

区块链关键技术中的数据一致性研究

翟社平,李兆兆,段宏宇,高山

(西安邮电大学 计算机学院,陕西 西安 710121)

摘要:区块链技术是一种新型去中心化协议,能安全地存储交易数据,信息可追溯、不可伪造和篡改,无需任何中心化机构的审核。随着以比特币为代表的数字资产的发展,区块链技术迅速成为国内外研究热点。针对传统分布式网络由于去中心化带来的节点信任缺失、恶意节点存在、各方利益差异化导致的数据不一致等问题,对区块链关键技术进行了深入分析与探讨。详细阐述了分布式网络中数据一致性维护的研究内容和目标,综合运用分布式数据存储技术、对等网络可靠传输技术、分布式共识机制技术、非对称加密技术搭建了一个决策权高度分散的去中心化网络。在此基础上提出一种基于区块链技术的数据一致性维护三层体系架构,有效维护区块链网络数据一致,最后对区块链的发展前景进行展望。

关键词:分布式网络;区块链;共识机制;非对称加密;数据一致性

中图分类号:TP391

文献标识码:A

文章编号:1673-629X(2018)09-0094-07

doi:10.3969/j.issn.1673-629X.2018.09.020

Research on Data Consistency of Key Technologies of Blockchain

ZHAI She-ping, LI Zhao-zhao, DUAN Hong-yu, GAO Shan

(School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: Blockchain is a new kind of centralized protocol, which can store transaction data safely. The information can be traced back, cannot be forged or tampered with, and it does not need the approval of any centralized institution. With the development of digital assets represented by Bitcoin, Blockchain technology has become the focus of research at home and abroad. In view of the data inconsistency of the traditional distributed network due to the lack of node trust, the existence of malicious nodes and the difference of interests caused by decentralization, the key technologies of Blockchain are analyzed and discussed deeply. The research contents and goals of data consistency maintenance in distributed network are discussed in detail. Based on the distributed data storage technology, the distributed consensus mechanism, peer-to-peer network data transmission protocol and cryptography principle, we construct a decentralized network with high decision-making power. On the basis, we present a three-layer architecture of data consistency maintenance based on Blockchain technology, which communicates well between each layer, and finally maintains the consistent data of Blockchain network effectively. Finally we prospect the development direction of Blockchain.

Key words: distributed networks; Blockchain; consensus mechanism; asymmetric encryption; data consistency

0 引言

区块链技术是一种新型计算模式,是经单主机计算、分布式计算和网络计算三种计算模式之后的新型创新应用模式^[1]。它将分布式数据存储、点对点传输、共识机制和加密算法等计算技术与互联网技术相结合,构建了一个高容错高可用的分布式网络,其去中心化、可追溯、不可篡改、安全可信等技术特点有效地保障了区块链的实用性以及区块链中数据的一致性,对

区块链的推广有着决定性的作用。区块链最初是为了实现去中心化交易提出的技术,发展至今,区块链已经不单局限于数字货币应用,其与人工智能、云计算、大数据等技术的结合应用已经在物联网、健康医疗、知识产权保护等领域展现出了独特的应用价值和市场前景。

国外针对区块链技术的研究开展较早,目前已经有一些成熟的系统应用。美国以太坊平台 Ethereum

收稿日期:2017-09-12

修回日期:2018-01-04

网络出版时间:2018-04-28

基金项目:工业和信息化部通信软科学项目(2017-R-22);陕西省社会科学基金资助项目(2016N008);陕西省自然科学基金资助项目(2012JM8044);陕西省教育科学研究计划资助项目(12JK0733);西安市社会科学规划基金(17X63);西安邮电大学研究生创新基金(CXL2016-24)

作者简介:翟社平(1971-),男,副教授,博士,CCF会员(77328M),研究方向为区块链、语义 Web、智能 Agent 及云计算;李兆兆(1994-),女,硕士研究生,研究方向为区块链、语义 Web。

