计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191000057

区块链新技术综述:图型区块链和分区型区块链

张长贵　张岩峰　李晓华　聂铁铮　于　戈
东北大学计算机科学与工程学院　沈阳 110169
(741454897@qq.com)

摘　要　区块链是一种创新性分布式账本技术,在金融、征信、审计等众多重要领域具有广泛的应用前景。但是,现有的基于比特币风格的分布式账本系统在可伸缩性、吞吐率、交易确认延迟等方面遇到了提升瓶颈。为此,业界提出了基于有向无环图(Directed Acyclic Graph,DAG)结构和基于分区(Sharding)的两种新型区块链技术,它们通过改变系统的数据结构和存储结构来弥补区块链的原生缺陷,从而得到更高的伸缩性和更大的吞吐量。文中综述了典型的DAG型区块链系统(如NXT,Byteball等)和分区型区块链系统(Elastico,RapidChain等),分别介绍了这两种新型区块链技术的发展现状,详细分析了系统模型、数据结构以及共识机制等关键技术,总结和比较了现有各类区块链技术的特点,指出了有待解决的技术挑战与未来的研究方向。

关键词:分布式账本;区块链;DAG型区块链;分区型区块链;共识机制
中图法分类号　TP315

Survey of New Blockchain Techniques:DAG Based Blockchain and Sharding Based Blockchain

ZHANG Chang-gui,ZHANG Yan-feng,LI Xiao-hua,NIE Tie-zheng and YU Ge
School of Computer Science and Engineering,Northeastern University,Shenyang 110169,China

Abstract　Blockchain is an innovative distributed ledger technology with wide application prospects in many important fields such as finance,credit reporting and auditing. However,the existing bitcoin-style distributed ledger systems have already encountered bottlenecks in terms of scalability,throughput,and transaction confirmation latency. To address these problems,researchers have proposed two new blockchain techniques. One is based on Directed Acyclic Graph(DAG) structure,and the other one is based on Shardind. They employ new data structure and new storage structure to overcome the native limitations and get better scalability and higher throughput. This paper reviews the state-of-the-art DAG-based blockchain systems (e.g. NXT,Byteball,etc) and sharding-based blockchain systems (e.g. ,Elastico,RapidChain,etc). It analyzes the key components of these systems,including system storage structures,data structures,and consensus protocols. It also compares these blockchain techniques,and summarizes the challenges and future research directions.

Keywords　Distributed ledger,Blockchain,Directed acyclic graph blockchain,Sharding-based blockchain,Consensus mechanism

1　引言

2008年中本聪发表了比特币白皮书,介绍了世界上第一个分布式加密货币——比特币[1]。比特币由于其核心技术——区块链具有数据持久化、防篡改、防抵赖、可靠性高以及去中心化等特点,在金融、征信、审计等众多重要领域具有广泛的应用前景,引起了国内外学者广泛的重视。近年来,基于区块链的分布式记账系统及应用层出不穷,如从最初的比特币[1]系统到支持智能合约的以太坊[2-3]以及Hyperledger超级账本[4]等。

区块链系统由数据层、网络层、共识层、激励层、合约层、应用层组成[5]。其中,数据层包含交易数据和加密技术等;网络层包含消息转发和传播机制,区块链采用P2P网络模型;共识层包含各种共识机制,大多数区块链系统都基于工作量证明PoW共识机制;激励层则决定了系统中货币的发行机制与分配机制;合约层可以运行智能合约,支持上层应用的开发;应用层开发可视化界面,并与合约层连接,进而实现用户与区块链的交互。

尽管区块链系统被广泛研究和开发,它始终没能得到大规模应用。一个主要的原因是,目前大多数的区块链系统不

到稿日期:2019-10-11　返修日期:2020-03-23　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61672141,61672142,61991404,U1811261),中央高校基本科研业务费(N171606005,N181605017,N181604016),辽宁省科学技术基金(20180550321)
This work was supported by the National Natural Science Foundation of China(61672141,61672142,61991404,U1811261),Fundamental Research Funds for the Central Universities (N171606005,N181605017,N181604016) and Science and Technology Foundation of Liaoning Province,China(20180550321).
通信作者:于戈(yuge@mail.neu.edu.cn)

能提供高吞吐率以及高可伸缩性来满足当前的大数据量或大交易量的处理需求[6-7]。以比特币为例，中本聪风格的区块链有以下 4 个显著的缺点：

(1)可伸缩性差。随着系统中的节点数量不断增加，系统的吞吐率和存储容量无法提高。

(2)吞吐率低。比特币系统平均每秒处理的交易数量是 7 笔[6]。

(3)确认延迟高。由于比特币区块产生速度为 10 min/个，确认延迟至少 10 min，而且由于分叉现象，一般认为 60 min 后才可以认为交易被确认[8]。

(4)高能耗。由于 PoW 机制，节点需要通过挖矿来争取记账权，因此会消耗大量的电力资源。据估计，比特币挖矿每年消耗数十太瓦时电量，足够一个中型国家全年的耗电量[9-10]。

因此，为了使区块链能满足实际应用需求，必须解决以上问题，尤其需要提高区块链系统的可伸缩性和吞吐率。针对这些问题，近年来涌现出了两大类解决方案，一种是基于有向无环图(Directed Acyclic Graph，DAG)的方法，将单链结构变成图结构；另一种是基于分区(Sharding)的方法，将单链分布存储变成多链分布存储。为叙述方便，本文将传统的单链区块链称为比特币区块链，将新的两种区块链分别称为图型区块链和分区型区块链；将区块链系统中的计算单位(如计算机)简称为节点，将存储单位(如区块)简称为单元。

