·论坛 / PERSPECTIVE·

关于区块链原理及应用的综述

姚忠将[1,2]，葛敬国[1*]

1. 中国科学院信息工程研究所，北京 100093
2. 中国科学院大学，北京 100049

摘 要： 近几年比特币价值逐年上升，能在其他电子货币中脱颖而出，主要得益于其低层技术——区块链。区块链为比特币提供去中心化性、开放性、安全性、独立性和匿名性的基础技术。区块链也随着比特币的升值，相关研究日益广泛深入。本文深入分析区块链基本原理，并剖析一些基于区块链技术的开源项目，给出了部分有代表性的应用领域研究成果。

关键词： 比特币；区块链；共识机制；IoT；BaaS；5G；AI；大数据

doi: 10.11871/j.issn.1674-9480.2017.02.001

A Summary of the Theory and Application of BlockChain

Yao Zhongjiang[1,2], Ge Jingguo[1*]

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: In recent years, the value of bitcoin has risen year by year, and it can stand out in other electronic currencies, mainly due to its low level technology - blockchain. BlockChain provides the basic technology for bitcoin to provide centrality, openness, security, independence and anonymity. With the appreciation of bitcoin, the research of blockchain is more and more extensive. In this paper, the basic principle of blockchain is deeply analyzed, and some open source projects based on blockchain technology are analyzed, and some representative application fields are given.

Keywords: Bitcoin; BlockChain; consensus mechanism; IoT; BaaS; 5G; AI; big data

---

基金项目：国家科技重大专项“5G 与信息中心网络 (ICN) 融合技术研发”(2017ZX03001019)；中国科学院科技服务网络计划 (STS) 项目“5G 网络关键技术研发与验证”

***通讯作者：**葛敬国 (gojingguo@iie.ac.cn)

引言

随着比特币的蓬勃发展，比特币所特有的解决完整性、安全性、真实性的底层技术——区块链——迅速进入研究人员的视野。区块链技术在节点间互不信任的前提下，通过数字签名的交易链、包含前驱区块hash的区块链和共识机制共同保证交易数据的完整性、不可否认性和安全性。伴随着比特币的持续发展，区块链的重要性也逐渐被发现，被认为是对计算机行业乃至整个社会的颠覆性技术。

2008 年中本聪 (Satoshi Nakamoto) 在《Bitcoin: A Peer-to-Peer Electronic Cash System》[1] 中描述了区块链的概念。因其具有以下特性而得到广泛关注：

- 去中心化。区块链技术不依赖第三方机构或硬件设施，没有中心管制。
- 开放性。区块链技术是开源的，数据对所有人开放，任何人都可以通过公开接口查询区块链数据和开发相关应用。
- 独立性。基于协商一致的规范和协议，所有节点能够在系统内自动安全地验证、交换数据，不需要任何人为的干预。
- 安全性。只要不能掌控全部数据节点的51%，就无法肆意操控修改网络数据。
- 匿名性。除非有法律规范要求，各节点身份信息无需公开或验证。

目前高校、科研机构及公司在金融、医疗行业进行了广泛深入的研究。2017 年新书《块数据 3.0：秩序互联网与主权区块链》认为区块链通过超级账本技术、智能合约技术和跨链技术建立起一套共识和共治机制，这套机制通过编程把时间、空间、瞬间多维叠加所形成的数据流加以固化，形成可记录、可追溯、可确权、可定价、可交易的技术约束力。2016 年 9 月国际标准化组织 ISO[2] 成立了区块链和分布式账本技术委员会 ISO/TC 307，并在 2017 年 4 月召开的 ISO/TC 307 第一次工作会议上，成立了七个工作组和研究组。

区块链的研究已经不局限于电子货币、银行等金融机构，在安全、医疗管理、信息安全、5G 应用、IoT (Internet of things)、AI 等领域也展开深入广泛研究。

本文在引言中描述了区块链相关背景和特性，然后通过第 1 节概述区块链技术的原理；第 2 节介绍区块链的典型开源项目；第 3 节中介绍当前针对区块链的研究方向和未来的应用领域；最后，第 4 节 给出对本文的总结。

1　区块链概述

区块链的创新之处不仅在于区块链技术的设计思想，更在于形成以区块链为中心的生态圈。在文献 [3] 中详细描述了比特币应用中形成的局部生态圈，包括发行、验证、流通等。现在区块链已经不仅局限于代币，还涵盖金融、医疗、教育、网络、安全、隐私、云存储、大数据、人工智能等领域。图 1 显示以区块链自身的安全运转支撑消费、医疗、教育[4]、智慧城市[5] 等领域高可靠高效率运作，形成超大规模生态圈。

1.1　区块链原理

研究区块链首先要了解区块链架构。袁勇曾在 [6] 中提出六层架构。Imfly 在 [7] 中提出三层区块链架构。谢铉洋在 [8] 提出三层模型。这几种架构虽然按照模块划分了层次，但有的整体的层间关系并不明确，有的在今天的应用中某个层次或者模块并非必需。因此本文重新分析总结出图 2 区块链架构模型。区块链架构基本分为三层：基础层、驱动层和应用层。基础层是区块链的生态基础，位于最下层，包括去中心化的对等网络及其承载的生成、验证并存储数据的数据层。驱动层用于上层应用驱动基础层的网络和数据工作，从而驱动区块链架构的运转。驱动层包括共识机制、激励机制和智能合约。应用层位于架构最顶端，包括专有应用和基于通用服务平台的应用。

