计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190800155

基于区块链技术的通证模型的设计与分析

巫光福　陈　颖　曾宪文　何道敬　李江华
江西理工大学信息工程学院　江西 赣州 341000

摘　要　文中通过对传统通证模型进行深入研究后发现,中心化的模式一直制约着通证系统的发展,区块链技术的出现无疑为通证的应用及推广提供了一个切入点,这将打通企业间的信息隔阂。区块链技术是一种互联网数据库技术,其中每一个用户都有相同的权利来编写数据库记录,且一旦记录,不可更改。文中基于区块链技术设计了通证链,该通证链具有去中心化和不可篡改的特点,可打通企业信息壁垒;再结合通证链上的通证的运用,可以增加企业间的信任度,增强企业间的信息流通。在设计通证链上,文中提出了更安全、高效的共识算法,即通证共识算法,使通证链在效率与性能上比传统公有链如比特币、以太坊更具优势。使用可插拔技术实现密码学和数据库的可插拔运用,将使区块链在不同应用场景的开发上更高效、便捷。

关键词:去中心化;通证模型;通证链;共识算法;可插拔技术
中图法分类号　TU375

Design and Analysis of Token Model Based on Blockchain Technology

WU Guang-fu,CHEN Ying,ZENG Xian-wen,HE Dao-jing and LI Jiang-hua
School of Information Engineering,Jiangxi University of Science and Technology,Ganzhou,Jiangxi 341000,China

Abstract　Through in-depth study of the traditional general evidence model,it is found that the centralized mode has always been restricting the development of the system,and the emergence of blockchain technology undoubtedly provides an entry point for the application and promotion of the certificate,which will break the information barrier between enterprises. Blockchain technology is an Internet database technology,where each user has an equal right to compete for writing the database records. In this paper,a pass-through chain based on blockchain technology was designed. The pass-through chain has the characteristics of decentralization and non-tamperability. It can break the information barrier between enterprises and combine the use of the pass on the pass-through chain to increase the trust between enterprises. To enhance the information flow between enterprises,the pass-through chain proposed a safer and more efficient consensus algorithm,that is,the pass-through consensus algorithm,so that the pass-through chain has better efficiency and performance compared with the traditional public chain such as Bitcoin and Ethereum. Using pluggable technology to realize the pluggable applications of cryptography and database will make the blockchain more efficient and convenient in the development of different application scenarios.

Keywords　Decentralization,General evidence model,Pass-through chain,Consensus algorithm,Pluggable technology

1　区块链概述

当大数据、物联网、云计算等技术在各个领域广泛应用时,一种以共识机制为核心结合密码学、P2P 网络、数据库等技术原理的新技术悄然诞生,并在金融、保险、物流、医疗等领域得到广泛的研究与实践。

区块链技术可以首先追溯到 2008 年的比特币,比特币的底层技术就是区块链。2008 年,由化名中本聪(Satoshi Nakamaoto)的比特币发明人发表关于比特币的白皮书《A peer-to-peer electronic cash system》,其描述了一种去中心化、不可篡改、安全、透明的、无国界的、低交易成本的数字货币系统,区块链技术的第一次大规模的应用系统由此出现,标志着进入了区块链 1.0 时代[1]。2013 年,"V 神"(Vitalik Buterin)受比特币启发后提出了以太坊(Ethereum)区块链平台,该平台除了有自身的数字货币体系特征实现数字货币交易外,还可以用 Solidity 语言编写智能合约,使用智能合约实现可编程金融,使各行业内都能轻松实现货币编程体系,称为区块链 2.0 时代[2-3]。区块链 3.0 时代要实现的是除金融外,其他领域内区块链的应用,包括政府、健康、文化和艺术等,这意味着整个社会的数据、信息都将通过区块链技术实现去中心化、不可篡改,可编程社会由此而来[4-5]。

区块链技术的突破本质上是一种数据库系统的突破。传统数据库不管是关系型数据库(Mysql,DB2,SQLite)还是非关系型数据(LevelDB,CouchDB)都可以对数据进行任意的增删改查,并且还能将修改记录也一并删除。但区块链技术的特点却改变了这一状态[6]。

基金项目:国家自然科学基金(11461031);江西省教育厅科技类重点项目(GJJ170492);江西省教育厅科技类一般项目(GJJ180442,GJJ170516);江西省自然科学基金(20181BBE58018)
This work was supported by the National Natural Science Foundation of China (11461031),Key Scientific Foundation of the Education Department of Jiangxi Province(GJJ170492),General Scientific Project of the Education Department of Jiangxi Province,China (GJJ180442,GJJ170516) and Natural Science Foundation of Jiangxi Province,China(20181BBE58018).
通信作者:巫光福(wuguangfu@126.com)