本文第 2 节和第 3 节从发展现状、系统模型、数据结构和共识机制等方面分别介绍了近年来学者提出的 DAG 图型区块链技术和分区型区块链技术；第 4 节对比并分析了 3 种区块链的性能；最后总结全文并展望未来。

2 图型区块链

图型区块链主要改进了比特币区块链的数据层和共识层，如图 1 所示。本节首先介绍图型区块链的发展现状，然后介绍图型区块链在数据层的改进，最后阐述图型区块链在共识层上的改进，并介绍了 NXT，Byteball，DagCoin，Nano 和 IOTA 等代表性系统的共识机制。

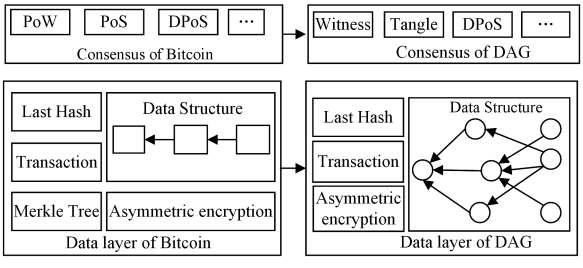


图 1 DAG 图型区块链与比特币区块链的区别

Fig. 1 Difference between DAG-Based blockchain and Bitcoin blockchian

2.1 系统概述

有向无环图是一个有向的、具有拓扑顺序的图数据结构，作为一种计算机领域常用的数据结构，因其独特的拓扑结构的优越性，常被应用于动态规划、寻求最短路径、数据压缩等算法[11]。同样，DAG 的拓扑结构也可以适用于分布式账本技术，因为分布式账本技术要求交易保持全局有序，该结构适合保存有序的交易信息。相比比特币区块链，图型区块链在数据层和共识层进行了创新。

2013 年 9 月，NXT 社区中有用户提出以 DAG 图作为区块链的底层数据结构来提高系统整体性能，将比特币区块链系统中的链式存储结构改成 DAG 图存储，即区块 DAG[12]。DAG 图中存储粗粒度的区块。2014 年 12 月出现了第一个细粒度区块的图型区块链系统 RaiBlocks[13]，每笔交易作为单独的存储单元，或者说，一个细粒度区块中只包含一笔交易。Byteball[14]是另一个细粒度区块的分布式账本系统，它采用最短路径最优父节点算法，选出一条全网共识的主链。DAGCoin[15]虽然提出较早，但是并没有代码实现，直到 Byteball 出现。它在 Byteball 的基础上进行修改，让每一笔交易都直接参与维护全网的交易顺序。这样，图型区块链进一步演变成了完全抛弃比特币区块链的一种解决方案，当交易发起后，直接广播全网，无需打包区块，从而提高处理速度。

2016 年 7 月推出了 IOTA 系统[16]，IOTA 中既没有打包过程，也不需要挖矿和矿工，还免去了交易费，提高了整个网络的吞吐量。另一个备受关注的图型区块链系统是 Nano(由 Raiblocks 更名而来)，其采用了一个用户一条链的方式，只记录自己的交易，不与其他帐户共享数据，从而使所有的交易都可以并行执行，能够提供秒级的交易确认速度和无限可伸缩性。

2.2 系统模型

图型区块链沿用比特币区块链的 P2P 网络结构来组织全网节点，P2P 网络的特点是网络中的每个节点都是对等的地位且互相连接，不需要类似于 C/S 架构中的中心化服务器，也不需要特殊层级的节点，这保证了区块链系统的自治性、开放性和公平性，每个节点都承担着验证数据区块、保存数据区块、转发消息等任务。

比特币区块链上，新发布的区块会加入到最长链之上，当发生分叉时，所有节点都以最长的链为准，依次无限延伸。而 DAG 中一个网络节点要发起一笔新的交易时，需要在网络中找两笔(或更多)其他交易去验证，并将自己新发起的交易指向这两笔交易，整个网络就是这样一点一点扩大的。正因为这样的设计，整个网络中验证交易的责任从传统的矿工转移到了网络的每个节点，这样的设计促使网络中的每个节点都积极地参与验证其他交易。

2.3 数据结构

比特币区块链将粗粒度的区块连接在一起，形成不可篡改的链条，而 DAG 图型区块链采用了以每笔交易为基本存储单位和处理单位的方式，相当于细粒度的区块。在执行过程中，由每笔交易对它之前的两笔或以上交易进行验证。如图 2 所示，DAG 区块链中每个节点只保存一笔交易和该单元验证过的单元哈希值，单元 U1 被 U2a 和 U2b 两个单元所验证，单元 U2a 被单元 U3a，U3b 和 U5a 所验证。当用户向区块链中添加数据时，所在网络节点创建一个新的存储单元并将其广播给其他节点，每个单元中必须包含一个或多个先前单元的哈希值(与本单元直接相连的单元称为父单元)，这样做的目的是使得各单元之间有序，如果尝试修改其中一个单

元，则必须改变它所有的子孙单元，如此就保证了数据的防篡改性。如果沿着父子链的历史单元前进，当同一个单元被多个后来的单元引用时，会观察到很多分叉，当同一个单元引用多个较早单元时，会出现融合，最终形成一个有向无环图(DAG)结构。

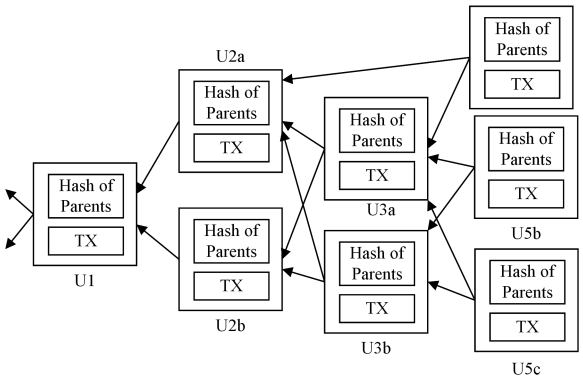


图 2 DAG 区块链的数据结构

Fig. 2 Data structure of DAG blockchain

2.4 共识机制

DAG 图型区块链采用的共识机制分为 PoS，Witness，DPoS，Tangle 4 种，下文将分别进行介绍。

(1)基于权益证明(PoS)