1.1.1　基础层

1.1.1.1　网络层

区块链节点互连形成网络，每个节点具备数据传输、验证功能。节点间通过 Peer-to-Peer 两两互连形成一张没有固定拓扑结构的松散网络。每个节点

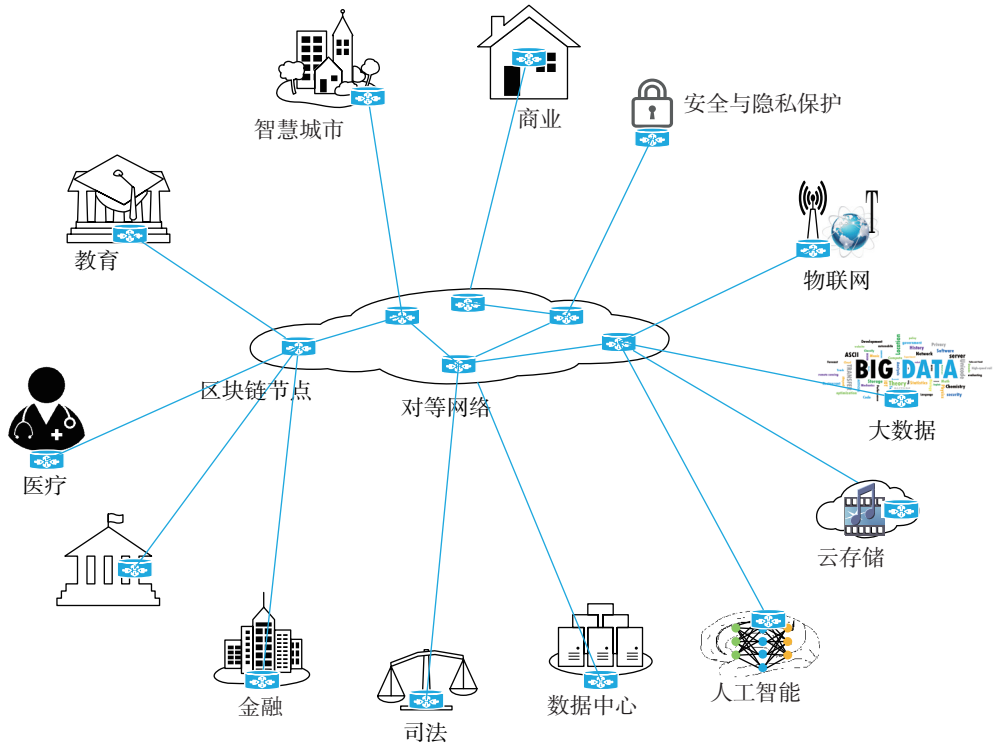

图1　区块链生态

Fig. 1　BlockChain ecology

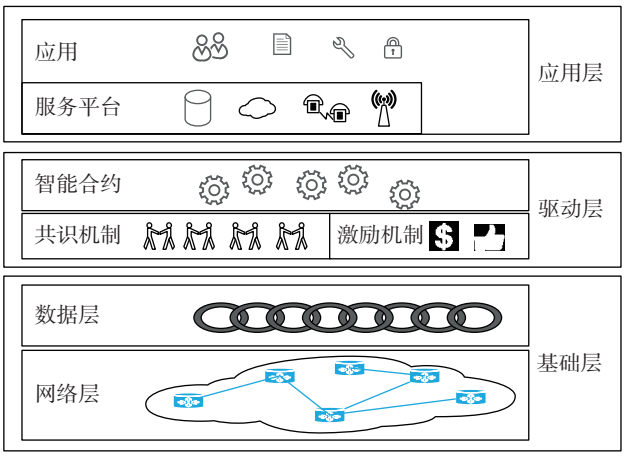

图2　区块链层次架构图

Fig. 2　BlockChain hierarchy

都具有泛洪式路由功能，保证交互信息和区块全网传播。节点具有验证能力，确保接受数据正确性，保证网络传播信息的正确性和可靠性。区块链节点都可以自由加入或者离开区块链系统，不影响区块链正常运行；区块链节点都是平等通信，不经过中间实体；区块链节点有权独立处理收到的数据，不受干扰。

(2) 广播协议

区块链网络需要广播两种数据：交互信息和区块信息。两种信息的广播协议是相似的。信息广播不需要发送者信任任何网络节点。如图 3 所示发送者产生的交互记录或区块向多个邻接节点传播。近似指数级

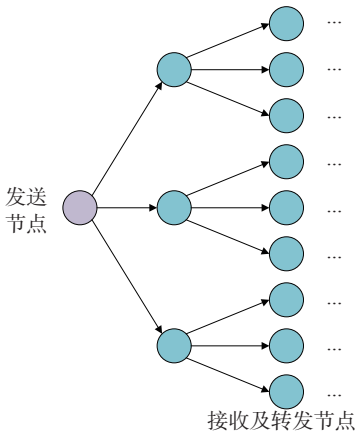

图3　信息传播过程

Fig. 3　The Way of information dissemination

的广播过程，可以使信息在数秒时间内扩散至整个网络。每个交互记录或区块都要通过有效性验证才能往继续传播，并返回给发送者验证通过的信息；否者，丢弃信息并返回给发送者一条拒绝信息。

对等网络中每个节点都存储一个交互记录池，也存储有一份区块链的副本。对于接收到的交互记录或区块可以独立验证区块的有效性，并自决交易区块的去留。验证如下公式所示。如果接受信息，则将其放入记录池或者连到区块链尾部，并开始新的记录收集或者区块挖掘。

$$\text{Verify}(\varepsilon, \vartheta, \varphi, \delta)$$

其中 ε 表示交易或者区块的数据结构，ϑ 表示字段取值是否在合理范围，φ 表示交易或者区块中的输入输出对应关系是否正确，δ 表示交易或者区块是否存在过。

1.1.1.2 数据层

交互记录

交互记录是一种数据结构，用于记录交互信息。交互记录中包含交互响应者 A 的签名、发起者 B 的公钥、输入信息、输出信息等。交互记录并未在数据结构中指明前驱交互记录和后继交互记录，仅利用交互的公钥和签名确定逻辑上授权关系。因此每一次交互都是相互独立的，仅在逻辑层面形成链式关系。图 4 描述了交互记录的链式信息逻辑关系。

图 5 是交互记录统一的数据结构，指明了版本信息，包含了时间戳服务，明确了输入输出的数量和信息。输入信息中包含输入交互的指针、输出交互的索引以及解锁脚本。输出信息包含交互数据、锁定脚本。由于节点相互缺乏信任，交互记录中不包含接收者或者持有者的任何账户或者身份信息。

区块结构

区块是区块链的组成单元，由区块头和区块体组成。如图 6 所示区块头又可以分为三部分：前驱区块哈希；基本信息部分，包含版本号、时间戳、困难值和随机值等信息；梅克尔树根 hash。每个区块中的前驱区块哈希指明上个区块的信息，逐级包含，形成区块链结构；基本信息中的时间戳确定区块生成时间，困难值动态调整区块挖掘时间，难度值越小挖掘时间越久。梅克尔树 [9] 是位于区块体的主要数据部分，叶子节点是记录信息，中间节点是对下层两个节点的哈希。梅克尔树结构保证了数据的真实性、安全性和不可抵赖。目前有多种树结构的升级，最具代表性的是基于 Redix 树 [10] 的梅克尔 • 帕特里夏树 [11]。

区块链结构

区块链数据结构是单向链式结构，如图 7 所示每个区块都有指向前一区块的指针。区块链通过新区块共识解决分叉问题，保证主链唯一。

非对称加密及哈希算法

非对称加密算法和哈希算法是区块链技术的基础，保证不可信网络的安全需求和验证需求。哈希算法用于生成前驱区块地址、记录信息摘要、交互者地址和构造梅克尔树数据结构等。以比特币账户地址生成过程为例如图 8。非对称加密算法用于信息加密、签名和认证。椭圆曲线加密算法 (ECC，Elliptic Curve