区块链技术主要具有以下4类特点。

(1)去中心化:任何节点都是对等节点。对等节点的数据传输及其他各类权限完全等同,不依赖额外的第三方管理机构或硬件设施。

(2)去信任化:整个系统中的多个参与方无须相互信任就能够完成各种类型的交易和协作。在区块链系统中,各节点依赖自身的共识机制,结合其他技术如密码学技术、P2P等对等节点数据的一致性。

(3)不可篡改:不同于传统数据库可进行任意增删改查的特点,区块链系统只能对数据进行增加和查询操作,通过密码学等技术实现交易及记录的不可篡改。

(4)匿名性:区块链系统如比特币,其身份是由公钥地址实现的,用户无需暴露自己真实身份即可进行相关交易,父地址可无限产生子地址,实现"找零",使得身份更加难以追踪。

2 区块链基础架构

区块链技术的应用模式呈现百花齐放的态势。在国外,比特币、以太坊、EOS和Ripple都是比较前沿的成功案例,国内如布比、NEO和TrustSQL等平台也已经是区块链应用的佼佼者[8-10]。关于区块链的分类有很多种,根据区块链的开放性,可将区块链分为以下3类。

(1)公有链:任何节点无须任何许可便可随时加入或者退出,对等节点的权限相同。节点可以投票、记账、建块、交易,所有节点都有相等的权利,对于公有链来说,任何人都可以对公有链中的数据交易进行访问查询并进行确认。现有的公有链如比特币、以太坊等采用共识效率较低的POW[11]和POS[12],容错性51%,节点可扩展性较强。

(2)联盟链:联盟成员在联盟链中有相应的身份权限,只有组织成员才能在区块链系统中进行交易、确认,只有获得许可的成员才能对系统的相关数据交易进行查询校验。联盟链一般采用BFT类算法,该类算法共识效率高,交易确认时间满足商业级应用,但是节点可扩展性差,容错率也更低[13]。

(3)私有链:企业内部使用的区块链平台,权限完全私有化,仅提供企业内部使用或访问。

不管是公有链还是联盟链,其架构的底层都是区块链的数据来源,包括区块头、区块体、Hash链、密码算法和通信协议等。区块链技术底层由区块及链式结构构成,其中区块分为区块头和区块体,区块头及区块体包含相应的数据结构,相关数据及其识别大多通过密码学算法进行加密处理[14]。

虽然区块链技术的使用越来越多样化,项目体系也趋于成熟化,但万变不离其宗。总体上来看,区块链的基础架构分为6层,包括应用层、合约层、激励层、共识层、网络层和数据层。每一层都会完成一项核心的功能,各层之间相互配合,从而实现一个去中心化的信任机制,如图1所示。

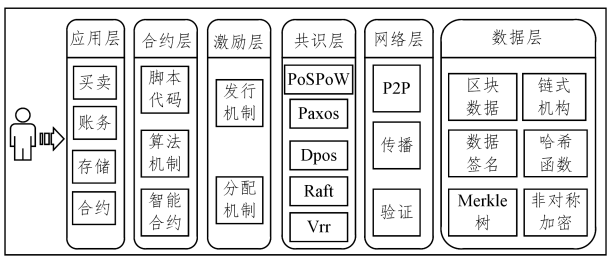

图1 区块链基础技术架构图

Fig. 1 Blockchain basic technical architecture diagram

2.1 数据层

数据层是描述区块链技术的物理形式。区块链系统设计人员首先建立一个起始节点,之后在同样的规则下创建规格相同的区块,通过一个链式结构相连组成一条主链,新的区块通过验证后被不断地添加到主链上,主链不断延长。每一个区块中包含了许多技术,如时间戳技术,它要确保每一个区块都按时间顺序相连接;Hash函数,它使得交易的信息不被轻易篡改。

2.2 网络层

网络层是实现区块链网络节点之间的信息互交。区块链本质上是一个P2P网络,每一个节点都可以创造出新的区块,然后通过广播的形式通知其他节点,其他节点反过来验证这个节点,当区块链网络中超过51%的用户验证通过后,新的区块就可以添加到主链上。

2.3 共识层

共识层能够让高度分散的节点在去中心化的系统中高效地针对区块数据的有效性达成共识,主要的共识机制有工作量证明(Pow)、权益证明(Pos)和股份授权证明(DPos)3种。

