明显的局部性特征,经过足够长的“学习”时间 t 之后,全网划分为若干区域子网, c 为稳定的常数,且接近 0,再经过足够长的区域区块链的创建时间 T 之后,全网区块链数据的冗余存储量将会大大降低,未划分区块链网络情况的冗余数据存储量是划分区块链网络之后的 $\frac{i \times (n-1)}{n-i}$ 倍,可见,在全网交易具有足够局部性特征的前提下,划分子区域网络个数 i 越多越好。

6 安全性分析

区块链全网共享交易账本数据,通过全网共识获得全网认可,这是交易安全、交易数据不可篡改的根本保证。当前的区块链网络很多基于“算力”共识,在算力共识的协议中,依靠全网的算力共识保护区块历史数据不被恶意节点篡改。本方法将全网划分为若干子网之后,全网算力也进行了划分,在形成子网共识记账的过程中,在网络之外引入恶意节点对子网区块链数据进行算力攻击的成本将会降低。因此,划分子网时,除了考虑交易局部性之外,还需考虑使每个区域子网的算力足够安全、每个区域子网是完全“去中心化”的、每个区域子网具有足够多的独立节点保存区域子账本数据。也就是说,将全局去中心化的区块链网络划分为若干“区域去中心化”的区块链子网,每个区域都应该是足够可信的。

这个安全问题并不是本方法新引入的,算力攻击导致的安全问题存在于原始的区块链协议中,只是在应用本方法时,需要慎重评估算力攻击风险。

7 结 论

现实中存在的交易网络具有明显的局部性特征,据此,本文提出了将全局区块链网络划分成若干区域区块链子网的方法,区块链网络的参与节点不再需要存储全网的区块链全账本数据,只需要存储本区域子网内的区块链账本数据即可,从根本上拆分全局区块链账本数据为多区域区块链账本数据;同时,将全网广播、收录交易单的网络 I/O 负载划分到每个区域区块链子网内。此方法解决了区块链的

存储瓶颈和网络 I/O 瓶颈造成的扩展性受限问题。该方法的核心价值在于解决网络划分前后的“双花”问题;解决跨区域节点移动和跨区域节点交易的问题,同样不会造成“双花”现象。该方法没有改变区块链的协议本质,没有引入额外的安全问题。目前,该方法暂时不能支持需要全局共识的“造币”交易类的应用。

参考文献

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin. org/bitcoin. pdf: bitcoin, 2008

[2] Swan M. Blockchain thinking: the brain as a DAC (decentralized autonomous organization[C]. In:Proceedings of the Texas Bitcoin Conference, Texas, USA, 2015. 27-29

[3] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494

[4] Lamport L, Shostak R, Pease M. The Byzantine generals problem[EB/OL]. http://www. microsoft. com/en-us/research/wp-content/uploads/2016/12/The-Byzantine-Generals-Problem. pdf: microsoft,1982

[5] Fan J, Yi L T, Shu J W. Research on the technologies of Byzan-tine system[J]. *Journal of Software*, 2013, 24(6):1346-1360

[6] Nelson M. The Byzantine general's problem:an agreement protocol for distributed system[EB/OL]. http://www. drdobbs. com/cpp/the-byzantine-generals-problem/206904396: drdobbs, 2008

[7] Lamport L. The weak byzantine generals problem[J]. *Journal of the ACM*, 1983, 30(3): 668-676

[8] Fedotova N, Veltri L. Byzantine generals problem in the light of P2P computing[C]. In: Proceedings of the 3rd International Conference on Mobile & Ubiquitous Systems: Networking & Services, San Jose, USA, 2006. 1-5

[9] Reischuk R. A new solution for the byzantine generals problem[J]. *Decision Support Systems*, 1985, 1(2):182

[10] Bamert T, Decker C, Elsen L, et al. Have a snack, pay with Bitcoins[C]. In: Proceedings of the 13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy, 2013. 1-5

[11] Decker C, Wattenhofer R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]. In: Proceedings of the 17th International Symposium on Stabilization, Safety, and Security of Distributed Systems, Edmonton, Canada, 2015. 3-18

[12] Lewenberg Y, Sompolinsky Y, Zohar A. Inclusive Block Chain Protocols[M]. In: Financial Cryptography, Puerto Rico: Springer Berlin Heidelberg, 2015. 528-547

[13] Sompolinsky Y, Zohar A. Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, not Chains [M]. In: Financial Cryptography, Puerto Rico: Springer Berlin Heidelberg, 2015

[14] Blockchian. info. Number of Transactions [EB/OL]. http://blockchain. info/charts/n-transactions: blockchain, 2017

[15] Maxwell G. Reducing UTXO: users send parent transactions with their merkle branches[EB/OL]. http://bitcointalk. org/index. php? topic = 314467 # msg3371194: bitcointalk, 2013

[16] Miller A, Litton J, Pachulski A, et al. Discovering Bitcoin's public topology and influential nodes[C]. In: Proceedings of the ACM Symposium on Applied Computing, 2013. 121-128

[17] Christian D, Wattenhofer R. A fast and scalable payment network with Bitcoin duplex micropayment channels[J]. *Stabilization, Safety, and Security of Distributed Systems.* 2015, 9212: 3-18,

[18] Miller A, LaViola J. Anonymous byzantine consensus from moderately hard puzzles: a model for bitcoin[R]. University of Central Florida. CS-TR-14-01, 2014

[19] Back A, Corallo M, Dashjr L, et al. Enabling blockchain innovations with pegged sidechains[R]. http://www. blockstream. com/sidechains. pdf: blockstream, 2014

[20] Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications[M]. Advances in Cryptology-EUROCRYPT 2015, Springer Berlin Heidelberg, 2015. 281-310

[21] He H J, Zhang J S, Tai H M. Block – chain based fragile watermarking scheme with superior localization[J]. *Lecture Notes in Computer Science*, 2008, 5284:147-160

[22] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, et al. Bitcoin-NG: a scalable blockchain protocol[C]. In: Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, USA,

2016. 45-59

[23] Min X P, Li Q ZH, Liu L, et al. A permissioned blockchain framework for supporting instant transaction and dynamic block size[C]. In: Proceedings of the Trustcom/Bigdatase/Ispa, Tianjin, China, 2016. 90-96

[24] Dennis R, Owenson G, Aziz B. A temporal blockchain: a formal analysis. In: Proceedings of the International Conference on Collaboration Technologies and Systems, Orlando, USA, 2017. 430-437

Research on splitting technology of blockchain data

Yu Lei[*,**], Jin Yan[**]

([*] University of Chinese Academy of Sciences, Beijing 100049)

([**] Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

Abstract

The technical characteristics of applying blockchains to transaction networks are analyzed, and facing the present block chain architecture, the bottleneck in scale expansion of blockchain systems due to the flooding of all network broadcast of transaction data and new blockchain data as well as the full copy storage of global blockchain data in all consensus nodes is pointed out. In consideration of the local feature of blockchain networks, a scheme dividing the consensus of whole blockchain network into multiple sub-networks' consensus is proposed, and the "double" problem before and after network partition and the cross zone movement and cross-border payment problem of nodes are solved, so the even dividing of the network I/O load and the blockchain data storage load cross the whole network is achieved. This scheme is optimized and improved based on the native protocol of blockchain, no other security threats are introduced. Finally, the storage load change is analyzed by the mathematical method, and the results show that the proposed scheme has significant advantage in resource consumption of blockchain networks.

Key words: blockchain, data partition, splitting technology, double-spending problem, cross-area transactions, scalability