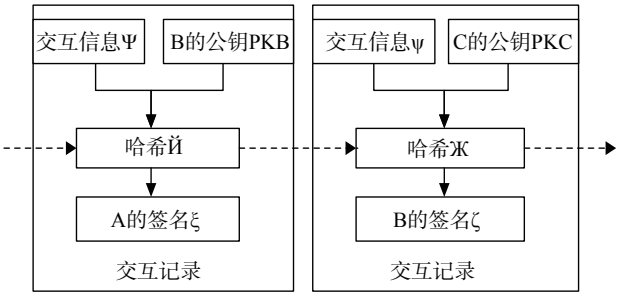

图4 链式信息逻辑关系

Fig. 4 Chain of information logic

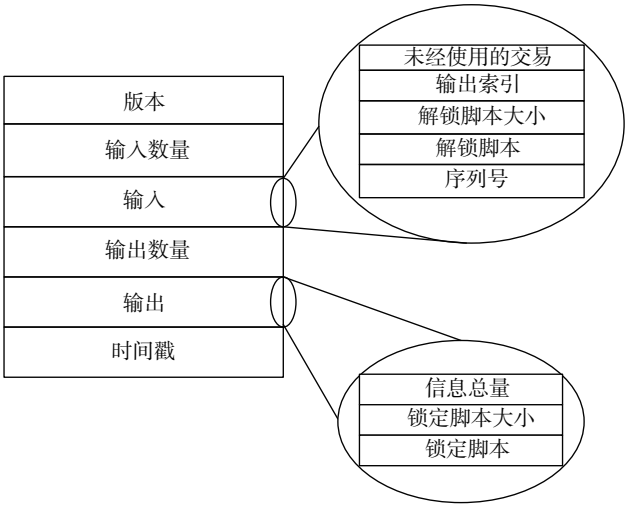

图5 交易信息数据结构

Fig. 5 Data structure of transaction

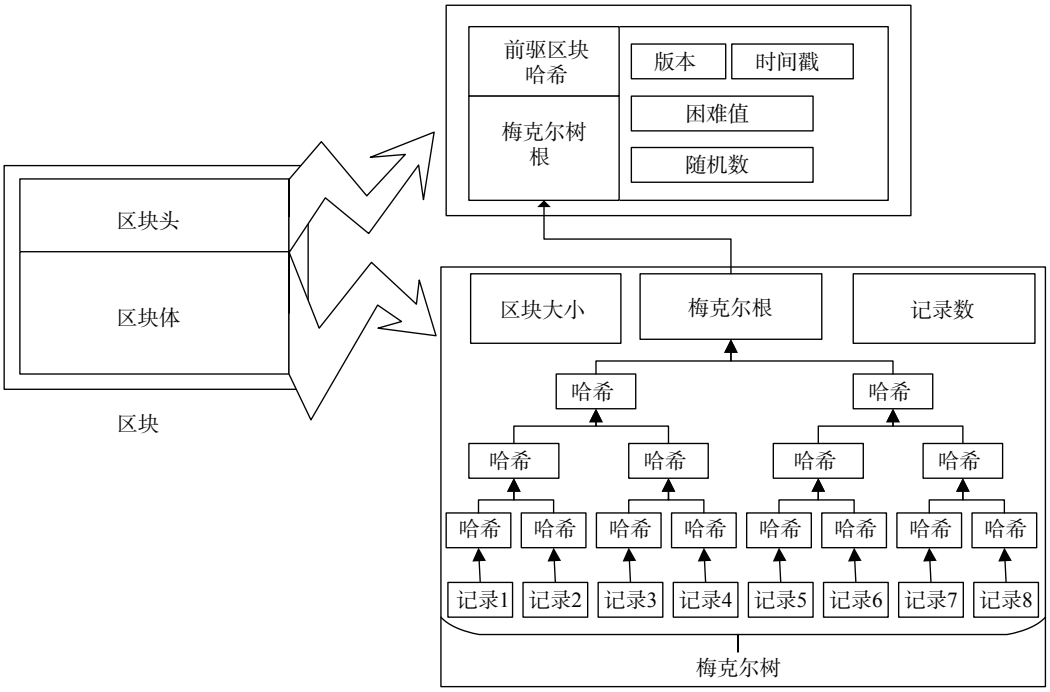

图6　区块数据结构

Fig. 6　Data structure of block

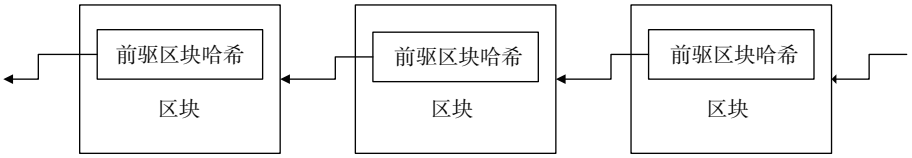

图7　区块链式数据结构

Fig. 7　Data structure of Block Chain

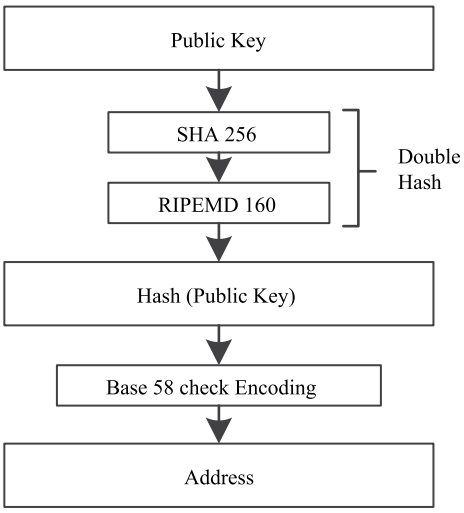

图8　比特币地址生成过程

Fig. 8　Bitcoin address generation process

Cryptography) [12] 是目前认为最安全的加密算法之一，PKI、OpenSSL 等也开始采用 ECC 算法。椭圆曲线取模形成有限的离散点集合 (阿贝尔群)，ECC 是基于离散集合对数问题的非对称加密算法。图 9 简要描述了 ECC 密钥产生及加解密过程。

1.1.2　驱动层

1.1.2.1　共识机制

点对点的去中心化网络中节点之间互相缺乏信任，各自无法可信操作，如何在决策上达成正确共识使所有节点一致行动，称为拜占庭将军问题 [13]。拜占庭将军问题不仅要有行动一致，而且要求正确性。

(1) 拜占庭将军问题

拜占庭将军问题针对一致性和正确性提出两个条件：

椭圆曲线加密算法生成公私钥对

第一步：
A选择一条椭圆曲线E(α, β)，然后在曲线上随机选择一个点作为基点Σ
第二步：
随机选择一个整数Θ作为私钥，生成公钥
Ξ=Θ·Σ

使用椭圆曲线加密算法公私钥对加解密

第三步：
A2 发送E(α, β)、Ξ、Σ 给B
第四步：
B1通过将明文编码到E(α, β)上的Ω点产生Φ
第五步：
B计算：C1=Ω+Φ·Ξ，C2=Φ·Σ
第六步：
B发送C1和C2给A
第七步：
A计算C1−Θ·C2, 解码Ω得到明文

图9　椭圆曲线加密算法

Fig. 9　Elliptic curve cryptography

IC1：所有忠诚的副官遵守一个命令，即一致性。

IC2：若司令是忠诚的，每个忠诚的将军遵守司令发出的命令，即正确性。

IC1 和 IC2 是解决拜占庭将军问题的充分条件。如果有将军持有不同意见，可以以司令身份表达自己观点，寻求协商一致。解决拜占庭将军问题有两种经典算法：口头协议和书面协议。

1) 口头协议

口头协议必须满足三个条件：

A1：每个发送的消息都能够正确传递；

A2：接收者知道谁发送的消息；

A3：可以检测到消息的缺失。

任意 m，如果总共有大于等于 3m 个将军并且最多 m 个反叛者，那么算法 OM (m) 满足条件 IC1 和 IC2。图 10 给出了 OM (m) 算法的具体过程。

2) 书面协议

书面协议在添加了签名，因此增加了第四个条件：

A4:

a) 忠诚将军的签名不可伪造，任何对签名信息的修改都可以被检测到。

b) 任何人都可以验证将军的签名认证。

书面协议算法假设一个函数 choice() 从一系列命令中选择一条命令，这一函数需要满足下列条件：

OM(0)算法：
1) 司令向每一个副官发送命令。
2) 每个副官使用接收到的司令命令；如果没有收到命令则默认使用RETREAT。
OM(m)算法，m > 0：
1) 司令向每个副官发送命令。
2) 对于每个副官i收到的司令命令为vi,如果没有收到司令命令则为RETREAT。副官i在算法OM(m-1)中作为司令发送vi给其他n-2个副官。
3) 对于每个副官i和副官j(j≠i)，vi是副官i从副官j收到的步骤2) OM(m-1)中的命令；否则使用RETREAT。副官i使用majority（vi,⋯,vn-1）计算的结果。

图10　口头协议算法 OM (m)

Fig. 10　The oral message algorithms OM (m)

