DOI：10.19788/j.issn.2096-6369.200201

区块链技术发展与展望

李　慧　袁煜明*　赵文琦

（火币区块链研究院，澄迈 571900）

摘　要：区块链技术和比特币在2008年相伴而生，但随着各界对其研究与应用不断深入，区块链技术已经开始独立于加密数字货币，发展成为一个新的研究领域。区块链技术利用密码学原理、分布式数据存储技术、点对点网络及共识机制构建的分布式账本为解决多方合作过程中的信任、隐私、数据差异等问题带来了契机。诸多产业领域如金融、政务、医疗、城市建设等均开始应用区块链技术。当前，随着区块链技术的应用与推广，区块链技术也遇到了诸如扩展性、安全性、监管难等方面的挑战，催生了各界围绕区块链技术的各个方面及相关的密码学技术不断进行创新研究或引入新技术进行补充。本文结合当前学界及产业界的研究及应用情况，总结了区块链技术的五层基础体系架构，即数据层、网络层、共识层、合约层及应用层，并综述了该架构中各个层次的原理与技术。在此基础上，进一步介绍了针对区块链与传统网络结合、区块链技术自身以及相关密码学技术的各种典型的扩展技术，并讨论这些技术对区块链技术带来的影响。最后，结合区块链技术当前的发展现状，分析了其在研究应用中面临的挑战及其未来的发展方向，以期为未来的研究工作带来启发与借鉴。

关键词：区块链；分布式；点对点网络；共识机制；智能合约；区块链技术

中图分类号：G203　　**文献标识码：A**　　**文章编号：**2096-6369（2020）02-0005-09

引用格式：李慧,袁煜明,赵文琦.区块链技术发展与展望[J].农业大数据学报,2020,02(02):5-13.

Li Hui,Yuan Yuming,Zhao Wenqi.Development and Visions of Blockchain Technology[J].Journal of Agricultural Big Data,2020,02(02):5-13.

Development and Visions of Blockchain Technology

Li Hui　Yuan Yuming*　Zhao Wenqi

(Huobi Research, Cheng Mai 571900,China)

Abstract: Blockchain (or distributed ledger) technology was introduced in 2008, when the famous Bitcoin cryptocurrency was initiated. Blockchain has been undergoing rapid growth in both academia and industry. Today, it is no exaggeration to say that blockchain has become a new, independent research topic—not a subtopic subsumed within cryptocurrencies. From a technical perspective, blockchain technology is based on various fundamental computing technologies, such as advanced cryptography, distributed data storage, peer-to-peer networking, and distributed consensus protocols. Generally, blockchain technology involves creating a shared, distributed ledger: that ledger can offer great flexibility and potential in resolving many important challenges in a complex computing context that involves multiple parties. Examples of such challenges include achieving mutual trust, privacy protection, and data consistency in large-scale business scenarios. Many business applications have already covered a

收稿日期：2020-05-20

第一作者简介：李慧，女，硕士，区块链技术和应用；E-mail：lihui0729@huobi.com

通讯作者：袁煜明，男，硕士，区块链技术和应用；E-mail：yuanyuming@huobi.com

broad range of industrial services, such as those related to finance, governance, medicine, and city construction. Blockchain technology is becoming increasingly adopted and applied; however, the current design of blockchain is practically far from sufficient—especially when dealing with critical domain challenges. Specifically, the key limitations of blockchain mainly derive from poor system scalability, weak resilience to external security attacks, and lack of computing interfaces for regulatory processes. Conversely, it is the very shortcomings of blockchain technology that motivate research efforts into many related technologies. Based on conventional blockchain design, new functional extensions and cryptography technical optimizations have been continuously proposed by researchers and practitioners: the aim is to make blockchain technology more practically applicable and meet various demands of different business users. In this overview paper, using the latest findings from both academic and industrial research, we systematically present the general architecture of blockchain technology with its five functional layers. The five-layered architecture comprises the following: a data layer; a network layer; a distributed consensus layer; a smart contract layer; and an application layer. We also provide a technical description of key theories and important techniques related to each functional layer. From the proposed general architecture of blockchain technology, we offer an in-depth explanation of its core technical extensions with respect to the following: blockchain integration with existing computer network techniques; the blockchain framework itself and important modules; and underlying critical cryptography techniques. Further, we discuss potential contributions that these promising technical extensions could provide with respect to reshaping and optimizing blockchain technology. Finally, following current developments with blockchain technology and its existing mainstream applications, the general views about future challenges and important directions for this technology is to facilitate future follow-up research.