工作量证明:每个节点都计算一个随机数,一定时间段内,找到随机数的难度是一定的,最先得到这个随机数的节点,将打包的交易区块添加到已有的区块链上,并向全网广播,其他节点验证、同步,这样就获得工作量证明。

权益证明:系统根据节点持有的Token(代币)的数量与时间的乘积分配相应的记账权,持有的越多,获得记账权的概率越大。

股份授权证明:由全体节点投票选举出一定数量的节点代表,来代理全体节点确认区块并维持系统有序运行。同时,区块链中全体节点具有随时罢免和任命代表的权力。

2.4 激励层

激励层提供一定的激励措施,鼓励节点参与区块链的安全验证工作。例如比特币,其奖励机制有两种,在比特币总量达到2100万枚前,一种是新区块产生后系统奖励的比特币,另一种是每笔交易扣除的比特币;当比特币总量达到2100万时,新产生的区块不再产生比特币,这时的奖励主要是每笔交易所扣除的手续费。

2.5 合约层

合约层主要指各种脚本代码、算法机制以及智能合约等。如比特币,它是一种可编程的货币,合约层封装的脚本中规定了比特币的交易方式和交易过程中涉及的各种细节。

2.6 应用层

应用层封装了区块链的各种应用场景和案例,如基于区块链的跨境支付平台等。

3 传统通证领域体系

3.1 通证类型

通证(Token)是用于资产价值确认的媒介、行业内价值流通的载体,任何有价值的资产都可以被认为是通证。通证体系指的是通过通证确保任意资产的价值得到有效认同,并可以通过通证进行物值流通,确保整个体系通畅[18],其中包括:供应链(如物流通证)、娱乐(如游戏通证)、金融(如金融通证)、公共服务(如资产通证)、物联网和公益慈善等。但各领域传统的通证彼此独立,互不影响,这是制约通证发展的一大障碍。如图2所示,区块链技术不断被熟知、被应用,将区块

链行业中众多角色连接，串联场景，可以实现金融闭环和落地应用。

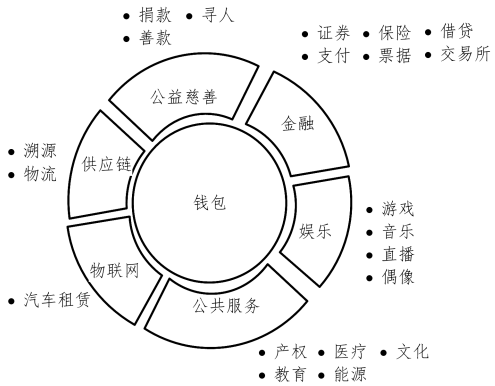

图 2 区块链应用行业

Fig. 2 Blockchain application industries

3.2 传统通证体系分析

由图 3 可知，传统的通证体系下，不管是商户还是会员（客户），在通证的消费和结算上都必须经过通证体系平台，都是单一方向的数据流转，传统的通证体系是基于中心化的模式。尽管存在诸多通证的应用案例，但通证却一直没有被充分利用，比如资产通证的商城积分、购物券体系等，其中的根本原因是其中心化的体系包含很多的应用痛点[19]。

中心化的业务模式、数据流转方式、技术架构、交易模式等都是阻碍通证发展的应用痛点，分析如下。

（1）中心化的业务体系妨碍了通证体系的建设。不管哪种通证模式，其本质上都是想吸引大量用户参与建设通证体系。在大量用户的基础上才能满足通证的业务体系质量，进而确保通证在体系中的流通效率。然而，中心化的业务体系却一直得不到客户的信任，海量用户的参与也只能凭空想象，这就导致通证生态体系的构建过程非常缓慢。

（2）中心化的数据流转方式传统的通证体系下采用传统数据库进行管理，在中心化的数据模式下可对数据进行任意的修改，这导致数据可信度低，企业间难以互信，很难形成一个统一的通证平台体系。

（3）中心化的技术架构，限制了通证体系的发展。在传统的中心化技术架构下，很难使平台间信息流通顺畅，不同体系、领域、模式下都有确实相关的重要数据，信息保护的思想在各企业间横行，这导致各体系自建中心化体系，各企业都拥有一套技术架构，要实现流通相当于一个人开通所有体系模式，一个平台与成千上万的其他平台逐个建立连接，实现信息流通难上加难，另外每个平台的构建、运行、维护、优化都是一笔巨大的投资，这更让企业退一步[20]。