SM(m)算法：
Initial　Vi=Ø
1) 司令向每一个副官发送经签名的命令。
2) 每个副官i:
(a) 如果副官i收到司令发来的v : 0形式的消息，并没有收到任何其他命令，那么：
(i) 副官i使Vi等于{i}；
(ii) 副官i向其他每个副官发送消息v : 0 : i。
(b) 如果副官i收到一条形如v : 0 : j_1:⋯ : j_k并且v不在集合Vi中，那么：
(i) 副官i将v加入到Vi中；
(ii) 如果k<m，那么副官i发送消息v : 0 : j_1:⋯: j_k:i到除j_1,⋯, j_k外的任何副官。
3) 对于每个副官i：当副官i不再收到消息，则开始运算choice(Vi)。

图11　书面协议算法 SM (m)

Fig. 11　The signed message algorithm SM (m)

OM(m,p)算法：
0) 从司令的邻接副官中选择一个包含p个副官的规则集合N。
1) 司令向N中的每个副官发送命令。
2) 对于每个N中的副官i，vi表示副官i从司令那里收到的命令，如果没收到则为RETREAT。副官i发送按照下面的规则向其他每个副官k发送vi:
(a) 如果m=1，通过发送沿着定义1中(A)(ii)中确保存在的路径γ i, k 发送命令。
(b)如果m>1，那么作为算法(m−1, p−1)中的司令，使用从G中移除源司令获得的将军图。
3) 对于每个副官k和每个N中的副官i(i≠k)，vi是步骤2)中副官k从副官i那里收到的命令，如果没有收到则为RETREAT。副官k使用majority (v_{i_1}, ⋯ ,v_{i_p})其中N={i_1,⋯, i_p}计算的结果。

图12　丢失通信路径的口头协议算法 OM (m, p)

Fig. 12　Oral message algorithm OM (m,p) when missing communication paths

1. 如果集合 V 由唯一元素 v 组成，那么 choice (V) = v。

2. choice(Ø)=RETREAT，其中 Ø 是空集合。

图 11 中 x:i 表示由将军 i 签名的命令 x；v:j:i 表示 v 表示将军 j 签名的命令，v:j 表示由将军 i 签名。SM (m) 算法中每个副官i维护一个包含目前收到的所有签名命令的集合 V_i。注意区别集合 V_i 和收到的消息集合，可能很多不同消息包含同一个命令。

对于任意 m，如果最多有 m 个反叛者，SM (m) 算法解决拜占庭问题。

3) 丢失通信路径的情况下对口头协议和书面协议算法的扩展

改进口头协议

定义1：

(a) 如果一个节点集合 $\{i_1, \ldots, i_p\}$ 满足以下条件就被认为是节点 i 的规则邻居集：

(i) 每个 i_j 是 i 的邻居。

(ii) 对于每个不同于 i 的将军 k，存在多条从 i_j 到 k 而不经过 i 的路径 $\gamma_{(i,k)}$，这样除了节点 k 之外任何两条路径不存在相同节点。

(b) 如果一个图 G 中每个节点都有一个由 p 个不同节点组成的规则邻居集 (邻居数相同) 那么图 G 就被认为是 p-regular。

为了解决在 3m-regular 将军图中有 m 个叛徒的拜占庭将军问题，扩展 OM (m) 算法为 OM (m，p) 算法，此算法要求将军图 G 必须是 p-regular 图。具体算法如图 12 所示。对于任意 m>0，p≥3m，如果有最多 m 个反叛者，算法 OM (m，p) 可以解决拜占庭将军问题。

改进书面协议

对于拜占庭将军最弱的连接假设是忠诚将军互连形成的子图，在这种假设下 SM (n-2) 是一种解决算法，其中 n 是忠诚将军和反叛将军总数。但是，仍然需要修改算法让将军们只发送命令到他们能够接收到的地方。具体说就是在 SM (m) 算法的第一步，司令只向邻居副官发送签名的命令，在第二步的 (b)，副官 i 只向不在 j_r 的每个邻居副官发送命令消息。

对于图的维度最小值为 d (任意两节点之间最多 d 条弧线) 的更通用结果，对于任何 m 和 d，如果最多有 m 个反叛者，而忠诚将军构成子图维度为 d，那么算法 SM (m+d-1) 解决了拜占庭将军问题。

所以，拜占庭将军问题的根本思想是少数服从多数，如果某一观点支持者过半，则采用这种观点。

(2) 共识机制扩展

区块链中针对拜占庭将军问题提出共识机制 [14]。候选区块构建后消耗大量“资源”“挖矿”，挖矿成功后，矿工在区块上签名并广播出去。接收者验证新区块挖矿结果和签名，有效则停止自己本次挖矿并将区块链接在区块链尾部，开始新的区块挖掘。根据拜占庭将军问题思想只有网络中 51% 以上的节点验证通过的区块才被接受，这就是共识过程。51% 的控制权确保恶意者在可预见时间内调用最大资源无法掌控。由于区块链的特性，恶意者必须把区块链中的同等“资源”重新调用一遍才能实现篡改，但往往超过所能获得的利益。

PoW (Proof-of-Work) [15-16] 是比特币的区块链采用的共识算法。每个节点接受上一区块后开始为新区块计算区块头 hash 值，直到满足困难值为止，具体过程如图 13 所示。PoW 的出现结合了货币发行、交

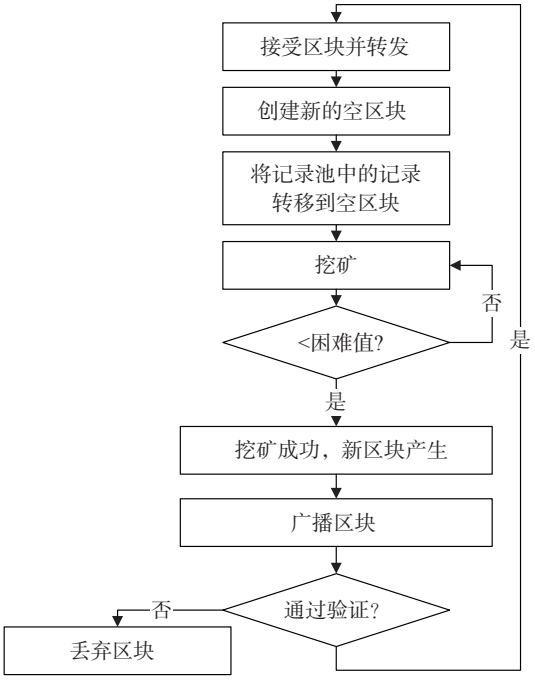

图13　共识过程

Fig. 13　Consensus Process

易支付和验证功能。PoW 主要依赖节点设备算力。PoW 有个弊端：设备越先进、计算能力越强，越容易掌握更多的财富。

PoS (Proof-of-Stack)[17]，又称权益证明，是 PeerCoin 低层区块链使用的共识机制。PoS 机制将难度值与币龄绑定 (两者呈反比关系)，节点获得记账权的难度就和币龄相关。PoS 相对于 PoW 来说减少了资源消耗，提高了节点性能，但不准确性导致其易受攻击干扰。DPoS (Delegate Proof-of-Stack)[18]，又称股份授权证明，是BitShares社区提出的一种共识机制。股份授权证明机制是为了解决 PoW 和 PoS 存在的问题提出的一种新的保障加密货币网络安全的算法。DPoS 机制中所有节点根据股份权益 (币龄) 投票的方式选出得票最高的 101 个记账代表负责交易的打包和挖矿，减少记账和验证者的数量。