基于权益证明最初由 PeerCoin[17] 区块链系统所采用，该方法与要求证明人执行一定量的计算工作不同，权益证明要求证明人提供一定数量加密货币的所有权即可，权益证明机制根据每个节点拥有数字货币的比例和时间，等比例地降低节点的挖矿难度，从而加快寻找随机数的速度。这种共识机制可以缩短达成共识所需的时间，但本质上仍然需要网络中的节点进行挖矿运算。值得一提的是，以太坊目前虽然采用 PoW 共识机制，但是其创始人 Buterin 提出，以太坊会经过一个过渡期 PoW+PoS(Casper 协议)，然后将共识机制转变为 PoS，目的是提高网络效率[18]。由此可见，PoS 相比 PoW 更适合实际应用。

(2)见证人机制(Witness)

见证人机制是 Byteball 区块链中提出的共识机制，它根据规则选取主链从而决定交易的全局顺序，见证人(Witeness)是系统中长期实名并且声誉较高的组织或者个人，他们是参与系统维护并自愿频繁发起交易单元的节点[19]，对于消极工作甚至作弊的见证人，可以经过用户投票更换。

在 Byteball 中，从任何一个顶端单元出发到达创世单元的最优路径称为候选主链(Candidate Mainchain)。最优路径通过选择最优父单元产生，全部节点运行相同的选取最优父单元算法，递归地选出主链。

单元级别是由当前单元出发至创世单元的最长路径长度。见证级别是：从当前单元的最优父单元开始沿主链回溯，并对路径中各个见证人进行计数(相同见证人只计数 1 次)，见证人数达到足够多(超过总数的 1/2)时停止回溯；然后计算停止位置的单元级别，将其作为当前单元的见证级别。

不同的候选主链会在某个单元位置交叉(最差的情况是在创世单元交叉)，该交叉点称为稳定点(Stable Point)。对于所有候选主链，从稳定点到创世单元的路径完全相同，该路径称为稳定主链(Stable Mainchain)，如图 3 所示。稳定主链是一条确定的路径，根据这条路径，与之相关的所有单元均可以在此基础上进行排序，其序号称为主链号(Main Chain Index，MCI)。创世单元的 MCI 为 0，依次加 1 直到链尾。对于不在主链上的单元，其 MCI 与其最近父单元的 MCI 相同。MCI 代表了从主链视角来看单元在 DAG 中的总序，总序使得全网达成共识。DagCoin 是建立在 Byteball 上层的区块链，因此它的共识机制和 Byteball 相同。

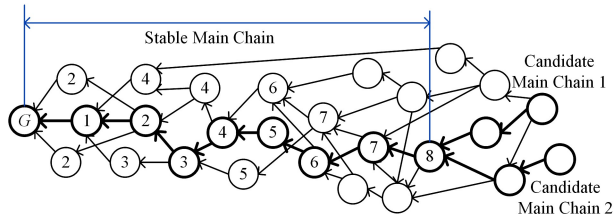


图 3 稳定主链和稳定点的形成过程[14]

Fig. 3 Formation of stable main chain and point[14]

(3)基于代理权益证明(DPoS)

该方法是对权益证明的改进，Nano 项目采用了 DPoS 共识机制，DPoS 的方法由 EOS 系统创始人提出[20]，即每位持币人都有权投票选出代理节点，持币量少的人也能参与投票。在 Nano 中每个节点基于持有的 XRB(Nano 中的流通货币)数量来选取代表，拥有的 XRB 越多，所选的代表权重就越高，最终全网会产生若干个权重较高的代表来验证交易，并维护网络运行。为了使一笔交易生效，节点必须发送交易到验证器节点，即所选取的高权重代表。由该节点验证交易，然后将其广播到与其连接的其他验证器节点。每个后续验证器节点都会执行相同的验证和传递过程，直到交易传遍整个网络。

(4)缠结(Tangle)

Tangle 是 IOTA 系统采用的共识机制，它是一个有向无环图(DAG)数据结构。随着越来越多的交易被添加到缠结中，一个“权重”被添加到附属的祖先交易中。当交易有足够大的权重时，交易将显示“确认”状态。理论上，如果整个网络中有足够多的交易流，则这个确认过程可以快到在几秒钟内完成。该共识机制的创新之处在于不再采用网络中的一个子集(如矿工)来专门负责维护共识，而是全网所有的参与者都来进行网络交易的验证工作。IOTA 中共识机制与交易过程是一体的，共识机制在运行的同时处理交易，IOTA 系统可以在没有任何交易费用的情况下进行扩展。

3 分区型区块链

分区型区块链主要在系统模型和共识层对区块链进行改进，每个区块中的数据结构几乎与比特币相同，因此其可以参考比特币的数据结构。本节首先介绍分区区块链系统，然后介绍分区区块链的系统模型和数据结构，最后介绍分区区块链中的共识机制。

3.1 系统概述

数据库中拓展存储容量和进行并行处理的一个有效方法是分片技术，其目的是将庞大的数据集划分成多个子数据集，

并分别存储到不同的节点上，使得不同节点上的交易可以被并行处理。对于区块链系统，分区机制通过将全网节点划分成不同的集合，来划分系统的通信资源、计算资源、存储资源，使每个集合独立并行地运行，从而提高区块链系统的吞吐率和可伸缩性。

