基于以太坊的分层区块链架构研究

黄振业[1] 苏 波[2]

[1](浙江金融职业学院信息技术学院 浙江 杭州 310018)

[2](北京魔链科技有限公司 北京 100080)

摘 要 针对以太坊区块链技术不能在完全去中心化、一致性和可扩展性上得到同时满足的缺点,以及它在应用落地方面的缺陷等问题,结合区块链技术发展的前沿方向,提出一种采用双层链设计架构的改造方案。通过将交易存储和智能合约计算分离的方法,使以太坊区块链技术支持符合互联网应用要求的复杂算法,优化分布式应用终端用户的体验,使得以太坊区块链技术在艺术品行业得到更好的应用,探索解决区块链技术应用落地的难题。

关键词 区块链 以太坊 分层 去中心化

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.09.003

LAYERED BLOCKCHAIN ARCHITECTURE BASED ON ETHEREUM

Huang Zhenye[1] Su Bo[2]

[1](*School of Information Technology, Zhejiang Financial College, Hangzhou 310018, Zhejiang, China*)

[2](*Beijing Moochain Technology Co., Ltd., Beijing 100080, China*)

Abstract Aiming at the shortcomings of Ethereum Blockchain technology that cannot be completely decentralized, consistent and scalable at the same time, as well as its defects in application and landing, combined with the frontier direction of Blockchain technology development, this paper proposes a transformation scheme using double-layer chain design architecture. By separating transaction storage from smart contract calculation, the Ethereum Blockchain technology supports complex algorithms that meet the requirements of Internet applications. It optimizes the experience of dApp end users, makes the Ethereum Blockchain technology better applied in the art industry, and explores solutions to the problem of promoting the application of Blockchain technology.

Keywords Blockchain Ethereum Layered Decentralization

0 引 言

2008 年 11 月,有人以中本聪(Satoshi Nakamoto)为化名发表了一篇研究论文[1],介绍了一种名叫比特币(Bitcoin)的新型电子现金系统。这种全新的数字货币具有使用方便、难以追踪等特性,它组合了密码学、工作证明和点对点网络等技术[2],创新地提出了一种分布式时间戳服务器,可用于分布式系统中数据的有序存储,这项技术在之后被称为“区块链”(Blockchain)[3]。世界各地的一些计算机爱好者利用设备和特殊软件进行“挖矿”,并形成一个网络来共同维持区块链。经过几年的发展,人们发现其潜力远不止电子货币。以 2015 年 10 月英国《经济学人》杂志发表的《信任的机器》(The Trust Machine)的封面文章为标志,大家意识到作为比特币底层技术的区块链,其价值甚至超过了比特币本身的价值。

比特币被称为区块链 1.0,因为比特币本身只是区块链技术在金融领域的一个应用,并没有太多办法在其上开发其他去中心化的应用。2015 年初,被称为区块链 2.0 的以太坊的第一个版本面世了。以太坊是一个去中心化区块链应用的开发平台,它对比特币区

收稿日期:2019-07-03。浙江省教育厅一般科研项目(Y201839058)。**黄振业**,讲师,主研领域:区块链技术,大数据。**苏波**,高工。

块链的一个最主要的增强是引入了图灵完备的智能合约,开发者可以编写智能合约代码来实现其行业内在的业务逻辑,这为应用区块链技术解决行业问题打开了广阔的空间。

1　问　题

随着区块链技术在传统行业中的大量应用,现有区块链平台的局限逐渐暴露出来,人们发现以太坊在实际行业应用落地中面临着诸多问题。

在分布式系统领域有一个帽子(CAP)理论:一个分布式系统不可能同时实现一致性(Consistency),可用性(Availability)以及分区容忍性(Partition Tolerance)。它可满足其中任意两个要求,但不能同时满足三个。对应在区块链工程技术领域,也有一个"不可能三角":完全去中心化、安全性和可扩展性,三者不可以兼得。如图 1 所示。

(1) 完全去中心化(Fully Decentralized):网络中在逻辑上不存在单个或多个中心节点。

(2) 安全性(Security):网络是否存在被恶意攻击导致瘫痪、区块被篡改的可能性。

(3) 可扩展性(Scalability):可以通过增加计算资源等方式有效提高网络的吞吐能力。

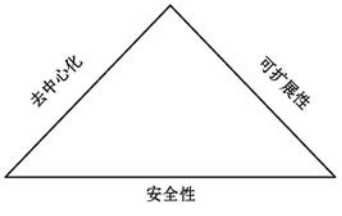

图 1　区块链"不可能三角"