Ripple 共识机制 RPCA (Ripple Proof-of-Consensus Algorithm)[19]，是 Ripple 协议的支撑技术。Ripple 是开源的金融交易互联网开放协议，支持随时免费的任何币种的去中心化交易。Ripple 共识机制依靠特殊节点投票，只有超过 51% 的特殊节点同意才算达成共识。Ripple 机制效率非常高，是共识机制的技术突破。

PBFT[20] 最初出现在 MIT 的 Miguel 和 Barbara Liskov 的学术论文中。拜占庭容错机制通过三个阶段的不断验证最终达到 commited 状态后才表示达成共识，期间允许对验证结果的误判。但是 PBFT 机制当仅剩 33% 节点在运行时就会停止工作。

除以上共识机制外，还有 Casper 共识[21]，Pool 验证池[22]，授权拜占庭容错 (delegated BFT，dBFT)[23]、消逝时间量证明 (Proof-of-Elapsed Time，PoET)[24]、Quorum Voting 共识[25] 等圄于代币的共识机制，也有传统的一致性算法，比如 Paxos 算法[26] 和 Raft 共识[27] 等。目前来看由于这些共识算法各有优缺点，但是都面临资源的消耗和共识速率问题。

2.1.2.2 激励机制

市场逐利而聚。为了保证区块链的持续性和吸引力，有些系统提出了激励机制：一方面制定代币发行机制 (仅限支持代币形式的区块链系统)，另一方面价值均衡机制，吸引更多节点加入参与区块挖掘。

代币发行机制主要是支持本区块链的所定义的电子货币的发行策略。只有让代币流通才能实现代币的价值。但是具体的如何发行有不同的策略：一种作为矿工奖励，劳有所得；一种是货币兑换，属于投资的一种手段。

价值均衡一方面扩大区块链系统的影响，让更多的参与者有利可图才有吸引力，才能有更大的市场价值；另一方面价值再分配，保证价值均衡，区块链系统也是一个小型金融系统，只有价值均衡才能保证系统健康运转。常见策略有 PPLNS (Pay per last N shares) 和 PPS (Pay per share)。

1.1.2.2 智能合约

智能合约是形成信息逻辑链式关系的基础，也是下层信息逻辑链式关系和上层服务的桥梁。智能合约是交易双方的自担保协议，交易方 A 向 B 提出交易条件，交易 B 给出信息，若满足则完成交易信息的传递授权，否则，放弃交易。智能合约从根本上来说是一段程序代码，是运行中因等待所需数据或者行为而被阻塞的一个线程。

协议

智能合约是部署在记录内的信息传递服务程序。比特币交易数据结构中的锁定脚本和解锁脚本组合是智能合约雏形。如图 14 所示，交互方 A 有锁定脚本，要求 B 提供解锁相关的信息，B 通过解锁脚本提供信息与 A 达成合约。最简单的协议：其中一方提出条件，另一方满足要求，双方达成一致形成合约关系。智能合约雏形是非图灵完备的。随着研究的深入，已经研发出越来越多图灵完备的合约脚本。

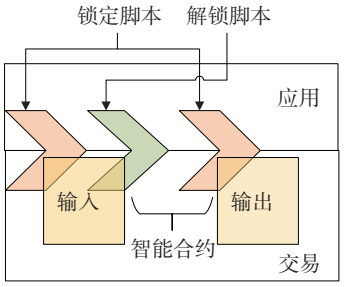

图14 智能合约应用位置

Fig. 14 The location of smart contract

Lock Script：°F (PubKey，Signature)

Unlock Script：℃ (PubKey，Signature)

模块化

模块化是现代程序设计的趋势，有利于代码重用和软件升级更新。对所有模块化的合约使用相同的 Interface，无论实现怎样的功能，信息传递的过程中都可以调用相同的 interface 获得需要的合约功能。利用统一的 interface，可以根据不同的需求替换不同的合约功能模块，或者由多个合约模块组装成一个大的智能合约系统，其中合约模块可以自定义组装。

1.1.3 应用层

应用层包含服务平台和应用。服务平台是对低层数据和计算工具的结合，用于为上层具体应用业务提供服务。目前服务平台主要由具体区块链应用公司独立开发，与应用耦合性强，缺乏通用性。也有部分科技公司开始致力于通用平台的开发，比如微软的 Azure BaaS、IBM 的 Hyperledger 等。应用层主要用于具体服务，比如银行的账目记录、医疗信息管理等。第 2、3 部分将详细介绍部分代表性服务产品和应用。

2 相关开源项目

2.1 以太坊

以太坊 (Ethereum) [28-29] 对区块中树的结构数量优化改进，提高了扩展性、安全性和灵活性。数据结构上采用 Merkle Patricia 树 [30]，这种是一种存储键值对的加密认证数据结构，是基于 Radix 树改进的 Trie 前缀树：(1) 将中间节点原来的内存地址改为子节点的 hash 值，然后利用 RLP 编码 sha3 hash 作为 key；(2) 引入多种节点类型，提高处理效率。以太坊不同对象使用不同的树：交易树，收据树，状态树。三种树各有分工，分别处理不同的事件。交易树处理交易信息，比如交易是否发生过，记录在哪个区块，交易查询等；收据树负责所有的行为的记录；状态树处理关于账户有效性、账户余额等信息。如图 15，以太坊还提供了一个良好的上层服务/应用开发平台：图灵完备的脚本语言 (EVM语言，Ethereum Virtual Machine code)，丰富的开发模块。上层分布式应用通过 Web3.js 调用智能合约，完成操作。

图15 以太坊架构

Fig. 15 Ethereum architecture

2.2 Adept

Adept 系统 (Autonomous DEcentralized Peer to Peer Telemetry) [31-32] 是 IBM 将区块链应用于物联网的尝试。考虑到未来 IoT 规模复杂庞大，集中管理不现实 [33]，区块链的问世给去中心化的管理互联网事物 (Internet-of-Things) 带来新的解决方案。

ADEPT 中通过分析当前无线网络、传感器网络、ad hoc 网络共存的问题，提出了三个关键解决方案组件：(1) P2P 去中心化网络：P2P 网络解决了单点失效问题，提高了网络鲁棒性。(2) P2P 消息和分布式文件传输：P2P 消息方法没有中心化的代理或者数据控制器，这种方法的关键特点是：1) 不可靠；2) 保证交付下的低时延；3) 存储转发消息到其他互连设备。分布式文件共享利用 DHT 使去中心化的数据共享，BitTorrent 就是非常有名的案例。(3) 自主设备的协调：P2P 网络需要设备具备自组织能力并基于协调获得共识。

ADEPT 中很多节点基本没有计算能力和存储能力来管理区块链，而有些则具备这种能力。因此依据资源能力，将架构模型分为三个等级：Light Peer、Standard Peer、Peer Exchange。图 16 仅以 standard peer 为例给出 ADEPT 逻辑架构。