Keywords: blockchain; distribution; P2P network; consensus protocol; smart contract; blockchain technology

1 引言

2008年10月31日,中本聪在密码朋克邮件组中发布了《比特币:一种点对点的电子现金系统》[1],由此开启了加密数字货币与区块链技术的兴起之路。作为加密数字货币的底层基础技术,区块链技术一度与其紧紧绑定在一起,应用在各类公链项目中。而后,随着对区块链技术价值的发掘,区块链技术逐渐发展成为独立的研究领域,二者开始逐渐被区分。区块链技术被视作为底层的分布式账本技术,加密数字货币则被视作该层技术之上的激励手段及其应用生态中的金融工具,在联盟链的应用领域中甚至可以不需要加密数字货币。

区块链技术的主要特征包括完全分布式、透明、不可篡改和可追溯。完全分布式:区块链利用分布式存储和分布式网络的技术,使得区块链网络中没有中心化节点且账本数据分散存储在网络中的各个对等节点中;透明:除了被加密的私有信息外,分布式账本中的所有信息均可以通过接口查询,网络中的所有节点均可以对其进行查询与校验。不可篡改:除了允许信息更改的部分私有区块链之外,区块中的信息一旦被全网达成共识并记录在区块链中,就无法再被更改。可追溯:存储在区块链中的交易可以通过其链式结构进行来源去向的追查。

这些特征对比传统中心化的技术架构体系在部分应用场景下有其特有的优越性,随着区块链技术的活力逐步彰显,越来越多的产业开始应用区块链技术。在金融领域,其被应用到支付清算、保险理赔、供应链金融等;在政务领域,被应用到数字身份、征信、司法存证、电子政务等;在医疗领域被应用到药品供应链、临床数据等;在城市建设领域被应用到交通运输、能源管理、公共建设等。同时,也有诸多国家颁布政策法令支持区块链技术的发展甚至将其与国家战略相关联。

在早期的研究中,区块链的体系架构主要聚焦在数据结构与共识机制上[2],还有一部分研究工作提出了完整区块链技术架构并做了充分的论述[3-4],但对区块链技术发展过程中涌现的扩展技术着墨不多,因此本文在前人的基础上,结合近年来区块链技术的发展现状总结了区块链的五层基础技术架构,并在此基础上讨论了各项扩展技术的研究与应用进展。

2　区块链基础架构

2.1 基础架构

区块链技术经过十多年的发展,基本形成了如图1所示的基础技术架构,自下而上分别是数据层、网络层、共识层、合约层以及应用层。数据、共识、网络是区块链分布式账本的核心内涵,可以合称为分布式账本层。

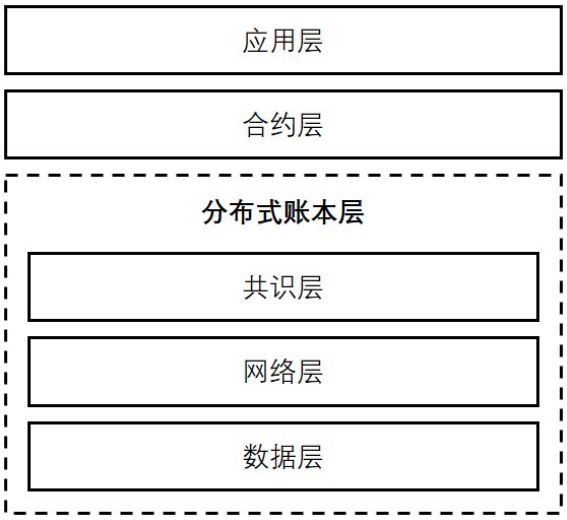

图1　区块链基础技术架构

Fig.1　Architecture of blockchain

其中,数据层的内涵主要包括数据结构、数据模型及数据存储;网络层负责组网、传输与校验;共识层通过共识算法协调分布式环境中的协作节点达成共识;合约层包含了智能合约编写和执行的环境;应用层则运行着基于区块链技术的各种应用。

针对区块链的基础技术架构,也有研究人员提出过不同的分层架构方案[3-4]。第一个不同之处体现在层次排列次序不同,区块链的共识层、网络层与数据层在技术实现上并无严格的次序依赖关系,其三者可被统一视作为“分布式账本层”,因此不同的排布方式不影响技术架构的内涵。第二个不同体现在是否将“激励层”纳入架构中,由于激励层的讨论内容更偏向经济模型而不是技术模型的设计,同时激励层在不同的区块链类型中并不普适存在,因而不被纳入到本文的基础技术架构中。