比特币和以太坊做到了完全去中心化和安全性,所以可扩展性(效率)很差,比特币的交易处理能力约为 7 TPS,以太坊的交易处理能力大约为 15 TPS,并且无法通过扩展服务器数量和计算能力来提高。

2　分　析

既然区块链技术领域存在一个无法突破的"不可能三角",那么怎样在工程领域突破这个理论限制,让区块链技术可以在更广阔的空间里得到应用? 目前存在以下几种探索的思路。

2.1　部分牺牲去中心化

牺牲"不可能三角"的一维,只实现部分的去中心,即可达到较好的可扩展性。时下比较热门的 EOS 项目即采用这种办法[4],使用委托权益证明机制(Delegated Proof of Stake,DPOS)共识算法,只有"授权代表"有记账的权力。"授权代表"是拥有超级计算能力的超级节点,由区块链网络中用户投票选举产生,因为总数不多且计算能力强,因此,提高了全网同步的速度及出块的速度。

这种实现部分去中心的做法在实际应用中是有应用场景的,因为现实世界中很难找到可以完全去中心化的业务场景,所以很难说它不是比完全去中心化的区块链更符合实际;缺点则是中心化导致的不安全、超级节点易被攻击以及串通作恶等问题。

2.2　提高网络吞吐能力

传统的区块链是链表式数据结构,每个区块(Block)唯一记录着前一个区块内容的哈希值(Hash),每个区块有固定的出块时间,必须保证一定的时间间隔,才能在全网或者"授权代表"间达成共识。这种链表结构以及同步机制决定了传统区块链网络的吞吐能力。

对此,有一种做法是采用图论中的有向无环图(Directed Acyclic Graph,DAG)进行改进。相比于一般图,DAG 的很多问题可以在多项式级甚至线性复杂度条件下得到解决,这使得通过 DAG 结构记录交易账本并取得分布式共识成为可能。

采用 DAG 技术的区块链中,交易不再是按照区块进行组织,各个交易之间按照一定的规则组成 DAG 网络,确实可以提高区块链网络的吞吐能力。原因在于,不必在一定的时间间隔后才能出块,交易经过广播后可以直接上链。但缺点是,即使上链了,仍然需要等待一段时间以得到足够多的交易确认才算达成共识;同时系统的复杂度大大增加了。

图 2 为采用 DAG 技术的区块链网络结构图,来自 Byteball 项目白皮书[5]。

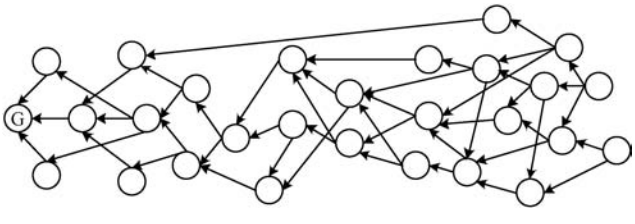

图 2　采用 DAG 的区块链结构

2.3　系统分层

分层处理方法在计算机软件系统设计中是一种经过验证的比较普遍的系统设计思路,适用于设计复杂的软件系统,可以提升系统的处理能力。互联网最成功的分层设计就是网络协议分层,就是我们熟知的七层网络结构。其基本设计原则是:各层是独立的,各自层做好自己的事即可;层和层之间的功能是不一样的;层和层之间的交流都是通过接口通信,只要接口保持

不变,层内部的设计可以改变,且不会影响别的层。

区块链系统的技术堆栈可分三个层次:相互通信的计算机节点网络;让节点可以一致认可新区块的共识算法;拥有自身状态的应用层(区块链状态机,存储智能合约的最终计算结果)。这三个部分构成一条完整的区块链,如图 3 所示。

图 3 区块链系统分层结构图

除此之外,区块链系统还流行一种多链的技术架构,即:一个单一的区块链网络由多条区块链组成,不同的链有不同的角色定位。如比特币区块链有闪电网络作为侧链[6],以太坊有 Plasma 作为二层链[7],卡尔达诺链分为两层[8]。多链架构中的主链通常是完全去中心化,负责记账结算;所谓的侧链、子链或二层链有部分中心化的特征,以提高处理效率。