网络出版地址:<http://kns.cnki.net/kcms/detail/61.1450.TP.20180427.1640.046.html>

基于区块链为用户提供可编程智能合约开发服务,微软公司在 Azure 云计算平台的基础上推出了 BaaS (Blockchain as a service,区块链即服务)服务等。虽然国内区块链起步比国外晚 2~3 年,但热度爆发的速度更快。2016 年《“十三五”国家信息化规划》首次提到支持区块链技术发展,强调加强人工智能、区块链、大数据认知分析等新技术基础研发和前沿布局。2016 年 10 月工业和信息化部发布《中国区块链技术和应用发展白皮书》。2017 年 5 月,国内首个区块链标准《区块链参考架构》正式发布^[2],区块链基础性标准确立。同时,在数字版权保护领域,蔡维德教授等针对公信力和隐私性要求较高的场景提出一种双链设计架构^[3]。朱岩等针对区块链中数据安全问题提出了使用基于属性的密码访问控制技术的设想^[4]。目前,区块链技术已经引起了很多专家学者的重视,随着大数据的发展,在政府大力扶持、高校院所助力、企业应用落地的形势下,区块链底层技术及其在场景中的应用将深刻颠覆人们的传统生活方式,成为研究的热点问题。

本质来看区块链是一种分布式数据库,与传统数据库操作不同,区块链利用一种新型块链式数据结构验证和存储数据,数据的生成和更新采用一种工作量证明的分布式共识算法,区块链中数据传输和访问的安全性则利用密码学原理来保障,同时区块链以智能合约的形式提供数据的编程操作^[5]。从数据去中心化的角度来看,区块链上的数据不存储在某一个特定的服务器或安全节点上,而是分布地存储于网络中所有的完整节点上,同时网络中每一个节点都保证数据信息的完整性和一致性^[6]。然而从技术角度分析,当区块链中每个数据对象存在多个副本时,必然会导致众多问题的出现,如数据副本负载不平衡、数据冲突、数

据篡改和破坏等问题^[7]。区块链采用去中心化的思想,使用对等网络中所有节点集体运作的方式,构建了一个没有中央控制节点的自组织网络,作为一个分布式、多中心的存储架构,数据一致性问题尤为重要。

针对上述问题,文中提出一种基于区块链关键技术的数据一致性维护体系架构。在数据一致性维护方面,从存储层、网络层、共识层和数字加密四个关键技术层面进行研究,阐述了如何通过分布式数据存储技术、数据传输协议技术、共识机制技术、非对称加密技术来维护数据的一致性。

1 分布式数据存储技术

由于数据一致性问题涉及到区块的结构以及区块不可篡改的重要特性,区块链中的数据可以从两方面描述,一方面是“区块+链”,另一方面是“交易+链”。区块链可描述为一个由多个节点组成的分布式数据存储系统,它将一段时间内的交易以 Merkle 树形式组织,将数据和代码封装形成区块,按照时间顺序组织区块,同时利用密码学原理保证数据不可篡改和伪造^[8]。

区块是包含了区块链全网中数据信息的一种数据结构,由包含元数据的数据头和包含所有交易数据构成的区块体组成。区块头由前一区块哈希、随机数、时间戳、难度目标以及 Merkle 根等关键字段构成。每个区块都有指向前一个区块的链接,一直到最初创建的区块,在区块链系统中发生的每一笔交易都会存在于某一个区块中并永久保存,如图 1 所示。例如,“区块 25”中包含前一区块哈希值链接到“区块 24”,“区块 24”中则包含“区块 23”的哈希值链接至“区块 23”,以此类推,可追溯至最初的一个数据区块即创世区块。

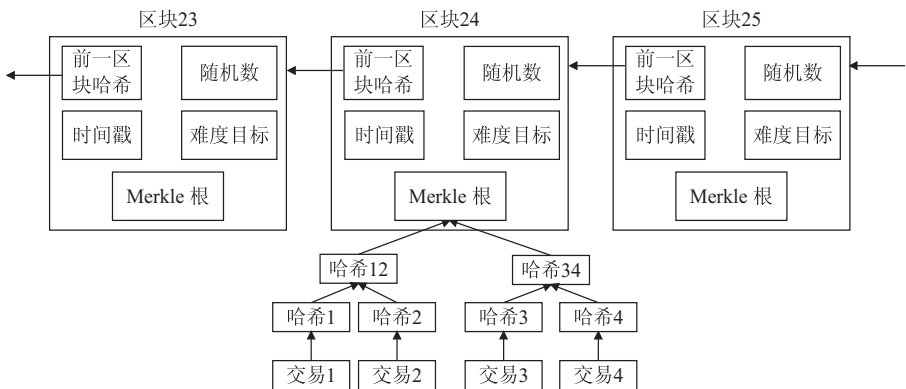


图 1 区块链式结构

其中“前一区块哈希值”字段是对其前一区块头的所有数据进行 SHA256 运算得到的结果,该字段使得各个区块之间可以连接起来,是保证区块连接成为区块链的关键字段。随机数、时间戳、难度目标字段与新区块的生成数据,分布在区块链网络中的各个节点