在该种架构下,应用层通过合约层提供的智能合约工具构建各类区块链应用,合约层依赖分布式账本层完成分布式网络下的共识达成、数据传播与存储。

2.2 数据层

区块链的数据层以分布式的方式存放着记录交易的区块。在业界实际的应用中,不同区块链的数据结构、数据模型及数据存储各有异同。

(1) 数据结构

就数据结构而言,区块链以区块为单位进行组织。

区块包含区块头和区块体两部分,典型的区块结构如图2所示。区块头中存放的数据为支持区块链运行的功能型数据,其数据域没有通用的标准,但通常会包含前块哈希、默克尔根及时间戳信息。前块哈希本质上是指向父区块的指针,将区块链接起来;默克尔根是区块体中的默克尔树树根的值;时间戳记录了区块的产出时间可用于存证。不同的区块链还会包含不同的与其数据组织机制和共识机制紧密关联的数据域。如比特币区块头中还包含版本、难度目标及一个与工作量证明算法关联的随机数等;以太坊的实现机制更为复杂,区块头中还包含了布隆过滤器、手续费gas上限、叔块哈希等更多的信息。

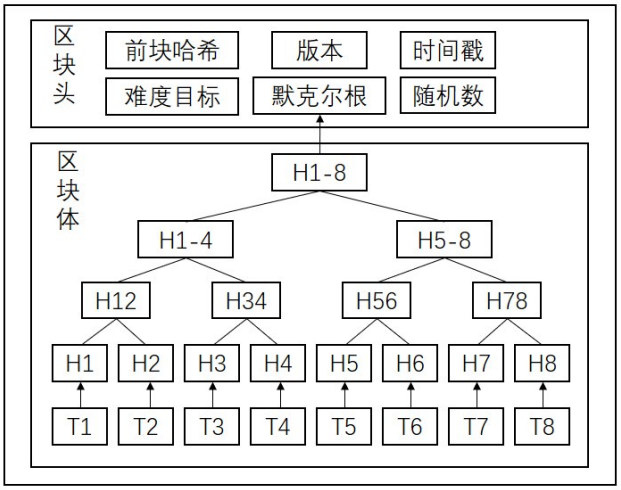

图2　区块结构

Fig.2　The structure of block

区块体中通常主要包含交易数据的信息,交易数据通常利用默克尔树[5-7]进行组织,以增加数据的篡改成本并实现数据的快速比对与存在校验。默克尔树中每一个节点都是哈希值,因而也被称作哈希树。

为了提升树的性能,以太坊提出了结合默克尔树与前缀树[8-9]的MPT(Merkle Patricia Trie)树[10]用于存储其交易、收据以及状态数据。

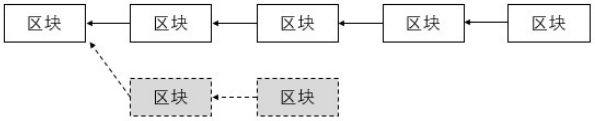

图3 链式结构

Fig.3 A chain structure

现今主流的区块链结构为链式结构,如图3所示,区块与区块之间由前序哈希连接。当链上产生分叉时,选取最长链作为主链。但近年也出现了以有向无环图(DAG)[11]作为组织形式的区块链项目[12-14]。

(2) 数据模型

区块链技术中的数据模型主要分为两种,交易模型和账户模型。交易模型侧重于记录交易的过程,即交易的来源与去向,以比特币、Corda[15]等为代表的UTXO模型,这种模型天然契合区块链的链式结构,可以快速追踪和验证交易,但扩展性不强。账户模型侧重于记录账户的状态,即交易的结果,以以太坊、Hyperledger Fabric[16]等为代表,这种模型灵活性更强,能支持更为复杂的业务处理逻辑。

(3) 数据存储

区块链的数据存储主要包括区块数据的存储和索引、状态等信息的存储。对于区块数据的存储,部分区块链选择了文本文件存储的方式,如比特币、Hyperledger Fabric,也有以以太坊为代表的一些区块链将区块数据存储在数据库中。索引和状态信息一般都被存储在KV型数据库中以实现快速检索,典型的KV数据库包括LevelDB等。

区块链中每一个节点都可以作为存储完整的区块链账本、索引、状态等数据的全节点,达不到全节点存储资源要求的节点也可以选择做存储部分数据的轻节点。

2.3 网络层

网络层的职责是组网、数据传播与数据校验。

(1) 组网

在组网方面,与传统的C/S、B/S架构使用的中心化网络不同,区块链中使用点对点网络(P2P Network),这种网络中每一个节点均是对等节点,均可以提供服务和获取服务。该种网络下不会因为中心节点的处理能力不足而形成性能瓶颈,网络中少部分节点的下线或者故障不会导致网络瘫痪或数据遗失。

特别地,在区块链的网络中,每一个节点均可以承担路由、传播、验证及引入新节点的职责。在应用实践中,各项目的组网思路基本一致,以太坊的组网模式是基于P2P网络的核心协议Kademlia[17]协议做了适应性的改动。

