区块链技术

孙善勇 张玉清*

[中国地质大学(北京)信息工程学院,北京 100083]

摘要:区块链技术源于比特币系统的底层框架,是具备去中心化、去信任化、集体维护、时序数据、可编程和不可篡改等特点的分布式存储方案,对于金融领域乃至整个宏观社会系统具有重大历史意义. 区块链是由一些已经成熟的技术整合而成,数据层、网络层、共识层、激励层、合约层和应用层构成了区块链底层基础架构. 区块链目前主要有公有链、联盟链及私有链 3 类,主流开发平台有以太坊和超级账本. 本文从区块链技术定义概述出发,介绍了区块链底层基础架构,阐述了各层架构中应用的核心技术,归纳了区块链主要类别以及相应类型下的区块链应用底层开发平台,最后列举了区块链技术当下面临的主要问题,希望能够为相关研究和学习提供参考.

关键词:比特币;区块链;共识机制;智能合约;以太坊;超级账本

中图分类号:TP315 **DOI**:10. 19789/j. 1004-9398. 2020. 02. 015

0 引 言

区块链源自以比特币为代表的数字货币系统支撑技术,具有去中心化、去信任化、不可篡改、集体维护、时序数据等特点. 在分布式网络中实现去中心化的点对点交易,并且无需节点信任,有效地解决了高成本、低效率以及数据安全问题等中心化机构存在的诸多弊端. 区块链技术如今在众多领域的发展潜力已经愈加显著.

本文主体由 5 节组成:第 1 节描述区块链技术定义;第 2 节介绍区块链底层架构,以及架构各层所使用的关键技术点;第 3 节介绍 3 种基本区块链类型,以及每种类型所对应的主流开发平台;第 4 节提出区块链技术的 7 大问题;第 5 节总结全文.

1 区块链技术

谈到区块链,多数人会把区块链和比特币混为一谈,比特币是一种基于点对点支付的数字货币,区块链是这种系统的底层实现技术. 狭义的讲,区块链是由区块数据按照时间为顺序,以图 1 的形式链接组成的一种数据结构,由密码学技术实现数据的不可篡改性和不可伪造性[1],是一种去中心化共享账本,或称为分布式数据库系统.

收稿日期:2019-03-17

* 通信作者:yqzhang@ cugb. edu. cn

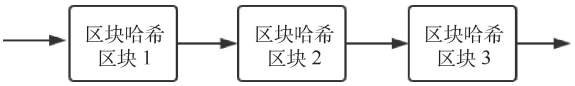


图 1 区块链接示例

区块链技术则是指多个节点间,基于加密链式区块结构、分布式节点共识协议、P2P 网络(对等网络)通信技术和智能合约等技术,组合而成的一种去中心化基础架构. 区块链技术是多项成熟技术的一次整合.

2 区块链架构及关键技术

区块链的基础架构由图 2 所示,每个层次相互协作,共同构成了区块链底层结构基础.

2.1 数据层

数据层用来存储数据区块,涵盖了时间戳、Merkle 树、非对称加密和哈希函数等技术点,确保数据的可追溯性和不可篡改性.

数据区块结构上有区块头和区块体 2 个部分. 区块头记录版本号、父区块哈希值、时间戳、随机数和 Merkle 根等信息. 区块体中存储以 Merkle 树为组织形式的交易数据. 数据区块以时间戳为顺序构成链式结构[2].

Merkle 树可用于快速校验区块数据的存在性和完整性. 椭圆曲线密码算法是区块链技术中使用的非对称加密方式,拥有公钥和私钥 2 个密钥的非对称加密方式确保了数据安全.

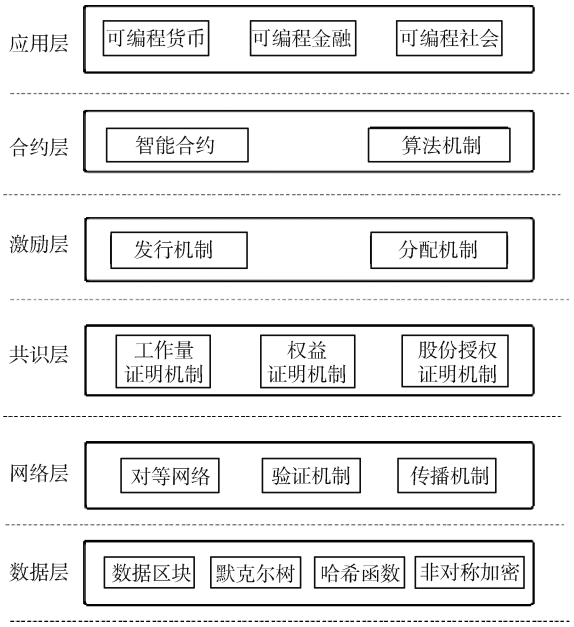


图 2 区块链技术架构

2.2 网络层

组网方式、消息传播协议、数据验证机制等构成了网络层. 构建去中心化的节点拓扑分布,任意 2 个节点无需建立互信即可交易,交易信息通过广播传递,为了维持整个网络的正常运转,利用激励机制来保证拥有足够的节点参与贡献算力.