贡献大量的算力资源竞争解决一个密码学安全的 SHA256 数学难题以生成新区块。随机数记录解密该区块相关数学难题的答案的值,时间戳是区块产生的精确时间,难度目标可动态调整以改变新区块形成的难易程度。Merkle 根是快速归纳和校验区块大规模

数据完整性和一致性的重要数据字段, Merkle 树自底向上构建, 首先将区块中的所有数据进行哈希运算得到哈希序列, 将哈希序列存储至相应的叶子节点, 对相邻叶子节点的哈希值进行哈希运算, 如此递归操作直至只剩顶部的一个节点, 即 Merkle 根计入区块头中。区块体主要记录所有交易的具体信息, 包括交易的输入和输出、交易值等具体的数据信息。

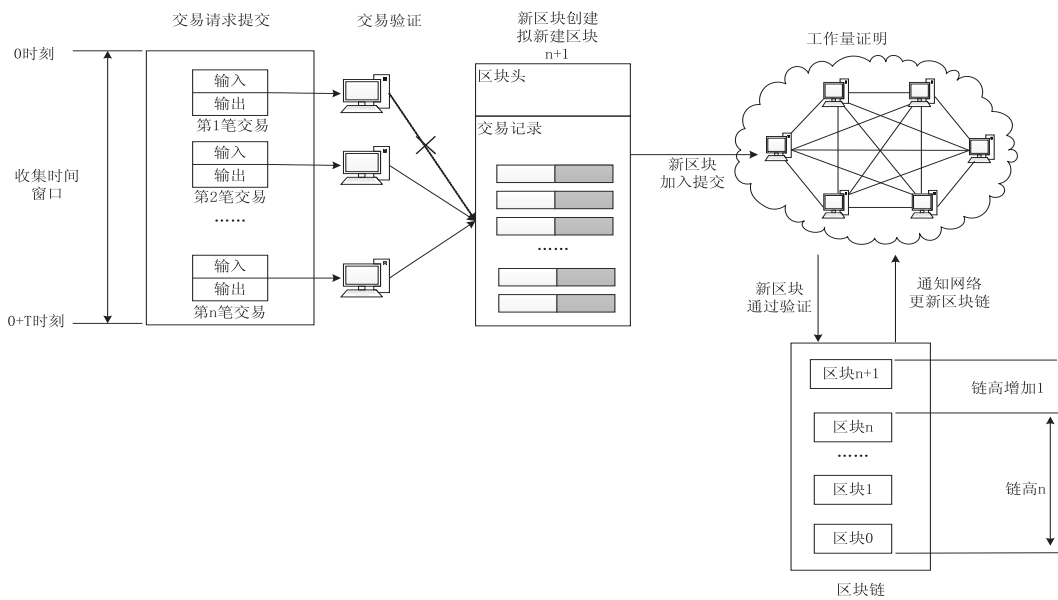
交易数据是区块链中最重要的组成部分。区块链综合应用多重技术都是为了确保新交易数据的快速生成、安全传播和有效验证, 并且最终添加至整个分布式总账即区块链中, 全网每个节点都拥有总账的副本以确保交易数据一致可靠不可篡改。同区块成链一致, 区块链中所有交易也构成了一组链式结构来保证数据的一致性。在区块链交易系统中, 交易的基本单位被定义成 UTXO (unspent transaction output, 未花费交易输出), 指记录于区块链系统中的无法再细分、被所有者“锁住”并被整个网络识别成货币单位的一定量的货币。每一个交易又可以分为交易输入 (input) 和交易输出 (output) 两个字段。交易输入由指向被花费的 UTXO 所在的交易的交易哈希值、表示被花费的 UTXO 的索引号的输出索引、满足 UTXO 解锁条件的解锁脚本等字段构成, 交易输出则主要包含一个定义了支付输出所需要条件的锁定脚本。

按照交易的输入和输出的个数可以将交易可以分为三种类型, 拥有一个输入和一个输出的一般交易、拥有一个输入和多个输出的用来分配资金的分散型交易与拥有多个输入和一个输出的用于清理支付过程中收到的小数额找零的集合型交易。每一笔交易的输出都链接到下一笔交易的输入, 因此全网所有合法交易都可以通过这种方式追溯到之前的一笔或者多笔交易的