(2) 数据传播

由于区块链中每个节点均只与相邻节点建立网络连接,故在数据传播时每个节点均只向相邻节点广播。核心传播步骤是,当某个节点产生了新区块,会将区块数据添加到本地链上并传输给临近节点;临近节点接收数据并校验通过后会存储到本地链并进一步传播,如果未通过校验则中止传播;如此循环直至区块数据同步到全网达成共识,或被废弃。经典的数据传播协议如Gossip[18]等也被应用到一些区块链的实践中。

(3) 数据校验

数据校验的主要是为了保证区块数据的合法性。校验内容在不同的区块链中有所不同,主要包含对共识证明、数字签名、数据结构、数据长度等的校验。以比特币为例,其校验中包含工作量证明、Merkle根、区块大小、交易数据结构及合法性等。

2.4 共识层

一致性问题是分布式系统面临的共性问题,共识机制是实现一致性的手段。传统的分布式系统本质上还是利用分布式技术的中心化系统,因此处理核心功能的节点接受统一的决策指令,共识问题也弱化成在节点诚实的基础假设上解决一致性的问题,只需要满足崩溃容错(Crash Fault Tolerance,CFT)共识协议即可,Paxos[19]、Raft等就是这类协议。

但在区块链这种完全分布式的场景中,决策权高度分散在好坏难辨的网络节点上,网络中的节点可能返回任意类型的结果,包括恶意的结果。因此,需要应用支持拜占庭容错(Byzantine Fault Tolerance,BFT)的共识协议,保证在网络内部分节点故障或作恶的情况下,整个网络仍能正常、一致地运行。这种共识协议主要分为两大类,概率性的PoX(Proof of X)类和确定性的BFT类。

主流的共识机制对比如表1所示,本文将主要讨论PoX和BFT类共识。

表1　主流共识机制比较

Table1　Comparison of mainstream consensus protocols

共识协议	核心算法	拜占庭容错	敌手模型	扩展性	分布式程度	应用
PoW	PoW	是	$<(1/2)n$	低	高	Bitcoin, Ethereum
PoS	PoS	是	$<(1/2)n$	中	高	Peercoin, Nxt
DPoS	PoS	是	$<(1/2)n$	中	高	EOS, Bitshares
PoA	PoW+PoS	是	$<(1/2)n$	中	高	Decred
PoB	PoW+PoS	是	$<(1/2)n$	中	高	Slimcoin
PoSV	PoW+PoS	是	$<(1/2)n$	中	高	Reddcoin
PoC	PoW+PoS	是	$<(1/2)n$	中	高	Lava
Paxos	CFT	否	$<(1/3)n$	高	中	Chubby
Raft	CFT	否	$<(1/3)n$	高	中	etcd, braft
PBFT	BFT	是	$<(1/3)n$	高	中	Fabric
HotStuff	BFT	是	$<(1/3)n$	高	中	Facebook Libra
LibraBFT	BFT	是	$<(1/3)n$	高	中	Facebook Libra
Tendermint	PoS+BFT	是	$<(1/3)n$	高	中	Monax

说明:表中PoW为proof of work,PoS为proof of stake,DPoS为delegated PoS,PoA为proof of activity,PoB为proof of burn,PoSV为proof of stake velocity,PoC为proof of capacity。敌手模型表示相应共识协议能够承受的最大恶意节点数量,其中n代表区块链网络的节点总数。特别的,Paxos和Raft共识协议不支持拜占庭恶意节点容错,其敌手模型代表能够承受的最大宕机节点数量。

(1) PoX类共识

PoX(Proof of X)类共识需要节点提供某种证明,才能以一定概率获得记账权,常被应用在公链中。最经典的PoW,即工作量证明,与比特币一同诞生,通过暴力求解SHA256问题提供工作量证明,最先求解的节点获得记账权,多个节点获得记账权的情况下,经过时间的推移,处于最长链上的区块的矿工是最终的记账者。PoW机制在比特币上运行十多年没有出现过致命的问题足见其健壮性,但过高的资源浪费和过低的效率催生了新的共识机制。

另一类主流的共识机制为PoS,即权益证明,节点通过消耗币龄提供权益证明。PoS认为在网络中投入通证数量越多持有时间越长的节点越值得信赖,因此有越大的概率成为出块者。在纯粹的PoS中,可以依据Follow-the-Satoshi等算法选择出块节点。PoS发展过程中也出现过各种变种,如DPoS、PoSV、Pow+PoS等。PoS共识下,出块速度更快,也解决了PoW资源浪费的问题,但其自身也存在强者恒强及一些安全性问题。