3 方 案

本文方案将以太坊区块链的交易处理和智能合约的计算分离。这是一个双层链:L1 层是结算层,只处理交易数据,没有智能合约,采用 DAG 技术,以提高网络吞吐能力,提升终端用户体验;L2 层是计算层,实现智能合约,采用高性能的超级计算节点,在后台实现商业应用要求的复杂计算。L1 层和 L2 层区块链可解耦,将来 L2 层可以适配新的更高效的 L1 层区块链;L1 层可以采用适用于记账结算的任何共识算法,L2 层则必须采用委托权益证明共识算法或类似的“授权代表”算法。

3.1 技术架构

技术架构如图 4 所示。

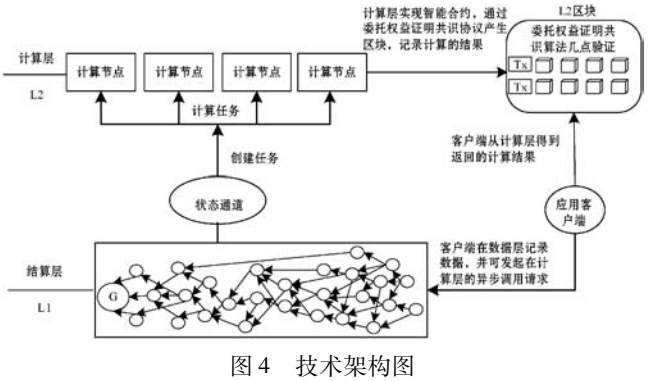

图 4 技术架构图

如图 4 所示,在系统中并行着两条区块链,基础的是结算层。结算层记录用户之间的转账交易,也可以触发对智能合约的调用;但是智能合约的发布和运行并不在结算层,是在计算层区块链上。

我们在从头同步一个以太坊全节点时会发现,区块的同步很快就可以完成,通常是几个小时的工作量;之后对状态的同步经常要花费数天的时间才可以更新到最新的状态。原因是区块仅仅是记录着交易,没有计算的工作量,截至本文撰稿日时,一共有 7 750 921 个区块,平均大概每分钟产生一个区块。但是状态就不同了,状态的数量是由智能合约中记录的可持久变量和智能合约被调用的次数决定的。而且状态的同步是需要每个节点在本地重新对智能合约进行运算来完成的。这对以太坊节点来说是个不可承受的工作量。

这就是将以太坊原有的结构分拆为两条链的原因。让结算层区块链只完成记账结算的功能,这样结算层的节点以普通的计算机资源即可运行,可以加入更多的节点来去中心化;把智能合约的运算放在计算层,留给计算层的超级节点或者云来完成。两者采用异步通信的方式。

3.2 技术实现

(1) 结算层。结算层采用 DAG 技术实现,账户系统采用未花费的交易输出(Unspent Transaction Output,UTXO)模式[1],不像以太坊通过状态记录账户钱包余额,仅仅通过区块即可计算账户余额。交易分为两种,一种是用户间转账,另一种是调用智能合约。对智能合约的调用是异步的,计算层将监听对智能合约的调用进行实际的合约代码执行。在结算层上可以采用去中心化效果较好的工作量证明(Proof of Work,PoW)或权益证明(Proof of Stake,PoS)共识算法,以获得更多的用户支持和更安全的网络。对于普通的转账结算的用户来说,只同步结算层的区块链就可以了,不需要对计算层做同步,可以实现点对点支付、积分等简单记账类的应用。

(2) 计算层。在计算层我们采用超级节点的方法,超级节点提供智能合约的计算服务。可以在超级节点上提供强大的计算资源,甚至在超级节点的背后采用云计算、并行计算技术来提供充足的算力。超级节点读取到结算层发起的对智能合约的调用请求,采用委托权益证明共识机制,选举一个出块人,执行智能合约的计算,并应用计算结果修改状态机的全局最终状态,将此全局最终状态打包进区块并用私钥签名,广

播给其他节点进行验证;其他节点验证无误后添加自己的签名,该区块最终获得足够多的签名确认,被区块链网络所接受。智能合约的调用者可以选择信任某个超级节点,订阅事件通知,异步收到智能合约的调用结果;有一定算力的用户也可以同步计算层的状态,以在本地进行验证。