目前，已有许多基于分区的区块链的解决方案，最初提出将分区技术应用于公有链的是 Elastico 系统[21]，该系统将区块链网络划分成了多个组，每个组处理互不相交的交易数据，在每个组中独立运行 PBFT 共识机制，然而 PBFT 协议需要极高的网络带宽，且在可任意加入的公有链系统中容易遭受女巫攻击(Sybil attack)[22]。因此，Elastico 系统设计了基于 PoW 的准入机制，防止女巫攻击。分区的方法虽然提高了吞吐率和可伸缩性，但是并没有解决跨区域的交易产生的事务原子性问题。

在此基础上，研究者提出了 Zilliqa 系统[23]和 OmniLedger 系统[24]。它们在事务的原子性问题上对 Elastico 系统进行了改进，其中 OmniLedger 系统在跨区交易过程中加入了两段封锁提交协议，保证了跨区事务的原子性，并使用了称为 ByzCoinX 的共识机制，它是由 ByzCoin[25]改进而来的。随后 RapidChain 系统[26]被提出，它将 PBFT 与纠错偏码(erasure-code)相结合，减小了 PBFT 带来的巨大通信量，但是它对网络带宽仍有较高的要求。Monoxide[27]是一种沿用 PoW 共识机制的分区方案，它提出了诸葛连弩挖矿(Chu-ko-numining)算法，解决了 PoW 共识机制在分区后算力被稀释，从而导致对单区域恶意攻击的难度降低的问题，也通过最终一致性原则解决了跨区域交易事务的原子性问题。

分区型区块链在数据层几乎与比特币相同，但是它改变了网络结构，采用了多层的 P2P 网络，并且对消息转发的方法也进行了优化。部分分区型区块链在共识层采用 PBFT 类型的共识机制，而 Monoxide 在解决了算力稀释问题的情况下，仍然采用 PoW 共识机制。

3.2 系统模型

区块链是一种线性的单链结构，单链结构并发度低。分区的方法将全网的节点分成了若干组，每个分组相当于一个相对独立的区块链系统，每个组中有若干个节点。所有的区块数据也被划分到多个组中，每一组只保存和本分组相关联的区块数据，但是这些数据组合起来仍然是一个完整的账本数据，多条分区链尽管在物理上是分区存储的，但是它们在逻辑上组成了全局链。如果全网包含 n 个分组，区块数据被分成 n 份分别保存在各组中，则全网所有节点的存储开销缩小为原来的 $1/n$。同时，在需要处理的交易数量一定的情况下，由于每组可以分别处理交易，使得系统吞吐量变为原来的 n 倍，在不考虑跨区域交易的情况下，通信量也会随着分组而减少为原来的 $1/n$，系统的伸缩性也得到了提升，因为随着分组的增多，系统整体的处理能力在理论上也会呈线性增长。

如图 4 所示，在一个由 8 个节点组成的网络中，每 4 个节点组成一个分组，各组内组成 P2P 网络，各组之间可以互相通信，这样组成一个两层的 P2P 网络。一个完整的区块链数据被分割为 2 份，每个分组保存其中的一部分。而各个分组内的 P2P 网络节点保存着相同的数据，因此构成了一个可以并行处理交易数据并产生区块的系统。

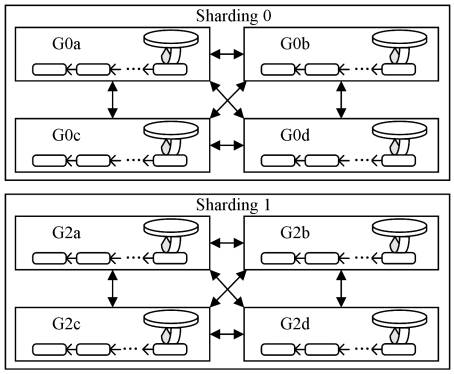


图 4 由 8 个节点构成的分区型区块链

Fig. 4 Sharding-based blockchain with 8 nodes

3.3 数据结构

分区型区块链的各个分组中包含多个并行延长的区块链，它们的区块结构和比特币区块链类似，如图 5 所示，分区区块链和比特币区块链都是由一系列包含了交易信息的区块组成，它的基本组成单元称为区块[28]。每个区块分为区块头和区块体两部分，区块头包含版本号、父区块哈希值、时间戳、难度值、随机数和默克尔树根等信息，区块体包含所有的具体交易信息，这些信息经过默克尔树生成过程，最终将生成的树根保存在区块头中。区块头包含前一个区块的哈希值，子区块又会包含它的哈希值，这样就形成了一条联系紧密的链条，若其中某个部分被修改，则需要修改之后的所有区块。区块链中的首个区块是特例，叫作创世区块(genesis block)，它没有父区块。

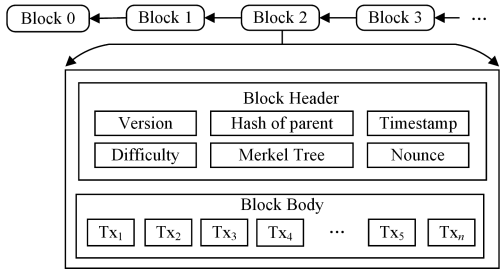


图 5 分区区块链的数据结构

Fig. 5 Data structure of Sharding-Based blockchain

3.4 共识机制

分区区块链的共识过程发生在每个分组内部，在每组中并行地运行着共识协议，处理并存储交易信息。部分分区型区块链系统不使用 PoW 共识机制的原因是，为分区带来的算力稀释问题导致对单个分区攻击的难度降低，所以其采用 PBFT 协议，它可以避免基于算力的恶意攻击。但是 PBFT 伴随着巨大的通信开销，同时也面临着女巫攻击的风险，因此这些系统通常会提高加入系统的要求，使得节点成为系统内节点的难度大大提高，从而避免女巫攻击。目前的分区区块链采用了多种共识机制，Elastico 采用了 PBFT 共识机制，OmniLedger 采用了 ByzCoinX 共识机制，而 RapidChain 采用了改进的 PBFT 协议，Monoxide 则采用了 PoW 共识机制，因为它通过诸葛连弩挖矿(Chu-ko-nu mining)算法解决了 PoW 共识机制在分区后算力被稀释的问题，使得攻击单个分区与