2.3 超级账本

超级账本 (Hyperledger) [34]，最初是 IBM 研发的 Open Blockchain 项目，后来将全部代码捐献给 Linux

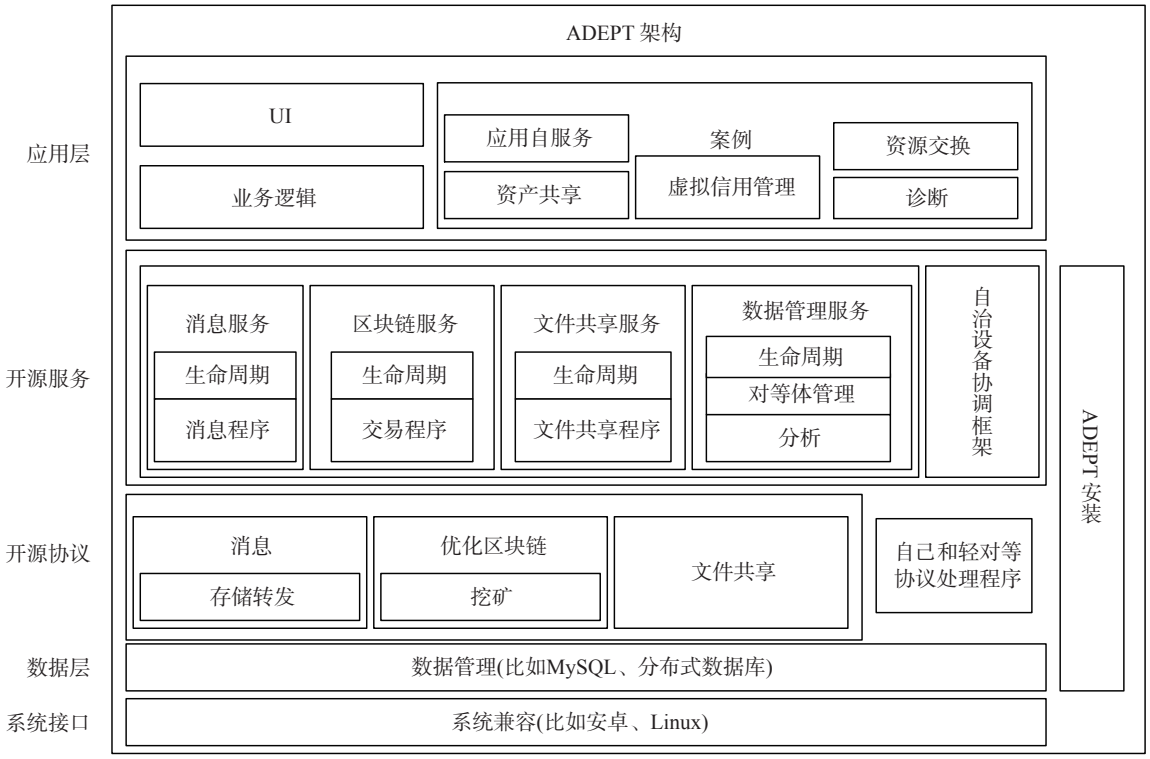

图16　ADEPTStandard Peer 逻辑框架

Fig. 16　The logic architecture of ADEPT standard peer

Foundation 下的 HyperLedger 项目形成当前的超级账本。根据超级账本的设计目标，不同领域需要不同的网络，不同的网络构建不同的区块链以便支持和服务不同的领域。超级账本白皮书 [35] 中罗列了未来可能支持的区块链应用领域：金融市场网络、全球贸易市场网络、局部财务管理等。

超级账本满足多种网络共同的属性：身份标识明确资产从属关系与交易行为人、利用切断身份和交易的联系提供隐秘交易、加密获得合约机密性、增值系统的可移植性、不同服务间互操作特性等。图 17 给是超级账本的整体架构，在对等网络的基础上提供成员关系服务、策略服务、区块链服务和 Chaincode 服务。成员关系服务管理网络中的身份标识、隐私和机密。策略管理服务负责访问控制策略、联盟策略、共识策略等非确定性策略机制。区块链服务通过 P2P 协议管理建立在 HTTP/2 上的分布式账本。智能合约服务提供安全运行环境、智能合约管理等功能。

3　区块链的研究与应用

3.1　安全

3.1.1　网络安全

区块链可以解决去中心化问题，防止单机构对系统拥有独立控制权，恶意篡改系统中信息。区块链节点间都是相互独立。为保证系统正常、安全运行，引入了共识机制，保证所有节点对某一事件的发生达成共识。

安全性是区块链得以发展的支柱，所以不断有人去研究。虽然区块链已经在安全方面展开了应用并取得了一定成果，但区块链本身仍存在安全问题。Ghassan 等人在 [36] 中分析了区块链安全规定并指出其中的薄弱之处：首先，安全。1) 快速支付不足以阻止“双花”攻击，尽管基于PoW的时间戳机制可以验证“双花”，但是验证周期长不适合快速支付。验证尚未结束，用户已获得了商品。2) 恶意主机可以阻止区块和交易的发送到受害节点。其次，扩展性。目前

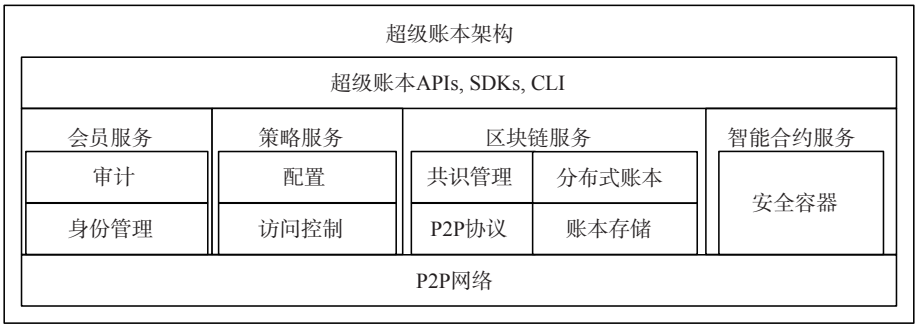

图17　超级账本的框架

Fig. 17　The architecture of hyperledger

区块链每秒处理的交易数为 7 笔，当网络节点不断增加，用户不断增多，必将对扩展性造成限制。最后，去中心化的限制：基于 PoW 的共识机制给去中心化引入漏洞，某些矿工可能集中网络中计算力形成对整个系统的控制。不仅区块链本身的设计思想，区块链的实现工具也存在安全隐患。Michael Coblenz 等人在文献 [37] 中发现脚本语言 Solidity 设计的智能合约 bug 非常多，因此设计了 Obsidian。

Hyperledger 提出基于策略服务的安全机制与区块链安全特点结合，基于策略的安全机制利用访问控制对系统和数据形成安全保护。文献 [38] 提出 Security Management Provider 负责基于内容的固定策略或者动态的策略的访问控制，用于控制数据和设备的访问。Ali Dorri 在文献 [38] 中提出分布式可信 (Distributed Trust) 概念。分布式可信确保收到的区块有效，减少区块验证负载。起初用户 Ψ 没有交易历史，被认为是恶意的，但是 Ψ 的交易都经过 PubKey 完成验证；然后，每个 Cluster Head 基于直接或者间接证据维护其他 Cluster Head 的可信率。直接证据是 ξ 可以通过 PubKey 直接验证数据是 ψ 产生，则 ξ 信任 ψ，如果 ξ 不能直接验证 ψ，但是多签名交易有多个 Cluster Head 签名，则 ξ 间接信任 ψ。这是一种比较新颖的想法，也有研究者希望通过这种方法评估网络链路的信誉度以评判是否从此链路路由。

3.1.2　隐私保护

安全可以保护数据不被非法使用，但不能阻止数据被观察，因此隐私保护也是区块链应用研究的重要环节。比特币提出隐私保护策略，旨在将用户钱包账户和交易间的联系匿名。《精通比特币》第四章给出匿名解决方案：为钱包提供不同的公钥地址，并基于动态公钥地址思想给出分层确定性钱包概念，利用种子为钱包衍生大量私钥，产生不同公钥，经过 hash 生成不同钱包地址。每一次交易使用一个新的地址，达到匿名目的。Yves-Alexandre de Montjoye 等人在文献 [39] 中提出加入噪声的聚合方法保护用户隐私。但是文献 [39] 可能导致服务不准确，Ali Dorri 在文献 [38] 中做了改进，通过创建 Overlay Network，在这个 Overlay 中提出隐私区 (Privacy Zone) 概念保护不同类型数据隐私，不同 PrivacyZone 有不同检查策略。