随着区块链技术的发展,除了上述两类主流的共识机制外,还涌现出许多其他PoX类的共识机制,如PoA、PoB、PoSV、PoC等。

(2) BFT类共识

BFT(Byzantine Fault Tolerance,拜占庭容错)类共识是对拜占庭问题经典解决方案的延续。不同于PoX类共识,BFT类共识通常是先达成共识,再记账,记账节点的认定也不再是基于概率的。

最早,Lamport等在1982年提出拜占庭问题[20],通过虚构描述拜占庭帝国的将军们打仗时如何让忠诚的将军在叛徒将军的扰乱下仍能就作战计划达成一致的问题,来提出如何在网络通信可靠但节点不可靠的情况下达成共识的问题。Lamport等人提出了两种协议作为解决方案,但都存在时间复杂度过高、扩展性不强的问题。直到1999年,Castro和Liskov提出了实用拜占庭容错PBFT[21]算法,将BFT的时间复杂度降低至多项式级别才真正能在工业界广泛使用。

自拜占庭问题被提出以来学术界和业界提出了各种解决方案,近年也出现了很多针对区块链的BFT优化算法及BFT与PoX类共识的混合算法。如Pass和Shi提出的PoW+BFT[22]共识、应用在Cosmos[24]的PoS+BFT共识Tendermint[25]等。

2.5 合约层

数据层、网络层与共识层构建了区块链的底层技

术,形成了分布式账本。合约层建立在分布式账本之上,该层包含了各类脚本、算法形成智能合约,为区块链提供了高度可编程性和可操作性。

智能合约的思想最早由Nick Szabo[26]于上世纪90年代提出,是一种执行合约条款的计算机交易协议,但由于没有相契合的运用场景,没有引起广泛的关注。区块链技术的发展推动了完全分布式交易的发展,为智能合约的应用打开了局面。

智能合约本质上就是一段预定义规则的代码,这种代码从技术视角看与传统技术行业的IF-ELSE逻辑的代码并没有本质区别,真正带来变化的是它运行在透明、不可篡改、完全分布式的区块链上而产生的"信任"带来了价值。

智能合约与区块链结合的雏形诞生在比特币上。比特币采用基于逆波兰表示法的堆栈执行语言来实现UTXO的锁定脚本与实现脚本,包括P2PKH(Pay-to-Public-Key-Hash)、P2PK(Pay-to-Public-Key)、P2SH(Pay-to-Script-Hash)、MS(Multi-Signature)和OP_Retuen等脚本分别实现不同的功能。使用该种脚本方式的多为早期使用UTXO模型的区块链项目及部分基于有向无环图(DAG)的项目。

由于脚本方式的智能合约通常图灵不完备,表达性有限,于是催生了多个方向上的探索。其中最有代表性的是以容器方式实现的Hyperledger Fabric、以虚拟机方式实现的以太坊。

容器方式在实现上比虚拟机方式更轻量级也更加灵活,但是这种轻量级和灵活是以容器中的智能合约和应用的实现更重为代价的。

目前最主流的实现方式还是虚拟机方式。相比较而言,这种方式提供了较为健全的基础设施,封装了底层环境的虚拟机和基于该虚拟机的高级编程语言,为在区块链上进行智能合约的开发提供了很大的便利性。如以太坊实现了一个图灵完备的虚拟机,并提供了用于编写智能合约的高级编程语言Solidity。该语言编写的智能合约编译成字节码之后可以部署在以太坊的区块链网络上,应用可以调用部署好的合约实现各种功能。

2.6 应用层

区块链的应用层与传统技术架构中的应用层类似,主要是封装一系列场景和应用。在以容器方式和虚拟机方式承载的智能合约诞生之前,区块链的应用十分有限,主要集中在数字货币上。智能合约的发展为应用层的丰富带来了福音。现今,区块链技术已经应用到金融、医疗、政务、商务、公益等各个领域,且都已经有了实践的案例,为提升各行业的效率提供了新的手段。

3 扩展技术

数据、网络、共识、合约、应用构建了区块链技术的基础架构。但是随着应用生态的发展,基础的技术架构在效率、扩展性、隐私性等方面都产生了瓶颈。因而催生了各种Layer0、Layer1、Layer2及其他方面的扩展技术。

3.1 Layer0扩展

区块链的Layer0层扩展主要集中在数据传输上,通过优化区块链和传统网络结合的问题来实现扩展。相比Layer1和Layer2层的扩展,该层的扩展对区块链技术架构的侵入性较小。

目前,Layer0层扩展方案主要集中在构建中继网络,提升数据传输的速度上。其思路类似于传统网络中的CDN(Content Delivery Network)技术,通过构建虚拟网络,部署边缘服务器,优化网络中的负载和内容分发。Layer0层中的中继网络通过在网络中部署一些中心化的中继节点,在中继节点或者中继节点构建的中继网络上做数据传输的优化,包括路由方式、传播方式、压缩技术等。目前,康奈尔大学和西北大学的研究人员提出的Bloxroute[27]与Marlin Labs提出的Marlin[28]是该方向上探索最多的项目。