（4）中心化的交易方式，降低了通证的流通效率。在传统的中心化交易方式下，通证只能在用户和商家（C2B）、商家和平台（B2B）之间流通，传统通证体系平台很难实现用户之间（C2C）关于通证的直接交易、流通，这就导致通证的流通效率大大受限，无法实现大众化消费。

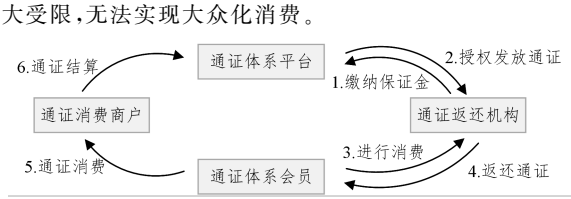

图 3 通证体系交易模式

Fig. 3 Token trading patterns

4 基于区块链技术的通证链的设计

中心化的通证体系存在着诸多不足，探究去中心化的体系模式尤为重要。区块链技术的大规模应用是去中心化通证体系的突破口，基于区块链技术的通证体系由此而来，如图 4 所示。

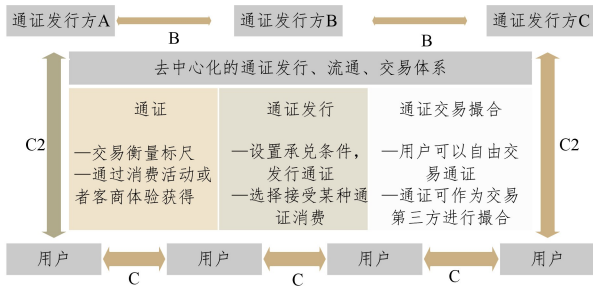

图 4 基于区块链的通证体系图

Fig. 4 Token system diagram based on blockchain

传统通证模式下，一般通证如商城积分，其主要用于提升客户忠诚度，增加客户粘性。行业大企业（简称大 B）一般采用图 3 所示的业务模式，大 B 运行通证体系平台，其他中小型企业运行通证返还平台，比如银行、电信等。在这种模式下，通证是一种工具，并不能变成一种商业运行模式。在这种发展有限的小众模式下，其发展一批中小商户形成联盟，用户能够用积分换礼品或者中小型的商品，以刺激一定的消费，中小商户可以凭借积分向大 B 通证平台进行兑现[21]。

运用区块链技术的通证链模式如图 5 所示，通证可以作为交易媒介实现 C2C，B2B，C2B（C 是 Client 代表客户端用户，B 是 Business 代表商家、服务方）的连通。无论是 B 端还是 C 端，亦或是 B 端、C 端的企业、用户在应用了去中心化技术的通证链之后实现通证的流通，解决了中心化模式下的诸多痛点。

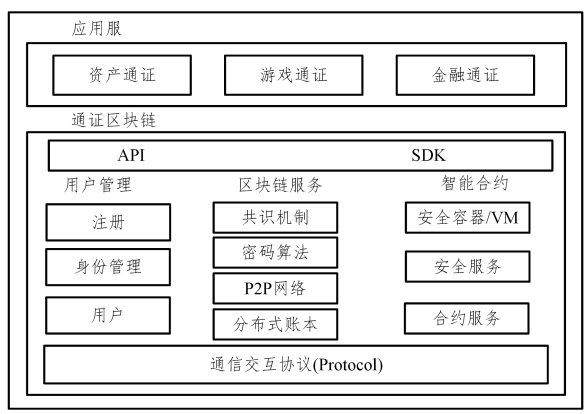

图 5 通证区块链模式图

Fig. 5 Token blockchain pattern diagram

区块链技术最早应用在比特币系统中，近年来在金融、知识产权、数据存储、电子存证、新能源等领域也越发引起广泛关注[22]，究其原因有如下几点。1）区块链具有去中心化的特征，其不会将参与交易的任意一方作为中心。相对于中心化体系，去中心化可以提升效率并降低成本，例如物流体系，在物流供应链中，各环节的确认及交易模式复杂，运用区块链技术可直接增加企业的利润，降低成本。2）区块链具有不可篡改的特征，如果有人修改了一个区块，那么后面所有的区块都必须修改，除非有人掌握了全网 51% 以上的计算能力，否则

同时修改多个区块几乎不可能发生。通过这种联动机制，区块链保证了自身的可靠性，数据一旦写入，就无法被篡改。3)区块链具有去信任的特征，假定参与交易的任何一方都在不可信网络环境下，我们运用了区块链技术，通过查询交易的信息，做到不可抵赖，使各方都遵守诚信[23-25]。通证区块链模式如图 5 所示。