输出, 交易链的源头是生成新区块的系统奖励 (又称 Coinbase 交易), 交易链的末尾则是许多 UTXO。交易输入和交易输出同时包含两个用来验证交易合法性的脚本。输出脚本位于交易输出, 明确了下一笔交易取得当前 UTXO 使用权的条件, 又称锁定脚本。输入脚本位于交易输入, 是满足被锁定脚本在其交易输出上所设定的花费 UTXO 的花费条件, 又称解锁脚本, 通常含有一个由用户私钥生成的数字签名, 允许交易输出被消费。在交易验证阶段, 需要将两个脚本组合在一起, 以堆栈执行引擎形式进行验证, 只有组合脚本验证通过, 包含在交易中的 UTXO 才可以被使用, 才可以证明交易有效, 从而保证了全网中所有数据一致可信。

2 对等网络可靠性传输技术

区块链系统自诞生至今一直保持着高稳定性, 这与其采用基于国际互联网的 P2P (peer to peer, 对等网络) 架构密不可分。P2P 指位于同一网络中的每台计算机都彼此对等, 各个节点共同提供网络服务, 不存在任何服务端、中央化的服务与层级结构^[9]。相较于传统 C/S (client/server, 客户/服务器) 模式的信息系统, 采用 P2P 网络结构的系统具有去中心、高容错、隐私保护和负载均衡等特点。系统中各个节点地位平等, 每个节点都可以独立完成系统服务功能, 因此网络中部分节点或者网络遭到恶意攻击时并不影响系统性能。区块链系统的每个节点承担了网络路由、验证区块数据、传播区块数据、发现新节点等功能且具有动态变更的特性, 任一区块数据生成后, 将由生成该数据的节点广播到全网其他所有节点来加以验证。区块链系统的交易数据传播协议包括以下步骤, 如图 2 所示。



万方数据

图 2 区块数据传输

(1)新的交易通过对等网络传输协议广播给 P2P 网络上的所有节点。

(2)每个节点首先对交易数据进行有效性验证,即利用非对称加密机制验证交易的签名和交易数据信息,如果验证无效则丢弃该笔交易数据。如果验证通过,节点将交易数据以 Merkle 树的形式进行组织,并且记录区块头的有效字段,盖上时间戳,填入区块头其他字段,封装产生区块。现有区块链网络规定新区块生成的时间是 10 分钟。

(3)为了竞争记账权,每个节点竞争自身算力解决 SHA256 难题以提交工作量证明。

(4)如果一个矿工节点解开了这 10 分钟的 SHA256 难题,就找到了工作量证明,获得该区块的记账权,该节点将数据打包封装成新区块,通过对等网络传输协议向全网各个节点广播该新区块。网络中其他节点接受到新区块将首先验证工作量证明是否有效,即每个节点计算区块头的双重哈希值,并与已知的难度目标作比较。

(5)所有参与记录的节点通过 Merkle 根共同验证交易记录数据的正确性,验证通过则节点接收这个区块,该区块被链接到区块链的尾部。一般来说,每一笔交易,必须经过 6 次区块确认,即 6 个 10 分钟记账,才能最终在区块链上被承认是合法交易。6 次确认使得恶意节点攻击需要耗费巨大算力,增加了区块数据攻击的难度,使得全网可以保证抵御 51% 攻击,同时也降低了双花问题出现的概率,有效维护了区块数据一致性。

(6)所有节点转向创造下一个区块,并将刚刚接受的区块的哈希散列作为父区块的哈希值记录在下一个区块的区块头中。

针对 P2P 网络中单个或者部分节点故障问题,区块链采用数据同步的思想来解决^[10]。区块链设置一套通信消息原语来进行数据同步。首先,网络中对等节点(节点 A 和节点 B)交换包含 BestHeight(区块链高度)字段的 version 消息,比较自身区块链所拥有的区块数量。然后,对等节点再交换一个包含本地区区块链的顶端区块哈希值的 getblocks 消息。节点通过比较顶端区块哈希值来判断本地区区块链与其他对等节点的区块链长度差异,拥有较长区块的节点(如节点 B)可识别出需要进行区块补充操作的其他节点,之后使用 inv 消息把这些区块的哈希值传播出去。区块信息不完整的节点(节点 A)发送 getdata 消息向节点 B 请求得到完整区块链的区块数据信息,之后发送 inv 消息,此 inv 消息包含了区块的哈希值,节点 A 判断所返回的哈希值来确认信息是否为被请求区块,从而选择性读取缺失区块,实现节点间区块数据的同步。这种

对等网络的数据传输机制,保证了在节点动态加入、退出的情况下,维护整个网络的稳定性,进而保证了区块链中数据的完整性和一致性。

3 共识机制

任何分布式系统都会面临网络延迟、传输错误、软件错误、安全漏洞以及黑客入侵等问题^[11]。为了防范这些潜在的错误,区块链系统需要一个高效的共识机制来确保每一个节点都有一个唯一公认的全局账本。随着人们对这种分布式账本一致性问题的不断探索,很多适合区块链的共识算法被提出。