3.2 Layer1扩展

Layer1层的扩展指对区块链基础架构中分布式账本层,即数据层、网络层、共识层的技术扩展,其核心在于对区块链技术自身的改造与扩展,以提升区块链的性能。

(1) 数据层

最直接的扩展方式为扩展区块大小,比特币的区块大小上限为1M,该限制成为制约比特币系统吞吐量的重要因素。扩展区块大小以实现性能提升最典型项目为比特现金(BCH)。但这种扩展方式也会带来对账本存储的挑战。

还有一种通过改变区块结构的变相扩容手段,隔离见证(SegWit,Segregated Witness)。这种方法将脚本签名从区块中拿出,使区块有更多空间用于容纳交易数据。但这种方式对吞吐量的提升很有限。

除了对区块做扩展外,也有技术对区块链经典的链式结构提出了挑战。链式的存储结构导致网络中

区块只能串行产生,无法并发处理交易数据。2015年开始,兴起了不同于链式结构的数据组织方式——有向无环图(DAG),舍弃了区块和链式结构的概念,以交易为单位做处理,支持异步并发。典型的基于DAG数据结构项目包括Byteball[12]、IOTA[13]、Hashgraph[14]等。

值得注意的是,类似DAG这种扩展技术往往也伴随着网络层和共识层机制的变化,并不仅限于数据层。

(2) 网络层

典型的网络层扩展技术为分片(Sharding)。分片是传统数据库行业中的水平扩容技术,引入到区块链中,通过将一个区块链网络分割成多个较小的片区,每个片区独立处理该片区的交易,以提升整个网络的吞吐量。

分片的内涵包括了网络分片、交易分片、计算分片和状态分片,各种分片都是以网络分片为基础的,并且实现难度逐级递增。在提升性能的同时,分片技术带来的片区之间的通信消耗及单个片区被作恶者控制的隐患等也为该方案的应用带来了挑战。典型的应用了分片技术的项目包括Ziliqa[29]等。

(3) 共识层

共识层的扩展主要是通过提出各种新的共识协议提升区块链的运行效率。

3.3 Layer2扩展

Layer2扩展指的是链下扩展方案,其主要的思想是在主链之外进行技术改进,将最终结果同步到主链上。该层的扩展方案目前主要分为状态通道、侧链、跨链等。

(1) 状态通道

状态通道是指在链下建立专属通道进行通信或交易,仅将最终的结果同步到主链上。这种方式便于将高频小额类交易移至链下进行,间接地提升了区块链系统的吞吐量,并降低了主链的存储量。

但该种技术目前也还面临着节点中心化、易遭受流动性攻击以及其本身的扩展性等问题。主要的项目包括基于比特币的闪电网络[30]、基于以太坊的雷电网络[31]及Celer Network[32]等。

(2) 侧链

与状态通道相比,侧链之于主链的独立性又进了一步,直接建立了新的链。该项技术由比特币的核心贡献者于2014年提出[33]。通过侧链,使用双向锚定技术,在不影响主链的情况下进行协议升级或引入新型服务。其具体的实现模式可分为单一托管模式、联盟模式、SPV模式、驱动链模式、混合模式等。比较典型的应用项目有Liquid①、Rootstock、BTC Relay、Lisk、Plasma等。

(3) 跨链

跨链技术可以使两个独立的账本实现资产、数据等的互操作。其核心要解决的问题是,如何实现互不信任的区块链账本的互通。其主要的实现模式包括公证人模式、侧链/中继、分布式私钥控制、哈希锁定及混合技术等。经典的跨链项目包括Cosmos[24]、Polkadot[34]、Wanchain、Fusion等。

3.4 其他扩展

区块链是一门建立在加密技术之上的技术,其基础架构中的各层都有加密技术的应用。因此,除了围绕数据传输、链上、链下的各种扩展方案外,围绕加密及隐私计算相关的问题也有不少扩展技术,如同态加密、安全多方计算、零知识证明、环签名、群签名、混币等技术,这些技术均期望达到在不泄露参与各方隐私、不依赖可信第三方的前提下,安全地完成计算或交易等。