(3) 层间通信。结算层不知道计算层的存在,计算层可以看到结算层,并监听和读取结算层的区块数据。两者的数据分开存储:交易数据存储在结算层,状态数据存储在计算层。

4　测　试

本文给出的设计架构仍然在设计开发阶段,并没有得到实际的测试数据来检验是否能够达到预期的改进目标。

一份对采用 DAG 技术的区块链 Byteball 主网的最新测试给出了三点结论:

(1) 交易处理速度仅能达到 15 TPS 左右;

(2) 网络容易遭受 DoS 攻击,大量突发式的恶意交易会阻塞网络、降低网络的交易处理速度;

(3) 随着交易数量增加,交易确认时间可以保持平稳。

作为 DAG 基础链,这个压力测试和大家的预期很不相符,显然没有充分发挥 DAG 技术的优势。不同于传统区块链交易处理速度受限于区块大小,Byteball 网络的交易处理速度与代码执行速度、网络传输时延、硬件处理能力等都可能有关系。Byteball 的创始人认为其代码实现中大量的 SQL 连接操作增加了处理时延,这可能是影响 Byteball 处理性能的重要原因。

显然,如果仅仅是 SQL 查询导致的性能问题,这实际上是区块链技术限制之外的领域,是比较容易进行优化的。但仍然需要在实际的产品测试中不断地去检验其产品的设计架构是否满足预期,并适时调整。

5　应用案例

我们已经计划使用以上的设计架构来实现一些行业应用的需求,比如在艺术品行业,我们正在开展一个全新的基于区块链的艺术品平台,在此之上建立一个开放的艺术品价值发现平台,通过技术手段为艺术品建立可信的价值评判体系。如表 1 所示,艺术品行业存在的行业痛点,以及期待采用区块链技术可以解决的问题。

表 1　艺术品行业痛点

痛点	传统艺术品市场	艺术品区块链平台
真伪难辨	纸质证书或某机构的中心化数据库,信息孤岛,制假造假空间大	区块链上登记艺术品相关信息的哈希,可以追溯历史交易记录
价格操控	由少部分人操盘,价格虚高、封闭、定价不均且各不一样,卖家吃亏、不相信或不敢买	由大众定价,提供市场参考价,买家相信,带动成交量
分配不均	机构通过炒作艺术家,获得大量金钱,而艺术家本身并没有从艺术品的增值中得到相应报酬	原创艺术家可以自动获得每次交易增值部分的分成
流通不足	大量艺术品通过虚假炒作套取升值空间,艺术品市场成为小圈子文化,大众无法参与	由登记和定价带动公开透明的价值交易,传统艺术品圈子以外的广大爱好者人群都可以参与

为解决以上的痛点,规划该艺术品区块链的三大功能模块:登记平台、定价平台和交易平台,如图 5 所示。为了完成艺术品的完整交易流程,在区块链上实现对艺术品的登记追溯、定价投票和在线交易。

图 5　艺术品区块链功能结构图

以上业务流程需要在智能合约中实现,包含大量的计算工作量,需要良好的用户体验,这在目前的以太坊区块链上是无法进行的,而本文提出的方案可以解决这个问题。

6　结　语

本文介绍了区块链 2.0 时代的代表——以太坊在当前阶段面临的问题,同时面临着解决当前问题的“不可能三角”,在此种情况下根据区块链行业技术的最新发展,提出几种可能的改进方向,包括:部分牺牲去中心化、应用 DAG 技术和系统分层。

同时,基于这几种改进的方向,提出一个分层的区块链设计架构,在底层结算层应用 DAG 技术提供交易的吞吐量,建立一个“第二层”——计算层实现智能合约功能。

(下转第 26 页)

4 结 语

本文结合先进的开源框架,实现了基于 WebGIS 的龙海市自然资源“一张图”管理信息系统。系统具有“统一数据访问、统一权限管理、统一日志管理”的优势,为数据的访问和获取提供便捷,有利于检查系统发生错误的原因,提升了系统的安全性、可扩展性和可维护性。

本文系统将自然资源空间数据和业务数据相结合,针对龙海市自然资源局各职能部门设计了不同的功能,在数据查询、统计分析、辅助审核、制图和数据可视化展示等方面具有实际应用价值。通过使用本文系统,龙海市自然资源局各职能部门可快速准确地掌握该地区土地、矿产、地质灾害等各类自然资源的布局和具体信息,有效提高了工作人员的办公效率,提升了数据共享程度,达到了增强自然资源数据管理水平的效果。本文构建的系统同时可为其他领域的“一张图”系统的建设提供有效的借鉴和参考。

参 考 文 献

[1] 黄俊,朱思源. 柳州国土资源“一张图”管理系统设计与实现[J]. 安徽农业科学,2010,38(20):10978 - 10980.