早期的区块链采用 PoW (proof of work,工作量证明)机制来解决存储时的分布式一致性问题,核心思想是各节点基于算力竞争来共同解决一个 SHA256 数学难题,最快解决该难题的节点将获得区块记账权和系统奖励,从而引入分布式节点的算力竞争来保证数据一致性和共识的安全性^[12]。PoS (proof of stake,权益证明)机制是为解决 PoW 共识的资源浪费和安全性缺陷而提出的替代方案,它采用权益证明来代替 PoW 中的基于哈希算力的工作量证明,由系统中具有最高权益而非最高算力的节点获得区块记账权^[13]。PoS 机制仅依靠内部币龄和权益而不需要消耗外部算力和资源,从根本上解决了 PoW 共识算力浪费的问题,但同时丢弃了 PoW 的一些优势,因此更容易分叉,一笔交易需要等待更多确认才能确保安全,链中数据有极大可能被篡改,存在一定的安全隐患。DPoS (delegated proof of stake,股份授权证明)机制实质上是一种“受约束的中心化”决策机制,它引入了“受托人”的角色以降低中心化带来的负面影响。在 DPoS 中新区块的生成过程是通过 101 位经由网络上所有分散节点投票产生的受托人来完成的,受托人负责新区块的生产和广播以此获取新区块生成的 Coinbase 奖励^[14],但也需要提前缴纳一定量的保证金,同时也需要付出强大的算力资源。DPoS 通过这种方式使得全网算力集中在 101 位受托人中,大幅缩小了负责生成新区块的节点数量,可以承载更多的交易量,同时可以达到秒级的共识验证。

上述三个共识机制虽然可以维护区块数据一致性,但均存在不同程度的算力资源浪费和安全隐患问题。PBFT (practical Byzantine fault tolerance,实用拜占庭容错)算法提出在异步网络环境下使用状态机副本复制协议来解决上述问题。PBFT 是一种基于消息传递的已执行算法,它的执行过程包括 5 个步骤,如图 3 所示。

(1)从全网节点选举出一个主节点 (leader),新区块由主节点负责生成。

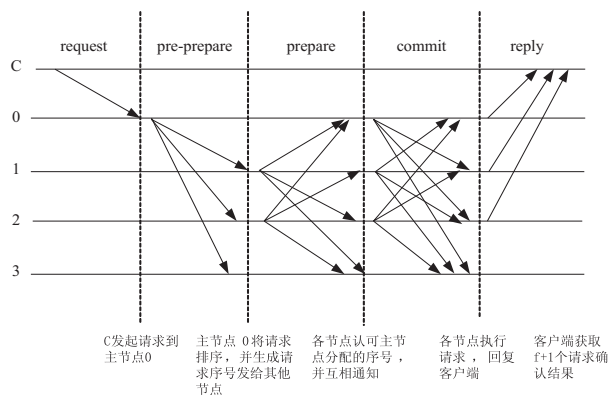


图 3 PBFT 算法执行流程

- (2) 每个节点把客户端发来的交易向全网广播, 主节点将从网络收集到需放在新区块内的多个交易排序后存入列表, 并将该列表向全网广播。
- (3) 每个节点接收到交易列表后, 根据排序模拟执行这些交易。所有交易执行完后, 基于交易结果计算新区块的哈希摘要, 并向全网广播。
- (4) 如果一个节点收到的 $2f$ (f 为可容忍的拜占庭节点数) 个其他节点发来的摘要都和自己相等, 就向全网广播一条 commit 消息。
- (5) 如果一个节点收到 $2f+1$ 条 commit 消息, 即