攻击整个系统一样困难。

3.4.1 实用拜占庭协议 PBFT 及其改进协议

实用拜占庭协议 PBFT[29]共包括 3 个阶段：预准备阶段、准备阶段和确认阶段。在预准备阶段，由主节点发布包含待验证记录的预准备消息。接受到预准备消息后，每一个节点进入准备阶段。主节点向所有节点发送包含待验证记录的准备消息，每一个节点验证其正确性，将正确记录保存下来并发送给其他节点。直到某一个节点接收到 $2f$ 个不同节点发送的与预准备阶段接收的记录相一致的正确记录，该节点才向其他节点广播确认消息，系统进入确认阶段。在确认阶段，直到每个诚实节点接收到 $2f+1$ 个确认消息，协议才终止，各节点对该记录达成共识。

Elastico 系统采用了 PBFT 共识机制。OmniLedger 系统中的 ByzCoinX 共识机制实际上是对 PBFT 的修改，但是相对减小了协议的通信开销。OmniLedger 区块链由一条身份链和多条子链构成，它使用了一个随机分配协议将所有的验证器(全节点)分配到不同的子链中。在每个子链中仍使用 PBFT 共识算法达成一致性。而 RapidChain 延续了 PBFT 共识协议，但是 RapidChain 通过被称为 Gossip-IDA 的消息传递协议减小了通信带来的巨大开销。它将每一个即将传播的消息分割成若干个块，在网络中传播消息的片段而不是整个消息来减少通信量，各个节点将接收到的消息通过纠错偏码的方法组合成原消息。

3.4.2 诸葛连弩挖矿算法(Chu-ko-nu)

比特币等大多数区块链系统都采用 PoW 共识机制，PoW 最初用来应对服务与资源滥用，或是拒绝服务攻击等[30-31]。在比特币中，必须选择一个节点来记录一段时间内的交易信息。最简单的办法是随机选择，但是这种方法极易受到攻击而失效；另外的办法是提高成为记账人的条件，即工作量证明[32]。

诸葛连弩挖矿算法是对基于工作量证明机制算法的改进。PoW 算法中矿工节点经过算力竞争，由胜出者产生全系统中唯一的下一个区块，它的安全风险在于当恶意节点掌握全网算力一半以上时，可以逆转已经发生的交易，造成双花(double spending)问题，由于这样的算力很难达成，这种攻击难以实现。在分区后，总体的挖矿算力被划分到不同的分组，会导致攻击单个分区只需要达到该分区的算力的一半即可，因此在分区后仍然使用 PoW 会带来安全隐患。

诸葛连弩挖矿算法允许任何一个分区内矿工在成功解决哈希难题时，同时在多个分区产生多个区块，但是每个分区最多产生一个区块。通过这种方式，使得每个分区内的矿工算力放大，从而达到攻击单个分区和攻击整个系统需要相同量级的算力要求。

4 综合对比与分析

4.1 3 类区块链系统的技术对比

表 1 列出了多个典型比特币区块链、图型区块链以及分区型区块链在技术上的区别。在数据结构上，比特币区块链将多笔交易打包进区块，区块之间形成稳定的链条，而 Byteball，Dagcoin，Nano 和 IOTA 区块链中，每笔交易以及父母单元的哈希值构成一个基本单元，各单元之间通过哈希值紧密连接，从而形成一个有向无环图，其中 NXT 较为特殊，它仍然以粗粒度的区块为基本单位，只是不再是一个区块连接一个区块，而是一个区块连接若干个区块。分区区块链保留了比特币区块链中大部分的数据结构，均以区块为单位组织数据。

表 1 3 类区块链系统的技术对比

Table 1 Comparison of techniques of three classes of blockchains

系统	年份	数据结构	体系结构	共识机制	项目阶段	是否开源
Bitcoin[1]	2008	Block	P2P	PoW	投入运行	是
Ethereum[3]	2013	Block	P2P	Casper	投入运行	是
NXT[33]	2013	Block-DAG	P2P	PoS	投入运行	是
Byteball[14]	2017	DAG	P2P	Witness	投入运行	是
DagCoin[15]	2015	DAG	P2P	Witness*	投入运行	否
Nano[13]	2014	DAG	P2P	DPoS	投入运行	是
IOTA[16]	2016	DAG	P2P	Tangle	投入运行	部分开源
Elastico[21]	2016	Block	Sharding-P2P	PBFT	实验阶段	否
Zilliqa[23]	2017	Block	Sharding-P2P	PBFT*	投入运行	是
OmniLedger[24]	2017	Block	Sharding-P2P	ByzCoinX(PBFT*)	实验阶段	否
RapidChain[26]	2018	Block	Sharding-P2P	PBFT-ErasureCode	实验阶段	否
Monoxide[27]	2019	Block	Sharding-P2P	Chu-ko-nu	实验阶段	否

在体系结构上，列举的比特币区块链和图型区块链均采用 P2P 网络结构。分区区块链相比其他两种区块链变化较大的是体系结构，分区区块链不再是所有的节点组成一个 P2P 网络，而是将多个节点分成若干组，每组中有局部的 P2P 网络，组和组之间又形成一个高层次的 P2P 网络，从而形成分区-P2P 的模型。