4.1 通证链应用服务设计

通证区块链的设计将实现各行业、各领域(游戏通证、金融通证、资产通证)的通证流通，打通各企业的壁垒。通证区块链上发行通证币(Token Coin，TKC)，它将实现一个去中心化的价值流通媒介，如图 6 所示，各类通证都可以通过 TKC 实现 B2B，B2C，C2C 的价值流转，真正打通企业壁垒，实现行业流通。TKC 将作为应用层提供应用层服务，它可以作为上层应用与底层的区块链平台进行交互，其作为流通媒介将有广阔的市场应用前景。

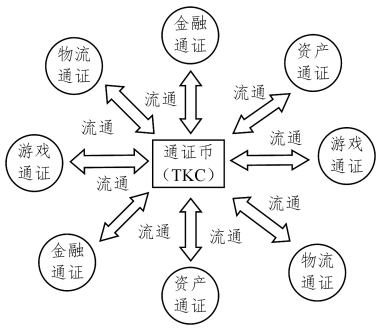

图 6 通证流通图

Fig. 6 Token circulation diagram

4.2 通证区块链设计

为了增加企业信息信任度，促成行业间的通证流通，通证区块链充分考虑了通证体系下的技术壁垒，本文将通证链结合区块链技术进行创新性设计以实现去中心化体系。通证链的创新性设计如下。

(1)共识机制设计

通证区块链的共识机制采用安全、高效的通证共识算法(Token Consensus Algorithm，TCA)，共识分为两部分，交易数据的收集及处理，过程如下：

1)节点在共识开始时收集交易，并将交易放到内存候选集；

2)节点分为共识节点与非共识节点，共识节点专门对交易进行合法投票，每个共识节点维护一组共识节点集(类似董事会)

3)共识节点集对交易进行投票，达到一定“赞同”票的交易得到确认并被放入内存，未达到票数的交易将被放弃或进入下一轮共识候选；

4)最终，所有“赞成”票超过一定阈值(一般为 80%)的交易将会被放入交易集中；

5)形成交易集后将相关信息进行 Hash 计算得到 Hash 值，随后将区块哈希进行广播；

6)节点收集共识节点集内广播过来的区块哈希值，结合自己生成的区块哈希，对节点集内的节点计算的区块哈希计算一个比例，如果某一 Hash 值的比例超过一个阈值(一般为 80%)，则认为这个 Hash 值是共识通过的区块哈希，该 Hash 值将被作为区块标志将写入区块链；

7)如果上面没有对某一区块哈希超过设定的阈值，那么将对该区块进行重新投票，直到满足条件。

至此，通证链的区块共识过程结束，开启下一轮共识。

(2)公有链类型设计

前文已经分析了通证体系在中心化体系下存在诸多局限，实现基于区块链体系的去中心化系统显得尤为重要，但如果仅是去中心化的区块链系统还不够，还必须保证该系统是公有链的设计。表 1 对区块链类型进行分析，通证体系必须保证所有数据都是公开、透明的，任何人都能随时对数据进行查询访问，这是联盟链和私有链不能提供的，因此，通证区块链必须是公有链类型，这样才能满足商用通证体系的要求，如比特币、以太坊等公有链，用户能够通过区块链浏览器等相关工具进行区块查询，确认交易是真实有效的。

表 1 区块链类型对比

Table 1 Comparison of blockchain type

类型性能	公有链	联盟链	私有链
中心化程度	去中心化	多中心化	相对中心化
参与方	任何人	特征成员	指定成员
记账者	任意参与者	参与者协商	内部决定
优点	完全解决信任问题	可进行权限控制	速度快，能耗低，
缺点	交易量受限，存在资源浪费	节点有区分，无法解决信任问题	节点数量受限，类中心化

(3)可插拔的密码学算法设计

研究表明，商用密码与国际密码算法在区块链系统中都得到了很好的应用。在商用密码方面，很多企业出于商用安全的层面考虑选择使用国内自主研发的商用密码系列，如 SM 算法系列，其中布比区块链已实现 SM 系列加密算法，华为、腾讯等也在积极响应。在国际密码的使用方面，大多选用 SHA 系列的加密算法，究其原委，SHA 系列如 SHA-256 已经是比较成熟的安全算法，其摘要值长，采用蛮力破解法破解困难。