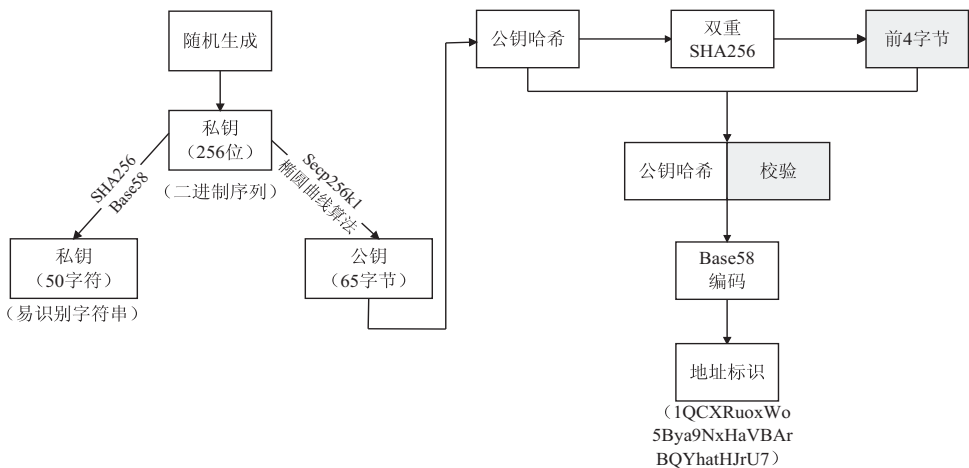


图 4 区块链非对称加密机制

系统首先使用随机数生成器生成一个 256 位二进制随机数作为私钥, 该私钥不直接提供给用户, 对其进行 SHA256 哈希运算生成 256 位哈希序列, 之后经由区块链自定义方案即 Base58Check 编码方案将哈希值和校验和数据转换为一种“字母-数字”表示, 形成 50 字符长度的易识别字符串提供给用户。二进制公钥经过 Secp256k1 椭圆曲线加密算法生成 65 字节的非压缩公钥, 该非压缩公钥被定义成一个点: $K = (x, y)$, 其生成过程是 $K = k * G$, 其中, k 是二进制私钥, G 是椭圆曲线中被称生成点的一个常数点, 定义为 $G = 0279BE667EF9DCBBAC55A06295CE870B07029BFCD B2DCE28D959F2835B16F81798$, 其中 K 代表所得公

可提交新区块及其交易到本地的区块链和状态数据库。图 3 展示了客户端发起请求, 经过预准备、准备、确认和回复四个阶段, 最终达成有效共识的执行流程, 其中 C 是客户端, 副本 0 至副本 3 都是网络节点, 0 是主节点, 3 是网络中的失效节点。

区块链系统中的 PBFT 共识算法使得交易确认速度显著提高, 交易吞吐量也可以满足现有的数据交易规模, 可以解决数据丢失、损坏、延迟的问题, 同时对于任何网络环境都具有较好的容错能力, 更为高效地保障了系统数据一致性。

4 非对称加密机制

非对称加密技术是保证区块链安全的关键, 最初是由美国学者 Dime 和 Henman 为解决信息公开传送和密钥管理问题所提出的一种密钥交换协议, 指使用公钥和私钥对数据存储和传输进行加密和解密^[15]。常见的非对称加密算法包括 RSA、Elgamal、背包算法、Rabin、D-H、ECC (elliptic curve cryptography, 椭圆曲线加密算法) 等。区块链使用非对称加密的公私钥对来构建节点间信任, 为数据一致性提供重要保障^[16]。

非对称加密机制在区块链中的应用如图 4 所示。

钥, $*$ 是椭圆曲线乘运算。该公钥用来生成区块链系统的交易账户地址标识, 对其进行两次 SHA256 哈希运算, 取运算结果的前 4 字节作为公钥哈希的校验值链接在其尾部, 最后经由 Base58 编码转化, 最终形成 33 字符的地址标识。

区块链中的数据加密和数字签名也是非对称加密机制的应用体现。信息发送者 A 采用信息接收者 B 的公钥对待发送的信息加密, 将加密信息发送给 B, B 使用自己的私钥对接收到的信息解密以获得原始信息, 这一过程称为数据加密。数字签名则是信息发送者 A 使用其自身私钥将信息加密之后发送给 B, B 收到信息之后采用 A 对应的公钥解密信息, 以确认信息

来源于 A^[17]。

区块链的交易应用了上述加密机制,如图 5 所示。

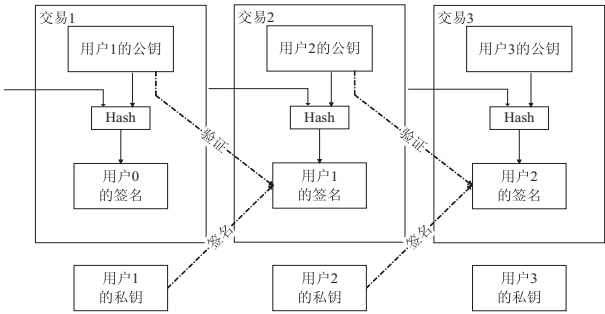


图 5 交易的签名和验证

在交易认证过程中,交易 2 的签名过程主要由付款方(用户 1)来完成,本次交易的发送方(用户 1)首先对上一笔交易(交易 1)的交易数据信息进行哈希运算得到一串哈希序列,用户 1 使用自己的私钥对所得序列加密,加密后的摘要将作为交易 1 数据信息的数