在共识机制方面，比特币采用 PoW 共识机制，而以太坊采用 PoW+PoS 混合的 Casper 共识机制。图型区块链中，NXT 采用了 PoS 共识机制，Dagcoin 系统是基于 Byteball 的源码修改而来的，因此也暂时采用与 Byteball 相同的 Witness 共识机制。分区区块链中，Elastico 采用 PBFT 协议，但是该协议面临着巨大的通信开销，因此 Zilliqa 共识将 PBFT 与 EC-Schnorr 多重签名相结合。Rapidchain 共识将 PBFT 与 ErasureCode 相结合，从而减小了通信量。而 OmniLedger 中的 ByzCoinX 是指每个分组包含若干验证器节点，分区内通过 PBFT 达成共识后，各验证器节点之间进行通信，分区之间不再需要运行 PBFT 协议，从而也减小了通信量。特别地 Monoxide 系统采用了 PoW 共识机制，它解决了分区后总算力被

稀释导致的 PoW 共识机制的安全性问题。

目前，表 1 中的各个传统区块链和图型区块链都已经通过各种方式发行货币，并开始流通，属于生产环境下的系统，且大多数已经开源，但 Dagcoin 仍然没有开放源码，而 IOTA 只开放了部分源码，对系统中的协调器部分代码闭源，因此导致其公平性备受争议。而分区区块链中只有 Zilliqa 投入了运营，且公开了源码，其他分区区块链仍处于实验阶段，暂时未公开源码。

4.2 各区块链的性能对比

表 2 列出了各区块链系统的性能指标。

表 2 3 类区块链系统的性能对比

Table 2 Comparison of performance of three classes of blockchains

系统	类型	容错率	挖矿	交易费	去中心化	确认延迟	吞吐率	伸缩性
Bitcoin[1]	传统	1/2	有	较高	是	>10 min	7 TPS	差
Ethereum[3]	传统	1/2	有	较高	是	18 s	30 TPS	差
NXT[33]	DAG	—	无	较低	是	1 min	100 TPS	较好
DagCoin[15]	DAG	—	无	较低	否	30 s	—	较好
ByteBall[14]	DAG	—	无	较低	否	>1 min	—	较好
Nano[13]	DAG	—	无	无	是	1−10 s	7000 TPS	较好
IOTA[16]	DAG	—	无	无	否	1−60 s	—	较好
Elastico[21]	分区	1/3	无	无	是	800 s	—	极好
Zilliqa[23]	分区	1/3	无	无	是	—	1400 TPS	极好
OmniLedger[24]	分区	1/3	无	无	是	20 s	6000 TPS	极好
RapidChain[26]	分区	1/4	无	无	是	8 s	7000 kTPS	极好
Monoxide[27]	分区	1/2	有	无	是	15 s	6000 kTPS	极好

在容错性方面，两种传统区块链和 Monoxide 的容错率都达到了 1/2，而采用 PBFT 类共识的分区区块链 Elastico，Zilliqa，OmniLedger 以及 RapidChain 的容错率和 PBFT 本身的容错率一致，为 1/3。在挖矿方面，采用 PoW 类共识的传统区块链以及 Monoxide 需要挖矿，而 DAG 图型区块链 NXT，DagCoin，Byteball，Nano，IOTA，以及采用 PBFT 类共识的 Elastico，Zilliqa，OmniLedger，RapidChain 分区区块链不需要挖矿。

在交易手续费方面，两种传统区块链一般需要支付较多的手续费才可以在系统中发起交易，DAG 图型区块链中 NXT，Dagcoin，Byteball 只需要支付较少的手续费，Nano，IOTA 和分区型区块链不需要手续费。

在交易确认速度方面，比特币至少为 10 min，以太坊约为 18 s，NXT 约为 1 min，Dagcoin 约为 30 s，Byteball 约为 1 min，Nano 为 10s 之内，IOTA 为 60 s 之内，Elastico 为 800 s，OmniLedger，RapidChain，Monoxide 分别是 20 s，8 s 和 15 s。在吞吐率方面，以每秒处理的交易次数为单位（TPS），比特币约达到 7 TPS，以太坊平均为 30 TPS，NXT 约为 100 TPS，Nano 和 Zilliqa 在理论上分别可达 7000 k 和 1400 k，而 OmniLedger，RapidChain 和 Monoxide 在实验条件下最高可达 6000 TPS，7000 TPS 和 6000 TPS。

在去中心化程度上，两种传统区块链、列举的分区区块链、NXT 以及 Nano 是完全去中心化的，而图型区块链 Byteball 和 IOTA 目前并不是完全去中心化的。在可伸缩性上，两种传统区块链几乎无法实现可伸缩性，而图型区块链有较好的可伸缩性，分区区块链在理论上可以随着网络节点和分组数的增加实现线性的无限拓展。

在安全性方面，传统区块链既有理论上基于算力的容错模型，又经过实际运行，充分证实了其安全可靠，分区区块链经过分区面临着单分区遭受攻击的风险，图型区块链中的中心化组件易遭受攻击也给系统的安全性带来了隐患。

4.3 两种新型区块链的优缺点

表 3 列出了两种新型区块链的优缺点及应用场景，图型区块链的优势在于其共识机制属于异步通信的一种，相比传统区块链，其具有实时性强和确认速度快的特点，因此图型区块链比较适合物联网、即时通讯、小额结算等领域，此外图型区块链还具有较高的可伸缩性以及较低的交易费用。然而图型区块链的缺点也很明显，首先图型区块链的验证机制是后面的交易验证前面的交易，在系统初期节点量较少的情况下，容易造成交易长时间无法验证的问题，虽然 IOTA 引入超级节点验证交易，但违背了去中心化的初衷；其次，图型区块链采用谣言传播算法，本质上属于异步通信，不存在一个全局的排序机制，因此也不支持强一致性；最后，DAG 的安全性没有经过大规模的长时间的验证，这是导致图型区块链还不能大规模应用的原因之一。