不管是商用密码还是国际密码，都各有千秋。如果能够结合两者优势，在不同应用领域灵活选用不同算法，这将为开发者和使用者带来诸多便利。可插拔的密码学算法设计就是基于这样的目的，通过配置文件的灵活选用，实现开发者在不同应用选用不同加密算法的目标。

5 基于区块链技术的通证链的分析

5.1 区块链通证分析

通证链使用区块链及相关服务作为技术底层，运用密码学及通信协议达到数据不可篡改的目的，基于区块链技术实现通证链系统。通证链致力于通证领域的区块链应用，在区块链技术飞速发展的今天，通证链的实现将具备如下特征。

(1)通证资产安全：通证链上的数据将永久记录，不可篡改，保证各方安全的同时可以做到随时随地快速查证；

(2)通证管理多样：管理节点随时掌握流通现状，通证全程追溯，职责明确，共识节点将负责进行交易的确认，非共识节点可以轻量化存储以进行交易；

(3)通兑机制：通证区块链将以区块链技术为底层实现 C2C，C2B，B2B 的跨领域资产互通。

TKC 可作为类似“法定货币”属性的法定通证，其作用是作为其它各行业、领域内通证的价值衡量标杆，通过金融学原理对各领域的通证进行价值锚定。以积分为例，假设有京东、天猫、美团、苏宁等企业的通证，其通兑 TKC 的汇率如表 2 所列，流通图如图 7 所示。

表 2 TKC 通兑汇率表

Table 2 TKC exchange rate table

通兑类型	通兑单位	通兑比例
京东通证/TKC	100	1∶2
天猫通证/TKC	100	1∶3
美团通证/TKC	100	1∶4
苏宁通证/TKC	100	1∶5

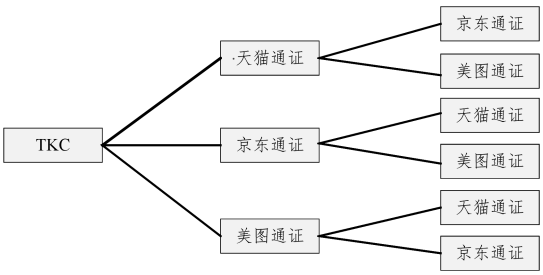

图 7 TKC 价值流通图

Fig. 7 TKC value circulation diagram

综上分析可知，在运用区块链技术解决信任问题的基础上，通证链上流通的 TKC 是一个巧妙的设计，是打通行业壁垒的关键。与传统通证模型相比，这是一个基于区块链技术安全、透明、不可篡改的特点，受各方信任的体系。每种通证和 TKC 之间将存在汇率关系，无论是企业内部流行的通证，还是不同企业间的通证，亦或是企业与客户间的通证都可以通过 TKC 实现价值锚定，以达到不同体系的流通。

运用区块链技术的通证链将确保数据的绝对安全，拥有多项优势。数据的不可篡改将提升企业间的信任度，增加通证链的应用率，降低开发及维护成本，这将打破传统模式下，各企业独自开发、维护、运行的的高成本状态，促使一个受各方信任的统一平台运用。

通证链上的通证(TKC)将带来众多利好：1)通证链上的通证 TKC 是打通行业壁垒的关键，根据市场规律，其内部运行着一套汇率法则，实现 TKC 与各领域通证连接；2)基于区块链技术的通证链具有去中心化、不可篡改等特点，以此可提高企业信任度，解决商业互信问题；3)通证链的使用可减少企业开发，维护成本。

5.2 通证链设计分析

研究表明，在共识机制上，POW 的实现非常依赖计算机的运算能力，因此，算力资源的消耗是非常严重的。另外，大多数的公链交易性能上也不太客观，在区块链的数据结构设计上，其大小只有 1MB，设定每十分钟产生一个块，这决定了比特币平均交易吞吐量仅为 7TPS，面对呈现指数级增长的交易量显然不够。虽然以太坊在此基础上进行了优化，对区块大小及出块时间都进行了改进，但交易吞吐量最高也只有 25TPS 左右，这对百万级别的用户显然是不够。

POS 是股权制的共识机制，拥有的股权越多，区块记账能力越大，虽然在一定程度上可以缓解交易吞吐，但非常容易造成分叉。DPOS 是采用超级节点(拥有记账权利的少数节点)共识的算法，但超级节点的概念本身就类中心化。

通证链的设计如表 3 所列，通证链采用的 TCA 共识算法，不需要复杂的算力计算，不会浪费资源，交易由共识候选集投票确认，只有得到认同(票数达到阈值)交易的区块才会被广播，不存在分叉问题，每个节点维护一份共识节点集名单，每个节点的共识节点集不同，任何节点都能成为共识节点，环环相扣，相互监督，是一个去中心化的共识体系。