字签名与交易 1 数据一起发送给接收方。用户 2 收到信息之后,将对交易 2 的合法性进行验证,用户 2 使用与上一步相同的哈希函数从接收的交易数据信息得到哈希摘要,之后利用用户 1 的公钥对上一步附加的数字签名进行解密得到另一哈希摘要。接受方(用户 2)将两个摘要进行对比,若二者内容相同,接受方(用户 2)就能确认该数字签名是发送方的,即确认交易单有效。非对称加密技术的应用保证了交易数据一致,确保了数据的真实和安全。

5 数据一致性维护体系架构

基于以上研究,文中提出了区块链数据一致性体系架构,如图 6 所示。该架构构建了面向区块链数据一致性关键技术研究的新模型,形成了一种新的数据记录、存储和展现的方式。

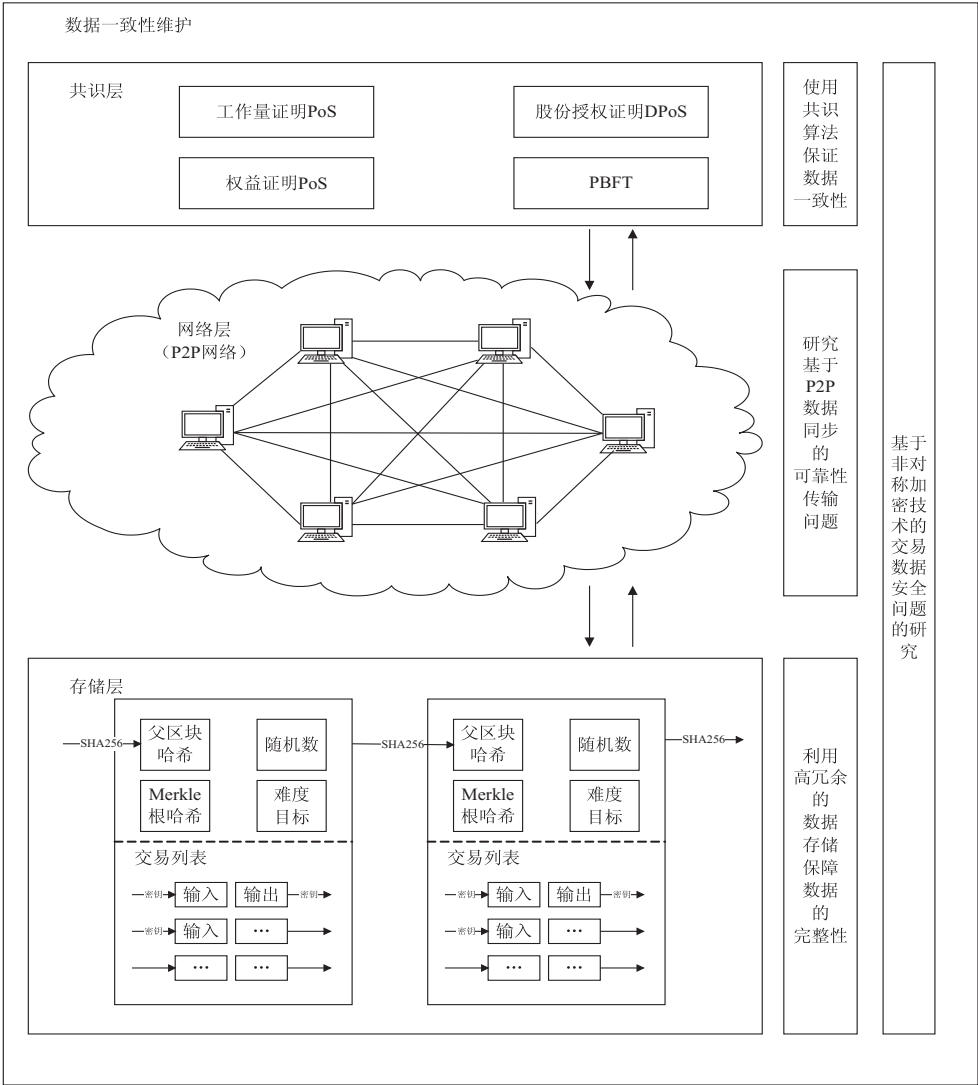


图 6 区块链数据一致性体系架构

该体系架构分为存储层、网络层、共识层和数字加密四个关键部数据存储在存储层主要利用块数据结构保障数

据存储的完整性,每个数据块将一段时间内接收到的数据交易封装到一个带有时间戳的数据区块中,并链

接到当前最长的主区块链上存储,形成最新的区块。该层涉及区块存储、链式结构、哈希算法、Merkle 树、时间戳等主要技术。网络层封装了区块链系统的组网方式、消息传输协议、数据验证机制等要素。结合实际应用需求,存储层上传新区块数据至网络层,网络层通过设计特定的传播协议和数据验证机制能够使每一个节点都参与新区块数据的传输和校验,当数据区块通过全网大部分节点验证后,新区块数据将被节点确认并存储在区块链中。共识层能够在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识,PoW、PoS、DPoS 和 PBFT 可以适应不同场景下共识的一致性需求。网络层节点数据上传至共识层,共识层中一系列共识算法可以确定新区块生成的方式,并且确认交易数据的一致性,保证全网数据保持同步。数字加密是保证区块数据安全的基础技术,其贯穿数据一致性维护的整个底层架构。一方面,数字加密对数据进行签名认证、确认数据所有权、使用权和流通过程;另一方面,数字加密技术可以通过多种加密方法保障数据不被泄露,使得区块数据是全网认可的、透明的和可追溯的。

6 结束语

区块链所存储数据的一致性直接关系到系统的高可用性和高可扩展性,只有分布式系统中各节点数据保持一致,区块链系统中数据才真实可信。文中依托工业和信息化部通信软科学项目的支持,对区块链底层进行深入研究,详细阐述了区块链是如何通过分布式数据存储技术、数据传输协议技术、共识机制技术、非对称加密技术等技术来保证数据一致性的。

区块链中数据一致性维护研究的技术成果必将促使越来越多的研究人员将区块链技术的关注重点由区块链的数字货币应用转移到区块链的底层数据一致性维护的共识算法和可靠性传输协议研究方面来。文中的研究成果可以为现实应用场景中数据一致性维护提供参考,为国内区块链技术发展与应用场景落地提供理论依据和技术支持,也会为区块链技术将物理世界的实体资产转移改变为链上智能资产的合约化转换的平行社会架构奠定技术基础。

参考文献:

- [1] SWAN M. Blockchain: blueprint for a new economy[M]. [s.l.]: O'Reilly Media, Inc., 2015.
- [2] 李 茜. 国内首个区块链标准发布[N]. 上海金融报, 2017-05-19(A03).