4　挑战与趋势

4.1 挑战

区块链技术未来发展的关键挑战主要来源于以下几个维度:系统安全、数据隐私、监管、扩展性、跨链协议、链下信息及存储。

系统安全:从软件系统角度来看,区块链技术包含了不同层次上的软件载体,如:客户端软件、智能合约、分布式应用、共识算法、虚拟机、网络通信模块等等。由于程序代码缺陷的不可避免性,区块链软件也同样面临着巨大的系统安全风险。例如,2016年以太坊智能合发生的The DAO攻击,来源于相关合约代码中的“重入漏洞”,而这一攻击也造成了超过5000万美元的财产损失。宏观上来说,因为区块链技术的应用场景往往直接与各类数字资产关联,任何系统漏洞被利用攻击都有可能造成无法挽回的财产损失和市场秩序混乱。

数据隐私:大量区块链的应用场景都有重要的数

①Liquid: https://blockstream.com/liquid/

据隐私保护需求。例如,区块链供应链金融应用中,交易订单信息只能在与交易相关的有限企业内共享,否则会引发商业机密的泄露以及不公平交易的现象。然而,当前主流区块链技术为了保证数据、交易的可信,利用分布式账本技术在网络内进行了数据、计算的重复验证,因而提高了保护数据隐私的难度。

监管:区块链技术的现有架构,有限程度上保证了部分监管合规性,如利用智能合约实现检测异常交易等监管逻辑。然而,在更广义的现实场景下的监管需求,目前难以得到有效支撑。如何高效的保证区块链交易、数据符合法律法规、行业规范、风控模型等特定监管规则,是区块链实现大规模落地应用的另一大挑战。

扩展性:随着区块链逐渐走向主流应用场景,大规模计算需求所带来的扩展性瓶颈将越来越显著。大量网络节点同步、海量交易都将成为区块链提高扩展性并成为新一代信息基础设施的关键障碍。

跨链协议:区块链技术的发展很有可能在应用生态上衍生出"一个行业一条链,多链共存"的情形。如何保证不同链之间的信息高效、可信流转和互通,是打通多个区块链及上层应用的关键问题。

链下信息:数据在链上、链下分治的情形在区块链应用中很普遍。然而,很多应用场景需要获取相应的链下信息并完成计算任务。这种情况下,区块链技术对链下信息的可信、一致性提出了较大挑战。

存储:由于区块链技术的基本设计原则是账本数据无法删除,使得账本数据不断膨胀。同时,由于区块链的安全可信相当程度上是建立在众多网络节点对账本的冗余备份之上,这愈发加重了数据存储上的挑战,让如何有效进行区块链数据分布式的存储和管理成为了重要的技术问题。

4.2 发展趋势

区块链技术的发展趋势主要有如下几个方面。

在区块链编程语言设计方面,一个技术研究趋势是,如何进一步强化区块链技术的开发支持,包括设计新的编程语言、开发已有语言的区块链SDK等,从而在软件开发的生命周期中降低区块链开发的复杂度、提高开发效率。在智能合约方面,当前主流开发语言包括Solidity、C++、JavaScript等,这些语言在安全性、隐私性角度的支撑都相对较弱。因此,正如Facebook在Libra项目中提出的Move语言一样,未来新的安全智能合约语言将会是新的研究重点。此外,智能合约语言是否需要做到图灵完备也会成为重要的讨论点。领域性强的非图灵完备语言同样是可能的研究趋势之一。

在密码学实用化方案方面,当前大量的密码学技术被应用在区块链技术架构的实践探索中,用以增强区块链的隐私保护能力,如同态加密、混淆电路、门限签名、零知识证明、安全多方计算等。这些技术在算法层次提供了强大的机密性以及平台通用性,然而在实践中,通常会引入很大的开销。因此,这一问题上的未来技术研究热点可能是如何基于密码学技术,提出实用化的实践方案。

在区块链性能优化方面,作为当前区块链大规模应用的主要瓶颈之一,性能优化在下一阶段仍将成为关键的技术研究点。具体而言,区块链未来可能的性能提升点包括:高性能区块链架构设计、应用导向的高效共识协议及优化、可并行的交易处理引擎、网络通信加速技术等。

在分布式存储方面,针对当前区块链数据膨胀难以管理、查询能力较弱的问题,未来的相关研究方向将重点面向分布式存储技术展开。FISCO-BCOS[36]区块链提出的AMDB可以认为是这一方向上的初步尝试。如何保证分布式存储数据的一致、完整、可信,并且与现有区块链架构有机结合都是重要的技术研究点。

在监管科技和合规协议方面,区块链应用与数字资产的强相关性,意味着监管、合规必将成为区块链技术的核心要点。如何在区块链中内嵌对于反洗钱、反恐怖主义融资等通用监管需求,如何构建标准化的数据合规协议,保障区块链技术在主流场景中得以应用,将成为重中之重。

参考文献

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [R]. Manubot, 2019.

[2] 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.