3.2　网络

3.2.1　5G 应用

当前 5G 研究主流思想是应用 SDN/NFV 技术实现。文献 [40] 中提出 KSI 使用全局区块链为 SDN 提供低层的安全保障。[41] 提出通信服务提供商应用区块链提供数据通信服务，管理服务，包括一些核心操作等。CSPs (Communications service providers) 将会看到区块链对其核心管理系统、邻接服务和降低消耗方面的重大影响，为 5G 提供新的接入方案。Catherine Mulligan 博士将在 2017 年于伦敦做过一个关于区块链重新定义 5G 研发的演讲。中国科学院信工所、声学所等与侯自强老师提出将区块链应用于 5G 与 ICN 融合，为网络提供计费、管理、安全等服务。项目仍处于研发阶段，将不断有新的研究成果和新的观点产生。

3.2.2 IoT

IBM 在比特币流行之初已经开始研究并形成利用区块链解决物联网的问题，在 ADEPT 中逐渐成熟的文档 [33, 42]。文献 [42] 提出 Empowering the edge 的思想，将区块链作为 IoT 去中心化的边缘增强方案的一个研究方向。在区块链中实时记录智能设备的运行状态，不仅保证设备的正常通信，而且有利于故障设备的跟踪维护维修。在文献 [33] 中提出 Device Democracy 的概念，认为未来的大规模多互连的场景中，对于 IoT 必须使用去中心化的管理方式获取高效可靠的设备管理效果。Zheng Yan 在文献 [43] 中提出 IoT 的可信管理。在这篇文章中提到 IoT 中的不同事物 (包括用户、数据、身份标识、传输、通信等) 的可信管理和隐私保护。文献 [40] 中提出 TO-BE——针对 IoT/M2M 的区块链自管理 P2P 网络。其中一个应用案例形成自管理物流网络、自管理产品网络、自管理的能源网络，三者之间形成全局的互联互通。

3.3 服务

服务主要是指用于为公司、科研机构、个人等上层用户使用具体业务提供支持的接口、平台或者应用，如图 18 可以具体到某一个行业，比如金融、医疗等等。业务属于最顶层的应用，具体业务由服务支撑。

3.3.1 BaaS

Baas (Blockchain as a Service) 是科技公司希望利用区块链提供类似 IaaS、PaaS、SaaS 的供广大用户使用的服务平台。IBM 最早提出 BaaS 的概念，并在 2016 年推出 BaaS。微软在 2014 年开始区块链领域的研究，2015 年联合 Consens Ys 推出了基于云的区块链技术平台，并于 2016 年开放了基于 Azure 平台 sandbox 区块链服务。用户可以简单高效的为区块链搭建虚拟机测试环境，降低开发成本。目前基于 Azure 平台的 BaaS 已经可以提供支持 26 种不同区块链实现的服务。Tencent 最近也成立的独立的区块链部门，致力于打造金融机构联盟区块链云服务。Google 和 Amazon 在 2016 年也加入了 BaaS 的争夺战。作为一种新的服务平台，BaaS 成为互联网公司争夺的新战场，从侧面反映出 BaaS 的重要性。

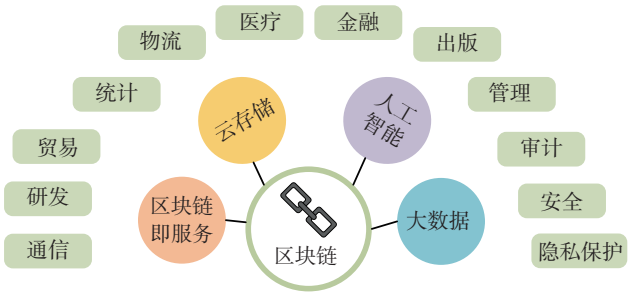

图18 服务范围缩略图

Fig. 18 Service area

3.3.2 云存储

在云存储领域，与区块链的结合目前尚处于起步阶段，参与研究的机构寥寥可数。但是区块链安全性和去中心化的巨大优势与云存储的结合将是必然的。目前基于区块链的云存储产品是 Storj [44]，一款源自开源项目 Metadisk 的产品。Storj 有媲美大多数高端云存储的可靠性。Storj 宣称可以达到 99.99999% 的可靠性，但是成本只有传统云存储的 1-2%。尽管这样的“物美价廉”，但是代表性产品屈指可数，这恰恰说明区块链在云存储方面的价值。

3.3.3 AI

AI 近几年以前所未有的速度发展，与区块链不分伯仲。IBM 于 2016 年将区块链技术与 AI 产品 Watson 融合。2017 年初，Google 子公司 DeepMind Health 借助人工智能和区块链涉足英国医疗机构。虽然 Watson 和 DeepMind Health 提出将两者用于融合的方案，但对两者的应用仍停留在“划江而治”的层面：区块链在低层提供安全保障，AI 提供业务上的处理。资深 AI 研究人 Trent 在 2015 年到现在不断思考 AI 与区块链的互补和融合可能性，并撰写了大量文章。Trent 借助 DAO 项目发表了三篇有关 AI 与区块链的文章 [45-47]，并提出 DAO 应该具有访问资源、征用资源、拒绝干涉的能力。Trent 还提出了三种将 AI 与 BlockChain 结合的实现途径：AI 负责区块链的智能合约边缘；AI 负责区块链的智能合约中心；集群自动表现 AI 复杂性。

3.3.4 大数据

大数据在计算机网络领域和社会生活中提供越来越多的服务，然而安全问题却一直没有的到有效的解

决。信息泄露称为当前网络环境中的重要安全隐患。目前的主流思想是结合两者优势：大数据内容丰富，统计分析能力强；区块链安全性高，可以保证数据的安全性、可靠性和完整性。2016 年 Trent 发表的文章 [48] 中思考区块链与大数据的融合。大数据和区块链有很多共同之处：分布式的计算与基于 P2P 网络去中心化；MapReduce 与共识机制；HDFS 和区块等。当前有两种结合方法：1) 在区块链上实现大数据，将大数据的统计分析等技术应用到区块链上；2) 将区块链技术嫁接到大数据平台，将区块链的安全、不可更改特性移植到大数据平台。具体哪种方法更有效，能够获得更好的融合效果，需进一步研究。

4 总结

区块链基本原理的研究是所有工作的基础。理解了区块链工作原理才能在区块链上进一步研究。虽然目前有很多对区块链的优化研究，但是对区块链固有的难题并没有彻底解决。Zooko 三角难题 [49] 就是区块链面临的一个难以完全克服的问题。不同方向之间相互影响，获取其中某一特性就要降低甚至舍弃其他特性。因此如何解决或者平衡好区块链的三角难题才能更好的优化区块链。

当前最广泛应用研究主要集中在安全、网络和服务。安全方面主要是问责、隐私保护、路由路径安全评估等。但是目前隐私保护由于保护的隐私内容不同、范围不同，提出的方法各种各样。路由路径安全评估，也称信誉评估，是全新方向，但却是保证网络安全的重要方法。网络方面主要将区块链集中在 5G 和 IoT 领域。5G 提供低层安全策略、隐私保护策略，网络管理、计费、新网络服务接入平台等。这些研究尚处概念阶段，对于深入理解实现有不少挑战。IoT [50-51] 主要研究对终端设备的管理、隐私保护，并在 ADEPT 上实现，但是未来有更多新型智能设备，新型服务需要提供，因此仍有大量工作需要做。对于服务的研发，目前金融服务是最成熟的，医疗服务由于主要利用区块链公共账本功能，实现难度相对较小。BaaS、云存储等方面的应用研究，尤其是人工智能方面面临巨大挑战。

区块链本身具有去中心化、安全、独立等优势，潜力非常巨大。对区块链的深入挖掘、与新领域的融合和周边应用扩展将是研究的重点。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[2] International Organization for Standardization [OL]https://www.iso.org/home.html.