表 3 通证链设计分析

Table 3 Design and analysis of token chain

区块链底层	链类型	共识机制	数据库	加密系统
比特币	公有链	POW	LevelDB	SHA
以太坊	公有链	POW/POS	LevelDB	SHA
Fabric	联盟链	Solo/Kafka/PBFT	LevelDB/CouchDB	SHA
通证体系	私有链	中心化数据库	常用关系型数据库	SHA/SM
通证链	公有链	TCA	可插拔	可插拔

通证链在链的类型、组件、共识上的设计将解决诸多痛点：1)公有链的设计将解决信任问题，打通行业壁垒，针对存在的安全、效率问题，结合共识、密码学、数据库的设计等方面进行优化处理；

2)可插拔的组件设计将简化流程，提高开发速度，为开发者提供敏捷的开发效果，为应用者提供适合自身商用体系的组件开发；

3)在共识机制的设计上，普通公链都存在算力浪费、交易拥堵，容易分叉等问题，对此，本文提出采用 TCA 算法设计，交易的确认通过共识节点进行投票处理，达到秒级处理，不存在算力的浪费，其独有的共识设计将解决上诉问题。

5.3 通证链性能分析

通证链的节点分为共识节点与非共识节点，这样的分类将增强 C 端客户体验，缓解节点存储压力。公链体系中，节点的加入首先面临历史账本的同步，即下载区块链数据，完整的数据至少 100 多 GB，随着时间的推移，节点的存储压力越来越大，以比特币为例，目前完整账本 200 多 GB，且还在不断加大，以太坊类似。通证链的账本由共识节点维护，普通用户作为非共识节点存在一个指向完整账目的快照，它只需下载部分近期的历史账目，无需下载完整账本，这将使用户便利化，更能增加用户的体验感及降低用户使用门槛。

通证链在组件(数据库、密码学算法、共识机制等)设计上采用可插拔的模式，可灵活地对相关组件进行优化调节。通证区块链的可扩展性强，节点数可扩展到百万级别，这是联盟链所不能比拟的，通证链交易秒级确认，相比于公有链的小时级确认或分钟级确认有显著提高。通证区块链性能对比如表 4 所列。

表 4 通证区块链性能对比表

Table 4 Performance comparison of token blockchain

区块链底层	存储空间	交易效率	可扩展性	灵活性	资源是否浪费
比特币	大	低	强	好	是
以太坊	大	低	较强	较好	是
Fabric	大	高	较弱	较差	是
通证体系	小	高	一般	一般	是
通证链	C 端小	高	强	好	否

通证链的各类创新性设计，使其在存储、效率、扩展性和灵活性等方面都有质的提升。

(1)在存储空间上，通证链的普通用户只是存空间，相对于目前众多公链少则 200GB 并还在不断增长的存储空间，是指数级的提升，相应地还增强了用户体验感，降低用户使用门槛；储近期的账本记录，存储量只需要个位数 GB 的。

(2)在交易效率上，绝大多数公链的交易都停留在 10～100 TPS，这在性能上是非常大的缺陷，通证链的设计使其能将交易处理量提升到 1 000 TPS，这解决了大用户需求，为未

来大数据量的系统应用奠定基础。

(3)高效的共识处理结合系统的模块化设计,通证链的使用对资源要求不高,不存在算力挖矿,更不存在对显卡、CPU的要求,普通硬件即可进行开发、使用。

(4)可插拔的第三方组件使通证链的使用灵活多变,不仅可使用商用密码、国际密码套件,也支持自身开发的密码学套件,前文基于纠错码的 Hash 函数的设计也将在其中得到充分利用,其满足绝大多数商业场景的灵活切换,在节点的扩展性上,对客户端可做到大数据量的处理,节点可扩展性强。

结束语 区块链技术被认为是继互联网之后的又一次重大革命。目前,金融、物流、医疗、新能源都有区块链的应用案例,随着区块链技术的不断发展,越来越多的应用将会利用到该技术。无论是技术创新还是模式创新的终极目标都是去中心化的组织形态,区块链技术首当其冲。信息技术创新是以提高效率、产能为核心方向的,但中心化模式一直是横在面前的难题,新一轮技术创新的方向将彻底解决这一问题,为社会带来跨越式的进步。

区块链的去中心化、安全、透明、不可篡改的特性可以很好地解决传统通证模型的痛点。本文系统地梳理了区块链底层技术架构,并分析了传统通证体系的壁垒,设计了结合区块链技术实现的通证区块链系统。此外,结合目前众多公有链系统的问题,文中提出了满足应用场景的共识机制,使通证链在效率和安全方面有显著提升,最后对通证链及部分公有链、私有链进行对比分析发现,其在存储、可扩展性、灵活性等方面有明显优势。结合以上分析可以看出该通证模型在未来市场的潜力。

参 考 文 献

[1] NAKAMOTO S. Bitcoin:a peer-to-peer electronic cashsystem [OL]. http://bitcoins.info/bitcoin.pdf,2018.