[2] 孙在宏,吴长彬. 基于“一张图”的土地动态监测系统研究[J]. 测绘通报,2012(6):22 - 24,100.

[3] 马晓云. 水文水资源“一张图”管理系统的设计与实现[J]. 测绘通报,2016,(11):114 - 117.

[4] 罗鹏,许等平,任怡. 全国林地“一张图”高性能地图瓦片服务技术研究[J]. 中南林业科技大学学报,2018,38(7):26 - 31.

[5] 侯水云,毛善君,李文生,等. 煤矿地测“一张图”平台关键技术研究[J]. 煤炭科学技术,2017,45(8):32 - 36,54.

[6] 张娜娜. 城乡规划一张图系统的建设实践探讨——以成都市温江区为例[J]. 测绘通报,2015(6):108 - 111.

[7] 任建刚,李瑞群. 煤矿“一张图”系统开发及应用[J]. 煤炭工程,2018,50(11):63 - 66.

[8] 吴庆双,吴松. 基于 GIS 的开发区“一张图”管理信息系统建设[J]. 安徽师范大学学报(自然科学版),2017,40(1):77 - 83.

[9] 许等平,罗鹏,郑冬梅,等. 林地一张图国家级互联网服务平台设计与实现[J]. 林业资源管理,2018(3):121 - 128.

[10] 魏圆圆,王雪,王儒敬,等. 基于 WebGIS 的农场生产管理信息系统的设计与实现[J]. 农业工程学报,2018,34(16):147 - 155.

[11] Zhang B, Ye Y W, Shen X Z, et al. Design and implementation of levee project information management system based on WebGIS[J]. Royal Society Open Science,2018,5(7):180625.

[12] Cui B, Zhou Z, Wang X, et al. System development for storm surge hazard assessment based on WebGIS for Tianjin Binhai New Area[J]. Transactions of Tianjin University, 2016, 22(1):50 - 56.

[13] Frederik V R, JamalJokar A, Andreas R. Visualization of geologic geospatial datasets through X3D in the frame of WebGIS[J]. International Journal of Digital Earth, 2013,6(5):483 - 503.

[14] 王伶俐,张传国. 基于 NodeJS + Express 框架的轻应用定制平台的设计与实现[J]. 计算机科学,2017,44(S2):596 - 599.

[15] 冯永玉. 省级国土资源“一张图”数据中心建设探讨[J]. 山东国土资源,2014(11):67 - 70.

[16] 刘文杰,李明建,岳俊,等. 基于 GIS 的煤矿地质测量信息系统的设计与开发[J]. 西南大学学报(自然科学版),2012,34(10):143 - 149.

(上接第 19 页)

虽然该设计架构并未得到实际测试数据的支持,但在一定程度上代表着区块链技术的演进方向,至少是一种短期内有效的临时解决方案,因为不可否认,目前对于区块链技术来讲还是处于早期的发展演进阶段,长期的解决方案仍然在技术构想或者正在开发中。

参 考 文 献

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [OL]. 2009. https://bitcoin.org/bitcoin.pdf.

[2] Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies[J]. IEEE Communications Surveys and Tutorials 2015, 18(3):2084 - 2123.

[3] 常兴, 赵运磊. 比特币扩容技术的发展现状与展望[J]. 计算机应用与软件, 2019, 36(3):49 - 56.

[4] EOS 项目官网[OL]. [2019 - 05 - 15]. https://eos.io/.

[5] Churyumov A. Byteball: a decentralized system for storage and transfer of value[OL]. 2019. https://byteball.org/Byteball.pdf.

[6] Poon J, Dryja T. The bitcoin lightning network: scalable off-chain instant payments[OL]. 2016. http://lightning.network/lightning-network-paper.pdf.

[7] Poon J, Buterin V. Plasma: scalable autonomous smart contracts[OL]. 2017. https://plasma.io/plasma.pdf.

[8] 卡尔达诺项目官网[OL]. [2019 - 05 - 12]. https://www.cardano.org/zh/home-3/.