表 3 两种区块链的优缺点及应用场景

Table 3 Pros and cons of two classes of blockchains and their applications

	优点	缺点	适应场景
DAG 图型区块链	1. 实时性强 2. 伸缩性强 3. 交易费用低	1. 具有中心化特性 2. 不支持强一致性 3. 安全性未验证	物联网、即时通讯、小额结算等
分区型区块链	1. 存储量高 2. 吞吐率高 3. 去中心化	1. 有单分区攻击风险 2. 多分区之间同步难度大	公有链数字货币系统、存证、信息溯源等

分区型区块链的优势是具有极好的可伸缩性，随着分区的增多，整个系统的吞吐率会随着分区的增多而线性提升，同时分区也可以提升系统的总体存储容量，相当于对整个系统进行一次数据分片，存储容量也是线性提升的。因此，分区区块链更适合处理高事务吞吐率和高存储容量的场景，如数字货币、存证、商品溯源等领域。另外，分区系统中无论采用 PBFT 还是 PoW 等传统共识机制，它们都具备去中心化特

性，而且不依赖于系统规模，这是这些共识机制本身的特征。分区区块链也有一些缺点，首先分区后的区块链会稀释系统总体抵抗攻击的能力，具有单个分区易遭受攻击的风险；其次多个分区之间的一致性对共识机制提出了更高的要求。

结束语 通过对两种新型区块链的介绍和对比分析发现，两种新型区块链尝试从多层次多角度对区块链进行改进，突破了区块链在吞吐率、伸缩性和安全性等方面的瓶颈，但是始终无法全方位地兼顾这些特性，如图 6 所示，这也与目前限制区块链实际运用的原因相符。当前区块链技术在系统层面的主要问题是在保证去中心化和安全性的前提下无法大幅度提高性能，即区块链不可能三角[34-35]。

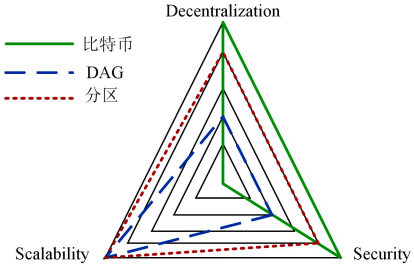


图 6 区块链不可能三角

Fig. 6 Impossible triangle of blockchain

区块链技术除了面临吞吐率、伸缩性、安全性等方面的问题，在数据存储、事务处理和数据查询等方面也亟待提出新的解决方案。近年来已有学者在数据存储[36-37]、事务处理[38-40]、数据查询[41-43]等方面进行研究。

为了平衡区块链不可能三角，一种思路是考虑不同业务应用对 3 个性质的要求各不相同，未来可能需要一种能够在不可能三角之间灵活调节的区块链系统，甚至是一种能够自适应调节的区块链系统，以满足各种业务不同的去中心化性、伸缩性和安全性需求。另外，还应该与传统数据库理论问题相结合，研究在区块链技术中的数据存储、事务处理、查询优化等关键问题。

区块链具有去中心化、完全防篡改、去信任等特点，这是传统数据库所不具备的，区块链去中心化和去信任的特性使得区块链可在无第三方的情况下进行匿名投票、在线拍卖、选举等，其防篡改特性使得区块链可应用于征信系统、商品溯源、数据存证等对数据篡改敏感的应用领域。未来区块链应该向多元化的方向发展，针对不同业务需求设计不同的区块链系统，在解决数据存储、事务处理、查询优化等关键问题后，与传统数据库的优势互补，在不同的领域充分发挥区块链的优势。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[2] WOOD G. Ethereum: A secure decentralized generalised transaction ledger [J]. Ethereum project yellow paper, 2014, 151: 1-32.

[3] BUTERIN V. A next-generation smart contract and decentralized application platform [EB/OL]. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf, 2014, 3: 37.

[4] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [C]// Proceedings of the Thirteenth EuroSys Conference. ACM, 2018: 30.

[5] YUAN Y, WANG F Y. Blockchain: The State of the Art and Future Trends. [J]. Acta Automaticsa Sinica, 2016, 42(4): 481-494.

[6] BENI F M, ŽARKO I P. Distributed ledger technology: blockchain compared to directed acyclic graph [C]// 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018: 1569-1570.

[7] ZHANG K, JACOBSEN H A. Towards dependable, scalable, and pervasive distributed ledgers with blockchains [C]// 38th IEEE International Conference on Distributed Computing Systems (ICDCS). 2018.

[8] SUDHIR Khatwani. How Long Does It Take To Transfer Bitcoins And Why? [EB/OL]. [2019-4-23]. https://coinsutra.com/bitcoin-transfer-time/.

[9] O'DWYER K J, MALONE D. Bitcoin mining and its energy footprint [C]// 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conferenceon Information and Communications Technologies (ISSC 2014/CIICT 2014). 2014: 280-285.

[10] BEALL A. Bitcoin mining uses more energy than Ecuador-but there's a fix [EB/OL]. [2019-4-29]. https://www.newscientist.com/article/2151823-bitcoin-mining-uses-more-energy-than-ecuador-but-theres-a-fix/.

[11] 维基百科. Directed _ acyclic _ graph [EB/OL]. [2019-05-06]. https://en.wikipedia.org/wiki/Directed_acyclic_graph.

[12] CAO Y, ZHANG C. Blockchain Technology : Principles and Practice [M]// Mechanical Industry Press. 2018: 1-2.

