基于有向无环图的新型联盟链架构设计

葛瑞泉 肖泽芸
（杭州电子科技大学，浙江 杭州 310016）

摘要：作为一种可靠的、安全的新型数据储存方式，区块链技术已经被广泛应用在我们日常生活中。本文主要基于有向无环图的技术以及各类共识和加密算法，实现新型的联盟链底层架构，旨在提升现有联盟链的出快速度以及上链灵活度。本文主要将自建的联盟链与目前主流的联盟链开源框架进行性能对比，以测试框架的整体性能及其可靠性。

关键词：有向无环图；区块链；联盟链
DOI：10.12373/xdhjy.2021.10.3762

国务院出台的“十三五规划”提出要强化区块链、人工智能等战略前沿技术，并在其他国家之前进行提前布局。同时，工信部也发布白皮书指出区块链的核心技术发展进程，部委也在与相关企业进行合作，希望尽快制定技术标准。

一、区块链研究现状及存在问题

（一）区块链研究现状

区块链按照部署范围可以分为公链、联盟链和私有链。公有链秉持着“去中心化”理念，主要用于世界范围内的数字货币交易，其中最具代表性的是被称为“区块链最成功应用典范”的比特币，以及“引领区块链 2.0 时代”的以太坊，但是公链技术因为无法得到各国政府的有效管制，经常被不法分子用作“洗钱”的手段，因此包括中国在内的很多国家和地区都将比特币等公链数字货币作为非法货币。

目前普遍推广的是第二种区块链架构，即联盟链。联盟链是部分去中心化的区块链架构，它和公链一样，利用共识算法和加密算法保证数据的安全性和可靠性，但是参与联盟的组织可以共同维护链上的数据，这有利于监管和统计，因此受到了政府和企业的青睐。联盟链最知名架构是 apache 基金会下的 Hyperledger Fabric，很多企业都参照这些开源项目实现了公链或者联盟链平台和数据存储架构。

（二）区块链框架普遍存在的问题

区块链目前主要应用于金融领域，随着国家政策转向等因素影响，区块链的应用场景也在不断拓宽。虽然区块链技术能够提高数据存储安全性，但是由于其本身存在性能等问题，导致其在数据实时性要求高、数据存储成本大的领域未能得到广泛应用，目前也没有太多将区块链应用与打破各类数据壁垒的联盟链实践，区块链技术在生活场景中的应用比较有限。

二、传统区块链框架研究

（一）区块链框架基本需求

1. 性能需求

根据目前已确定的基本区块链架构，其交易处理速度理应比大部分的现有区块链结构要快，因此架构最终需要测试的参照对象主要有比特币，以太坊和 Fabric。性能比较主要考虑系统的吞吐量、共识消耗、交易处理速度等方面。

2. 安全性需求

双花问题作为区块链研究的基本问题之一，也是框架加密和共识算法选择所需考虑的问题，需要保证同一交易的唯一性，同时也应当配置出现双花问题的多余项处理方式。

3. 功能性需求

现有的联盟链架构虽然能够实现跨链访问，但其资源开销都比较大。但是对于 DAG 联盟链而言，有着更强的可延展性，不同的组织隶属于不同的联盟分片，不同的联盟分片从属同一个联盟，从数据的储存方式上提供了跨链的可能。

（二）传统区块链框架分析

1. 区块结构模型

以代表性区块链比特币为例，其主要包括版本、前区块哈希值、区块交易生成默克尔树哈希值、区块产生时间、难度和随机数。版本用于记录当前的版本信息，前区块哈希用于记录上一个区块的哈希值以防止篡改区块，生成默克尔树哈希主要用去确保交易的正确性，产生时间记录区块的产生时间。难度主要表示计算区块哈希的难易程度，而随机数则作为区块链挖矿的解题结果。

以太坊区块可以拆分为区块头和主体两部分。和比特币结构类似，以太坊的区块头包含指向父区块的指针、矿工的地址、叔块哈希、根节点哈希、交易哈希、过滤器、区块难度、区块序号、创建时间、消耗 gas 的上限、实际 gas 消耗、nounce 值等。

超级账本（Hyperledger Fabric）作为联盟链的开源项目代表，fabric 的区块结构相对于前两者更加复杂，前两者主要用于数字货币交易，而联盟链可用于各类数据的存储过程。Fabric 的整体数据结构包含三部分：区块头、区块数据和区块元数据。

2. 区块哈希链接模型

传统单链架构中任何区块仅有一条通向创世区块的路径，但是从创世块出发可能存在分支路径，这时需要使用最长链保留原

则进行链的选择，在比特币系统中，当长链被保留时，分叉生成的单链就被孤立，其中包含的所有的收益都消失。

联盟链中的处理方式与上述公链方式略有不同。以Hyperledger Fabric为例，其开发者引入了联盟、组织等概念，所谓联盟和组织，指的就是参与区块链网络的集体以及集体中的每个企业或者部门。公链的记账节点主要是矿工，它们通过付出算力解决问题，实现交易打包。因为这是一种有利可图的经济活动，因此矿工们为了获得更多的挖矿奖励，不断提升自己的算力水平，也引发了比较激烈的算力竞赛，这也是传统公链POW（Proof of Work）机制非常容易导致的问题。联盟链通常是范围性、有组织性发起的区块链平台，其中往往会储存较为敏感的信息，这些信息不宜存放公链作为公开信息，同时联盟链往往是为了实现数据共享等活动发起，参与组织一般也不愿意在上链过程投入较高资金，这也就意味着联盟链是不存在真正意义上的矿工的，其各类的记账信息都由组织指定的peer节点进行，然后交由order节点进行具体存档工作，这也是联盟链与公链架构的最大区别之一。