[2] BUTERIN V. A next-generation smart contract and decentralizedApplication platform[J]. White paper,2014:1-36.

[3] Ethereum Whitepaper[OL]. http://github.com/Ethereum/wiki/White-Paper.

[4] Hyperledger white paperwg[OL]. http://wiki.hyperledger.org/groups/Whitepaper/whitepaper.wg.

[5] SWAN M. Blockchian:Bluprint for a New Economy[M]. O'Reilly Media,Inc,2015.

[6] ANTONOPOULOS A M. Mastering Bitcoin:Unlocking Digital Crypto-Currencies[M]. O'Reilly Media,Inc,2014.

[7] YUAN Y,WANG F Y. Blockchain:the state of the art and future trends[J]. Acta Automatica Sinica,2016,42(4):481-494.

[8] YU M,LI Z H,ZHANG L B. P2P data management[J]. Journal of Software,2006,17(8):1717-1730.

[9] GRIBBLE S D,HALEVY A Y,IVES Z G,et al. What can database do for peer-to-peer? [C]// Proceedings of the Fourth International Workshop on the Web and Databases (WebDB). Santa Barbara,USA,2001:31-36.

[10] HE P U,YU G E,ZHANG Y F,et al. Survey on blockchain technology and its application prospect[J]. Computer Science,2017,44(4):1-7.

[11] JAKOBSSON M,JUELS A. Proofs of work and bread pudding protocols (extended abstract)[M]// Secure Information Networks. Boston,MA,Germany:Springer,1999:258-272.

[12] Proof of stake[OL]. https://en.bitcoin.it/wiki/Proof_of_Stake, April 11,2018.

[13] CASTRO M,LISKOV B. Practical Byzantine fault tolerance [C]// Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans,USA:USENIX Association,1999.

[14] WU G F,ZENG X W,LIU J,et al. Design and Analysis of Hash Function Based on Error Correcting Code[J]. Netinfo Security,2018(1):67-72.

[15] Bit Shares. Delegated proof of stake[OL]. http://docs.bitshares.org/bitshar-es/dpos.html.

[16] SHENTU Qing-Chun. Development guide of blockchain[M]. Beijing:China Machine Press,2017.

[17] YANG B H,CHEN C. Principle,programming and applications of blockchain[M]. Beijing:China Machine Press,2017.

[18] GOLDWASSER S,MICALI S,RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing,1989,18(1):186-208.

[19] QIAN W N,SHAO Q F,ZHU Y C,et al. Research problems and methods in blockchain and trusted data management[J]. Journal of Software,2018,29(1):150-159.

[20] GREEN T J,TANNEN V. The semiring framework for database provenance[C]// Proceedings of the 36th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems (PODS). Chicago,USA,2017:93-99

[21] LIANG X P,SHETTY S,TOSH D K,et al. ProvChain:A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability[C]// Proc. of the CCGrid. 2017:468-477.

[22] DWYER G P. The economics of bitcoin and similar private digitalcurrencies[J]. Social Science ElectronicPublishing,2015,17:81-91.

[23] SCHAUB A,BAZIN R,HASAN O,et al. A trustless privacy-preserving reputation system[C]// Proc. of the IFIP Int'l Information Security and Privacy Conf. Springer Int'l Publishing,2016:398-411.

[24] YANG Z,ZHENG K,YANG K,et al. A blockchain-based reputation system for data credibility assessment in vehicular networks[C]// Proc. of the IEEE Int'l Symp. on Personal,Indoor,and Mobile Radio Communications. 2017:1-5.

[25] DENNIS R,OWEN G. Rep on the block:A next generation reputation system based on the blockchain[C]// Internet Technology and Secured Transactions. 2016:131-138.

WU Guang-fu, born in 1977, Ph.D, associate professor, master supervisor. His main research interests information theory and channel coding, cryptography, network Security and blockchain technology.