[3] Andreas M. Antonopoulos. Mastering Bitcoin [M]. O'Reilly Atlas, 2013.

[4] Sharples M, Domingue J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward[C]//European Conference on Technology Enhanced Learning. Springer International Publishing, 2016: 490-496.

[5] Biswas K, Muthukkumarasamy V. Securing Smart Cities Using Blockchain Technology[C]//High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE, 2016: 1392-1393.

[6] 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.

[7] imfly, Node.js开发加密货币[E/OL] https://www.gitbook.com/book/imfly/bitcoin-on-nodejs/details

[8] 中国人民银行合肥中心支行科技处课题组, 谢铉洋. 区块链结构、参与主体及应用展望[J]. 金融纵横, 2017(1).

[9] Merkle Trees[OL] http://en.wikipedia.org/wiki/Merkle_tree.

[10] Redix Tree[OL] https://en.wikipedia.org/wiki/Radix_tree

[11] Merkle Patricia Tree[OL] https://github.com/ethereum/wiki/wiki/Patricia-Tree.

[12] 椭圆曲线密码学[OL]https://zh.wikipedia.org/wiki/%E6%A4%AD%E5%9C%86%E6%9B%B2%E7%BA%BF%E5

%AF%86%E7%A0%81%E5%AD%A6.

[13] Lamport L, Shostak R, Pease M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, 4(3): 382-401.

[14] 共识机制[OL] https://yeasy.gitbooks.io/blockchain_guide/content/bitcoin/consensus.html.

[15] Proof-of-Work[OL] https://en.bitcoin.it/wiki/Proof_of_work.

[16] Proof-of-Work[OL] https://en.wikipedia.org/wiki/Proof-of-work_system.

[17] PoS [OL]https://bytecoin.org/blog/proof-of-stake-proof-of-work-comparison/.

[18] DPoS White paper[OL]https://bitsharestalk.org/index.php?topic=4031.0.

[19] Ripple Consensus[OL]https://ripple.com/build/ripple-ledger-consensus-process/.

[20] PBFT Algorithm[OL] http://pmg.csail.mit.edu/papers/osdi99.pdf.

[21] Ethereum Mauve Paper[online] http://8btc.com/forum.php?mod=viewthread&tid=40113.

[22] Pool验证池[OL] http://blog.csdn.net/jeffrey__zhou/article/details/56672948.

[23] delegated BFT Algorithm[OL] http://www.8btc.com/onchain-paper-antshares.

[24] Crypto 2.0 Musings - Proof of Elapsed Time[OL] https://www.linkedin.com/pulse/crypto-20-musings-proof-elapsed-time-alex-batlin.

[25] 中国区块链技术和应用发展白皮书[OL] http://odbyaalgf.bkt.clouddn.com/%E4%B8%AD%E5%9B%BD%E5%8C%BA%E5%9D%97%E9%93%BE%E6%8A%80%E6%9C%AF%E5%BA%94%E7%94%A8%E5%8F%91%E5%B1%95%E7%99%BD%E7%9A%AE%E4%B9%A6-2016.pdf.

[26] Paxos Algorithm[OL] https://zh.wikipedia.org/wiki/Paxos%E7%AE%97%E6%B3%95.

[27] Raft Algorithm[OL]https://raft.github.io/.

[28] ethereum official website[OL]https://ethereum.org/.

[29] Patricia-Tree[OL] https://github.com/ethereum/wiki/wiki/Patricia-Tree.

[30] ethereum-whitepaper [OL]http://ethfans.org/posts/ethereum-whitepaper.

[31] ADEPT Whitepaper[OL]http://8btc.com/doc-view-489.html.

[32] IBM ADEPT Practictioner Perspective - Pre Publication Draft - 7 Jan 2015 [OL]https://archive.org/stream/pdfy-esMcC00dKmdo53-_/IBM%20ADEPT%20Practictioner%20Perspective%20-%20Pre%20Publication%20Draft%20-%207%20Jan%202015#page/n7/mode/2up.

[33] Device democracy: Saving the future of the Internet of Things[OL]http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF.

[34] hyperledger official website[OL] https://www.hyperledger.org/.

[35] hyperledger-whitepaper[OL] https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/edit#heading=h.m6iml6hqrnm2.

[36] Karame G. On the Security and Scalability of Bitcoin's Blockchain[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 1861-1862.

[37] Coblenz M. Obsidian: a safer blockchain programming language[C]//Proceedings of the 39th International Conference on Software Engineering Companion. IEEE Press, 2017: 97-99.

[38] Dorri A, Kanhere S S, Jurdak R. Towards an Optimized BlockChain for IoT[C]//Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. ACM, 2017: 173-178.

[39] Yves-Alexandre de Montjoye, Erez Shmueli, Samuel S Wang, and Alex SandyPentland. 2014. openpds: Protecting the privacy of metadata through safeanswers.PloS one 9, 7 (2014), e98790.

[40] Guardtime KSI Use of a globally distributed blockchain to secure SDN whitepaper [OL]https://

www.ciosummits.com/Guardtime_KSI_Use_of_a_globally_distributed_blockchain_to_secure_SDN_whitepaper_1602.pdf.

[41] Microsoft Azure BaaS[OL]https://azure.microsoft.com/en-us/solutions/blockchain/.

[42] Empowering the edge: Practical insights on a decentralized Internet of Things[OL]https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf.

[43] Yan Z, Zhang P, Vasilakos A V. A survey on trust management for Internet of Things[J]. Journal of network and computer applications, 2014, 42: 120-134.

[44] Storj official website[OL]https://storj.io/.

[45] AI DAOs, and Three Paths to Get There[OL] https://blog.bigchaindb.com/ai-daos-and-three-paths-to-get-there-cfa0a4cc37b8?gi=28320cd870d8#.8btx9jds3.

[46] Wild, Wooly AI DAOs[OL] https://blog.bigchaindb.com/wild-wooly-ai-daos-d1719e040956#.qquk7dsbs.

[47] The AI Existential Threat: Reflections of a Recovering Bio-Narcissist[OL] https://medium.com/@trentmc0/the-ai-existential-threat-and-the-bandwidth-scenario-4573c1cb085f#.8x4rgi4nc.

[48] Blockchains for Big Data[OL] https://blog.bigchaindb.com/blockchains-for-big-data-from-data-audit-trails-to-a-universal-data-exchange-cf9956ec58ea.

[49] Zooko's triangle[OL]: http://en.wikipedia.org/wiki/Zookos_triangle'.

[50] Dorri A, Kanhere S S, Jurdak R. Towards an Optimized BlockChain for IoT[C]//Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. ACM, 2017: 173-178.

[51] Bitcoin official website[OL]https://bitcoin.org/en/.

收稿日期：2017 年 1 月 20 日

姚忠将：中国科学院信息工程研究所，博士研究生，主要研究方向为网络体系结构、问责与隐私保护。
E-mail: *yaozhongjiang@iie.ac.cn*

葛敬国：中国科学院信息工程研究所，博士，博士生导师，研究员，主要研究方向为网络体系结构、未来网络。
E-mail: *gejingguo@iie.ac.cn*