三、联盟链设计过程及应用场景分析

（一）区块设计

本区块结构预期与fabric相似，采用区块头、区块主体和区块数据体三部分。区块头由等区块类标，宽度，前块哈希，数据哈希，时间，链接，高度等部分组成。区块主体主要包含数据规范和数据内容。数据规范默认仅对业务块生效，用于创建业务规范并作用于业务块创建的所有数据块单链。

（二）链接设计

本区块链系统主要包含：联盟块、组织块、业务块、数据块四种类型。同一个联盟通常只拥有一个联盟块，作为整个联盟链系统的创世区块，联盟中各类组织创世区块均直接与该联盟块相连，并且储存联盟块的哈希值作为可信标记。组织块通常的延伸选项为组织块和业务块，用于细分组织部门和业务逻辑，子区块同样需要储存其父区块的哈希值。业务块后继区块一般为业务块和数据块，实现细分业务需求和创建数据储存空间。

基于DAG的联盟链架构与普通联盟链略有不同，每一个区块可以与多个子区块直接相连，这也可能导致区块链DAG图无限横向扩展，不但会大幅提高链数据的不稳定性，同时也加大了校验、查询难度。因此在创建父区块的同时对子链的宽度进行限制，合适的链宽不仅能保证较高的上链效率，同时也可提高检索和验证速度。因为区块链通过哈希相连，因此对于数据的篡改难度是较大，这也导致了数据正常修改的难度较大，因此本架构也希望能够以这种方式让链组织对区块进行合法修改。当组织用户试图修改某一个系统单链数据块时，修改后的数据块并不直接替换相应区块，而是在储存父区块的同时也存储其预期修改的区块哈希，同时与预期修改区块共用同一个区块高度，这样既实现了区块修改，也实现了原始数据的存根。

（三）共识算法设计

区块链最常用的共识算法主要有Pow、Pos、Pbft等。Pow主要通过挖矿工作量达成出块共识。因为其仅仅根据工作量给予奖励，因此相对公平。但其工作量分发奖励会导致其容易引起算力竞赛，造成大量资源浪费。Pos没有挖矿过程，用户所获收益与其股权大小有关。但是其信用无法得到保障，因此很多发行币都用pow和pos结合的方式共识。联盟链常用共识算法有严格可靠的数学证明，具有（n–1）/3的容错性，因此当链上1/3记账节点宕机时会失去共识能力。

基于DAG的联盟链架构旨在提高联盟内数据的透明度，因此其主要储存的数据不一定与资金等信息相关，这意味着传统共识机制无法形成有效的联盟间节点共识。对于非资金类数据，其共识是困难的，也是非必要的，因此，对于强业务类型数据，系统通常采用非共识验证。此时，联盟链主要作用于“锁定”数据，为后续可能出现的问题做存证。而对于资金类数据，主要采用pbft算法共识。

（四）应用场景分析

目前国内外的联盟链架构主要用于企业间的合作管理、物联网产线的数据管理、生产链的流程控制等方面，本文设计的联盟链架构满足上述场景的业务需求。其次，本文希望搭建出一条适用于集团内部业务数据互通的数据链框架。对传统的联盟链而言，其记录的内容还是以各类数据为主，而在DAG的联盟链架构中，因为链既可以纵向拓展，也可以横向拓展，这意味着不同的链可以用于存储不同的组织数据，不再像传统联盟链一样单链数据杂乱或是为了储存多种数据创建或加入多个组织。

同时，这种基于DAG的联盟链架构也为业务标准化、规范化执行和存储提供了新的有效方式，区块头可以存储单链的数据规范，以此构建一条标准化单链，多个区块头隶属同一组织，用于存储该组织的各类标准化业务流程，这样也能够让参与联盟的组织业务流程更加清晰，也可以让其他组织快速借鉴优秀组织的业务处理方式。

四、结语

本文旨在提出联盟链相关的新解决方案，主要用于解决联盟内数据不透明、交互困难、对外公开难等问题，并且增强传统联盟链的可拓展性，使其能够适应不同的业务需求，融入更多的行业领域。目前本文所提出的联盟链架构已经进入开发阶段，未来将会投入更多的精力用于框架的具体实现，并且对其性能进行相关实验测试，以使此框架尽早运用于实际业务场景中。

参考文献：

[1] 潘吉飞，黄德才 . 基于跳跃Hash和异步共识组的区块链动态分片模型 [J]. 计算机科学，2020，47（03）：281–288.