- [3] 蔡维德, 郁 莲, 王 荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.
- [4] 朱 岩, 甘国华, 邓 迪, 等. 区块链关键技术中的安全性研究[J]. 信息安全研究, 2016, 2(12): 1090-1097.
- [5] 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.
- [6] 袁 勇, 周 涛, 周傲英, 等. 区块链技术: 从数据智能到知识自动化[J]. 自动化学报, 2017, 43(9): 1485-1490.
- [7] KRAFT D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2): 397-413.
- [8] 何 蒲, 于 戈, 张岩峰, 等. 区块链技术与应用前瞻综述[J]. 计算机科学, 2017, 44(4): 1-7.
- [9] 魏恒峰. 分布数据一致性技术研究[D]. 南京: 南京大学, 2016.
- [10] PASS R, SEEMAN L, SHELAT A. Analysis of the blockchain protocol in asynchronous networks[C]//International conference on the theory and applications of cryptographic techniques. [s.l.]: [s.n.], 2017: 643-673.
- [11] 田怡萌, 李小勇, 刘海涛. 分布式文件系统副本一致性检测研究[J]. 计算机研究与发展, 2012, 49(S1): 276-280.
- [12] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending bitcoin's proof of work via proof of stake [Extended Abstract]y[J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37.
- [13] GAO Y, NOBUHARA H. A proof of stake sharding protocol for scalable blockchains[J]. Proceedings of the Asia-Pacific Advanced Network, 2017, 44(1): 13-16.
- [14] 夏 清, 张凤军, 左 春. 加密数字货币系统共识机制综述[J]. 计算机系统应用, 2017, 26(4): 1-8.
- [15] PECK M. A blockchain currency that beat s bitcoin on privacy [News][J]. IEEE Spectrum, 2016, 53(12): 11-13.
- [16] 祝烈煌, 高 峰, 沈 蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.
- [17] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//IEEE security and privacy. San Jose, CA, USA: IEEE, 2016: 839-858.