[3] 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
Yuan Y, Wang F Y. Blockchain: the State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016,42(4): 481-494

[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.
Shao Q F, Jin C Q, Zhang Z, et al. Blockchain: Architecture and Research Progress[J]. Chinese Journal of Computers, 2018. 41(5): 969-988.

[5] Merkle R C. Protocols for Public Key Cryptosystems[C]//

1980 IEEE Symposium on Security and Privacy. IEEE, 1980: 122-122.
[6] Merkle R C. A Digital Signature Based on a Conventional Encryption Function[C]//Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1987: 369-378.
[7] Szydlo M. Merkle Tree Traversal in Log Space and Time[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2004: 541-554.
[8] De La Briandais R. File Searching Using Variable Length Keys[C]//Papers Presented at the March 3-5, 1959, Western Joint Computer Conference. 1959: 295-298.
[9] Brass P. Advanced Data Structures[M]. Cambridge: Cambridge University Press, 2008.
[10] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger[J]. Ethereum Project Yellow Paper, 2014, 151(2014): 1-32.
[11] Christofides N. Graph Theory: An Algorithmic Approach (Computer Science and Applied Mathematics)[M]. Academic Press, Inc., 1975.
[12] Churyumov A. Byteball: A Decentralized System for Storage and Transfer of Value[J]. URL https://byteball. org/Byteball. pdf, 2016.
[13] Popov S, Moog H, Camargo D, et al. The Coordicide[J]. 2020.
[14] Baird L, Harmon M, Madsen P. Hedera: A Public Hashgraph Network & Governing Council[J]. White Paper, 2019, 1.
[15] Brown R G, Carlyle J, Grigg I, et al. Corda: An Introduction [J]. R3 CEV, August, 2016, 1: 15.
[16] Cachin C. Architecture of the Hyperledger Blockchain Fabric[C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016, 310: 4.
[17] Maymounkov P, Mazieres D. Kademlia: A Peer-to-Peer Information System Based on the Xor Metric[C]//International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002: 53-65.
[18] Van Renesse R, Dumitriu D, Gough V, et al. Efficient Reconciliation and Flow Control for Anti-Entropy Protocols [C]//Proceedings of the 2nd Workshop on Large-Scale Distributed Systems and Middleware. 2008: 1-7.
[19] Lamport L. The Part-Time Parliament[M]//Concurrency: The Works of Leslie Lamport. 2019: 277-317.
[20] Lamport L, Shostak R, Pease M. The Byzantine Generals Problem[M]//Concurrency: the Works of Leslie Lamport. 2019: 203-226.
[21] Castro M, Liskov B. Practical Byzantine Fault Tolerance [C]//OSDI. 1999, 99(1999): 173-186.
[22] Pass R, Shi E. Hybrid Consensus: Efficient Consensus in the Permissionless Model[C]//31st International Symposium on Distributed Computing (DISC 2017). Schloss Dagstuhl-Leibniz-Zentrum Fuer Informatik, 2017.
[23] IO E O S. Eos. Io Technical White Paper[J]. EOS. IO (accessed 18 December 2017) https://github. com/EOSIO/Documentation, 2017.
[24] Kwon J, Buchman E. Cosmos: A Network of Distributed Ledgers[J]. URL https://cosmos. network/whitepaper, 2016.
[25] Buchman E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains[D]. , 2016.
[26] Szabo N. Smart Contracts: Building Blocks for Digital Markets[J]. EXTROPY: The Journal of Transhumanist Thought, (16), 1996, 18: 2.
[27] Klarman U, Basu S, Kuzmanovic A, et al. Bloxroute: A Scalable Trustless Blockchain Distribution Network Whitepaper[J]. IEEE Internet of Things Journal, 2018.
[28] Marlin Labs . Design and Analysis of a Decentralized Relay Network[J]. URL https://www.marlin.pro/whitepaper, 2019.
[29] ZILLIQA Team. The ZILLIQA Technical Whitepaper[J]. Retrieved September, 2017, 16: 2019.
[30] Poon J, Dryja T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments[J]. 2016.
[31] Network R. What is the Raiden Network[J]. 2018.
[32] Dong M, Liang Q, Li X, et al. Celer Network: Bring Internet Scale to Every Blockchain[J]. arXiv preprint arXiv: 1810.00037, 2018.
[33] Back A, Corallo M, Dashjr L, et al. Enabling Blockchain Innovations with Pegged Sidechains[J]. URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 2014, 72.
[34] Wood G. Polkadot: Vision for a Heterogeneous Multi-chain Framework[J]. White Paper, 2016.
[35] FUSION FOUNDATION . An Inclusive Cryptofinance Platform Based on Blockchain[J]. FUSION Whitepaper, 2017.
[36] FISCO. Financial Blockchain Open Source Platform[J]. FISCO BCOS Whitepaper, 2017.