扁平式拓扑结构的 P2P 组网方式,使得网络中的每个节点承担相同角色,主要具备路由发现、验证交易信息、广播交易信息和发现新结点等功能[1]. 整个网络的正常运转不会被部分节点的损坏而影响,但同时提高了维护全部节点的成本.

全部的网络节点会实时监听网络中的广播信息,发现其他节点的广播数据后,会查看交易中的签名和时间戳等标记,并利用区块的工作量证明去验证此次交易和区块有效性. 若通过验证则进行存储并继续转发广播. 否则,废弃此数据信息并不再转发.

节点通过广播将自己生成的交易信息向周围节点发送,其他节点验证通过后继续传播,当大多数(51%)节点接收到信息后即为交易通过. 若信息验证未通过,便会废弃,停止继续传播错误信息.

2.3 共识层

去中心化网络中的决策权高度分散,必须有效实现各节点对数据的有效性,高效地达成共识. 共识层利用工作量证明机制(PoW)、权益证明机制(PoS)、股份授权证明机制(DPoS)以及分布式一致性算法等几种方案[3],有效地解决了这个问题.

共识过程与经济激励的结合极大地增强了区块网络的可靠性. 在 PoW 机制中,要想达到篡改或伪造区块的目的,必须对此区块以及后面的所有区块都重新寻找随机数[4],控制区块网络 51% 以上的算力后才有可能,因此攻击的成本极大.

为了克服 PoW 算力资源被浪费,以及 51% 攻击等问题,PoS 机制用权益证明(币龄和代币数量等)来替代 PoW 中的算力证明,挖矿难度随着拥有的资源数量增多而减小. 在一定程度上违反了完全去中心化的概念.

DPoS 机制类似董事会投票,每个节点可将其权益授权于一个节点代表,节点代表对其他节点负责,由节点代表轮流记账的形式生成新区块. 由于减少了数据验证时节点参与的数量和记账权竞争的资源消耗,实现了秒级的共识验证.

在联盟链中不同于完全去中心化要求的公有链,其更适合无需大量消耗算力资源的分布式一致性算法. 在区块网络中推选出一个主节点,来完成产生新区块、广播节点交易信息等工作.

2.4 激励层

在激励层将经济因素集成到区块链体系之中,共识节点之间构成了服务众包机制[5]. 共识节点既可最大化自身的利益,又可保障整个系统有效地整体运作. 比特币系统常见的分配机制有每 N 股支付、每股支付和按比例支付等.

2.5 合约层

合约层的本质是区块链底层的商业逻辑及算法[6],合约层的存在能够实现对区块数据的灵活操作,还可在合约层实现区块链系统的应用编程. 比特币平台使用脚本去保证合约控制,新一代区块链平台大多开始使用智能合约.

使用编程语言编写的智能合约实现了商业逻辑,在区块链中的全部节点发布合约,被调用时会在虚拟机上进行运行,运行后无法被强行停止. 将交易的商业逻辑以及访问数据的规则封装为智能合约后,外部应用通过调用智能合约来跟区块链进行访问区块状态或交换数据等操作.

智能合约的主要优点包括:较低的人为干预风险、准确的执行、高效的实时更新、去中心化的权威以及低运行成本[7]. 智能合约为数据层的数据赋予了可灵活编程的机制,承担起了区块链中的机器代理的的角色.

2.6 应用层

基于区块链平台在应用层可实现各种应用场景和现实案例.

区块链 1.0 支持虚拟货币相关应用,可构建与转账、数字化支付相关的去中心化电子货币应用,能够实现跨国交易和快捷支付等多样化服务. 比特币应用是其典型代表.

区块链 2.0 增加了智能合约的创新应用,智能合约在金融领域被作为金融市场的公正基石之后,在债券、股票、产权、贷款和抵押等方面便可得到广泛应用. 同时将技术拓展到支撑一个去中心化的市场,扩大交易范围.

区块链 3.0 则是以去中心化的思想去配置全球资源,将区块链的应用范围拓展到货币和金融以外的领域. 比如政府选举、文化版权、社会公正和健康医疗等.

3 区块链类型

区块链类型可基本被分为公有链、联盟链和私有链 3 类. 公有链最早出现,是最能体现区块链理念的一种类型. 针对当下的需求场景和公有链的一些问题,具备联盟属性的联盟链开始被推向市场. 私有链是开放程度最低的一种类型,仅供内部人员使用. 目前区块链开发平台层出不穷,图 3 列举了一些当前主流区块链应用开发平台.



图 3 主流区块链平台

3.1 公有链

公有链完全对外公开,用户可自由访问区块网络,以及在链上广播交易数据,还可即时参与网络共识过程.

公有链是真正具备完全去中心化特征的区块链,能够在去信任化的网络环境中快速建立共识,形成去中心化的运行机制[8],并且交易信息不可篡改. 共识机制一般采用 Pow 或 PoS. 比特币系统就是基于公有链,但其应用范围仅限于数字货币类型,以太坊(Ethereum)是在公有链场景中应用最广泛的通用开发平台.