[13] LEMAHIEU C. RaiBlocks: A feeless distributed cryptocurrency network [EB/OL]. https://nano.org/en/whitepaper.

[14] CHURYUMOV A. Byteball: A decentralized system for storage and transfer of value [EB/OL]. https://obyte.org/Byteball.pdf.

[15] LERNER S D. DagCoin: a cryptocurrency without blocks [EB/OL]. https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf.

[16] POPOV S. The tangle [EB/OL]. http://www.tangleblog.com/wp-content/uploads/2016/11/IOTA_Whitepaper.pdf.

[17] KING S, NADAL S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake [EB/OL]. https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf, August, 2012, 19.

[18] VITALIK Buterin. Vitalik Non-giver of Ether [EB/OL]. [2019-05-02]. https://twitter.com/VitalikButerin/status/1072162014498148355.

[19] LEMAHIEU C. Nano: A feeless distributed cryptocurrency network [EB/OL]. https://nano.org/en/whitepaper.

[20] GRIGG I. Eos-an introduction [EB/OL]. Whitepaper iang.org/papers/EOS_An_Introduction.pdf, 2017.

[21] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains [C]// Proceedings of the 2016

ACM SIGSAC Conference on Computer and Communications Security. ACM,2016:17-30.

[22] DOUCEUR J R. The sybil attack[C]// International workshop on peer-to-peer systems. Berlin:Springer,2002:251-260.

[23] ZILLIQA T. The ZILLIQA Technical Whitepaper[EB/OL]. https://docs.zilliqa.com/whitepaper.pdf.

[24] KOKORIS-KOGIAS E,JOVANOVIC P,GASSER L,et al. Omniledger:A secure,scale-out,decentralized ledger via sharding[C]// 2018 IEEE Symposium on Security and Privacy (SP). IEEE,2018:583-598.

[25] KOGIAS E K,JOVANOVIC P,GAILLY N,et al. Enhancing bitcoin security and performance with strong consistency via collective signing[C]// 25th {USENIX} Security Symposium ({USENIX} Security 16). 2016:279-296.

[26] ZAMANI M,MOVAHEDI M,RAYKOVA M. RapidChain:Scaling blockchain via full sharding[C]// Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM,2018:931-948.

[27] WANG J,WANG H. Monoxide:Scale out Blockchains with Asynchronous Consensus Zones[C]// 16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19). 2019:95-112.

[28] DRESCHER D. Blockchain Basics:A Non-Technical Introduction in 25 Steps[M]. Apress; 1st ed. 2017.

[29] CASTRO M,LISKOV B. Practical Byzantine fault tolerance[C]// OSDI. 1999,99:173-186.

[30] JAKOBSSON M,JUELS A. Proofs of work and bread pudding protocols[M]// Secure Information Networks. Springer,Boston,MA,1999:258-272.

[31] DWORK C,NAOR M. Pricing via processing or combatting junk mail[C]// Annual International Cryptology Conference. Springer,Berlin,Heidelberg,1992:139-147.

[32] ZHENG Z,XIE S,DAI H,et al. An overview of blockchain technology:Architecture,consensus,and future trends[C]// 2017 IEEE International Congress on Big Data (BigData Congress). IEEE,2017:557-564.

[33] Nxt Whitepaper[EB/OL]. [2019-04-20]. https://whitepaperdatabase.com/nxt-nxt-whitepaper/.

[34] SWARTZ A. Squaring the triangle:Secure,decentralized,human-readable names[J]. Retrieved,2011,11(30):2015.

[35] WILCOX-O'HEARN Z. Names:Decentralized,secure,human-meaningful:Choose two[J/OL]. https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html.

[36] WANG S,DINH T T A,LIN Q,et al. Forkbase:An efficient storage engine for blockchain and forkable applications[J]. Proceedings of the VLDB Endowment,2018,11(10):1137-1150.

[37] XU Z,HAN S,CHEN L. CUB,a consensus unit-based storage scheme for blockchain system[C]// 2018 IEEE 34th International Conference on Data Engineering (ICDE). IEEE,2018:173-184.

[38] SHARMA A,SCHUHKNECHT F M,AGRAWAL D,et al. Blurring the Lines between Blockchains and Database Systems:the Case of Hyperledger Fabric[C]// Proceedings of the 2019 International Conference on Management of Data. ACM,2019:105-122.

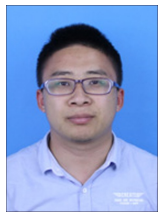
[39] AMIRI M J,AGRAWAL D,ABBADI A E. CAPER:a cross-application permissioned blockchain[J]. Proceedings of the VLDB Endowment,2019,12(11):1385-1398.

[40] AMIRI M J,AGRAWAL D,ABBADI A E. Parblockchain:Leveraging transaction parallelism in permissioned blockchain systems[J]. arXiv preprint arXiv:1902.01457,2019.

[41] XU C,ZHANG C,XU J. vChain:Enabling verifiable boolean range queries over blockchain databases[C]// Proceedings of the 2019 International Conference on Management of Data. ACM,2019:141-158.

[42] XU C,ZHANG C,XU J. vChain:Enabling verifiable boolean range queries over blockchain databases[C]// Proceedings of the 2019 International Conference on Management of Data. ACM,2019:141-158.

[43] RUAN P,CHEN G,DINH T T A,et al. Fine-grained,secure and efficient data provenance on blockchain systems[J]. Proceedings of the VLDB Endowment,2019,12(9):975-988.



ZHANG Chang-gui, born in 1996, postgraduate. His main research interests include blockchain technology and storage system.

YU Ge, born in 1962, professor, is a member of China Computer Federation. His main research interests include distributed system and big data management.