3.2 联盟链

联盟链中只有联盟成员可加入联盟链网络,按照联盟规则来制定用户在链上的读写权限和记账权限. 由于联盟链的注册许可限制的特征,对于金融机构的交易、结算或清算场景非常适用. 共识机制对安全性能要求较高,一般采用权益证明或实用拜占庭容错算法、Raft 算法等共识算法来代替工作量证明的挖矿机制. 常见平台有超级账本(Hyperledger)以及国内的 FISCO-BCOS.

3.3 私有链

私有链网络仅在私有组织内部使用,按照私有组织规则来制定用户在链上的读写权限和记账权限. 应用场景一般是数据库管理和审计等企业内部的私有应用. 私有链可有效防范来自内部或外部对数据的安全攻击. 许多公有链是基于无政府主义理念而设计的,所以采用 P2P 网络以实现完全去中心化. 私有链是由私有组织进行管控,数据信息不对外开放,只有内部人员能够参与.

4 区块链存在的问题

(1)安全问题.

基于 PoW 共识协议的区块链系统,51% 攻击问题是其面临的最大安全威胁,虽然通过掌握 51% 算力去攻击网络难度极高,并且收益小于投入,但是威胁始终存在.

(2)匿名性和隐私性.

区块链网络中的节点并不具备真正的匿名性,在数据传输时仍然给出了一个地址,就拥有了被识别和定位的可能性,导致隐私性无法保障.

(3)吞吐效率.

区块链系统安全性的确保牺牲了性能指标[9],交易数据的签名、验证以及区块的哈希运算等都占用大量系统开销. 比特币系统每秒最多仅能完成 7 笔交易,吞吐量仅仅为 7 TPS;以太坊的吞吐量也仅为 25 TPS.

(4)资源浪费.

PoW 共识机制中的大部分算力消耗在搜索随

机数,进行哈希运算的过程中,并没有产生实际的价值,是一种典型的资源浪费.算力证明导致世界范围内大量矿池的出现,同样是资源的浪费.

(5)数据空间存储.

区块网络中的所有节点存储着相同的数据信息,当数据与日俱增积累到一定量级时,如何有效的解决存储空间的需求问题是一个严峻挑战.

(6)并发处理.

区块链网络是以 P2P 形式相互关联,每个节点的身份对等,对于高并发服务场景下的相关设计不够周全.

(7)去中心化的自治组织.

当下的区块链系统本质上并未达到完全的去中心化,更多的是一种弱中心化或多中心化[10].

5 总 结

本文概述了区块链技术的基本原理、技术要点和基本类别,希望能够对区块链初学者提供有价值的启发与帮助.人工智能、物联网技术飞速发展,区块链技术可以与其进行广泛的深入结合,未来的"区块链 +"时代定会改变人类生活方式,给社会发展带来深刻变革.

参 考 文 献

[1] 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 - 194

[2] 孙国茂. 区块链技术的本质特征及其金融领域应用研究[J]. 理论学刊,2017(2):58 - 67

[3] HUGHES F, MORROW M J. Blockchain and health care[J]. Policy, Politics & Nursing Practice,2019,20(1):4 - 7

[4] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J].计算机学报,2018,41(5):969 - 988.

[5] 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.

[6] 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 - 15.

[7] 邹均,曹寅,刘天喜.区块链技术指南[M]. 北京:机械工业出版,2016:12 - 33.

[8] 杨保华. 区块链原理设计与应用[M]. 北京:机械工业出版社,2017:44 - 55.

[9] 马昂,潘晓,吴雷,等. 区块链技术基础及应用研究综述[J]. 信息安全研究,2017,3(11):968 - 980.

[10] KIM Y, RAMAN R K, KIM Y S. Efficient local secret sharing for distributed blockchain systems[J]. IEEE Communications Letters,2019,23(2):282 - 285.

Summary of Blockchain Technology

SUN Shanyong ZHANG Yuqing

(School of Information Engineering, China University of Geosciences, Beijing 100083)

Abstract: Blockchain technology originates from the underlying framework of the Bitcoin system. It is a distributed storage scheme with the features of decentralization, de-trust, collective maintenance, time series data, programmable and non-tampering, etc. It is provided with great historical significance to the financial field and even to the whole macro social system. The blockchain is composed of some mature technologies. The data layer, network layer, consensus layer, incentive layer, contract layer and application layer constitute the bottom structure of the blockchain. At present, there are three main categories of blockchain: public blockchain, consortium blockchain and private blockchain. The mainstream development platforms include Ethereum and Hyperledger. Starting from the definition of blockchain technology, this paper introduces the basic architecture of blockchain, expounds the core technologies used in each layer architecture, and summarizes the main categories of blockchain and the underlying development platform of blockchain application under the corresponding types. Finally, the main problems faced by blockchain technology at present are listed. We hope to provide reference for relevant research and study.

Keywords: bitcoin; blockchain; consensus mechanism; smart contract; ethereum; hyperledger