计算机科学
COMPUTER SCIENCE

区块链跨链技术发展及应用

孙浩，毛瀚宇，张岩峰，于戈，徐石成，何光宇

引用本文

孙浩，毛瀚宇，张岩峰，于戈，徐石成，何光宇. 区块链跨链技术发展及应用[J]. 计算机科学, 2022, 49(5): 287-295.

SUN Hao, MAO Han-yu, ZHANG Yan-feng, YU Ge, XU Shi-cheng, HE Guang-yu. Development and Application of Blockchain Cross-chain Technology[J]. Computer Science, 2022, 49(5): 287-295.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210800132

区块链跨链技术发展及应用

孙 浩[1] 毛瀚宇[1] 张岩峰[1] 于 戈[1] 徐石成[2] 何光宇[2]
1 东北大学计算机科学与工程学院 沈阳 110169
2 东软集团股份有限公司技术与战略发展事业部 沈阳 110179
(704825130@qq.com)

摘 要 随着区块链技术的不断发展与创新,大量基于区块链的应用不断诞生,如今的区块链系统大多是异构且不互联的,链与链之间无法进行直接的价值流通,这在很大程度上限制了区块链的功能拓展与发展空间。跨链技术指在不同区块链系统实例之间交换信息,并对交换的信息加以利用,实现区块链之间的互联互通和价值转移。文中首先介绍了区块链跨链技术的发展历程,详细介绍了公证人机制、侧链中继、哈希锁定和分布式私钥控制4种当前主流的跨链技术;接着,基于上述跨链技术,介绍了几种当前的主流跨链项目与应用;最后,通过对比几种跨链技术在信任模型、安全性、原子性和可扩展性等不同性能上的异同,总结分析了当前跨链技术的发展趋势,并探讨了跨链领域面临的难点问题和今后的发展方向。

关键词:区块链;跨链技术;公证人机制;侧链中继;哈希锁定;分布式私钥控制
中图法分类号 TF315

Development and Application of Blockchain Cross-chain Technology

SUN Hao[1],MAO Han-yu[1],ZHANG Yan-feng[1],YU Ge[1],XU Shi-cheng[2] and HE Guang-yu[2]
1 School of Computer Science and Engineering,Northeastern University,Shenyang 110169,China
2 Neusoft Corporation,Shenyang 110179,China

Abstract With the continuous development and innovation of blockchain technology,a large number of blockchain-based applications have been generated. Today's blockchain systems are mostly heterogeneous and not interconnected,and there is no direct value circulation between chains. This greatly limits the functional expansion and development of blockchains. Cross-chain technology refers to the exchange of information between different blockchain system instances and the use of the exchanged information to achieve interconnection and value transfer between blockchains. Firstly,this paper introduces the development process of blockchain cross-chain technology,and introduces in detail four current mainstream cross-chain technologies including the notary mechanism,the side chain relay,the hash lock and the distributed private key control. Then,based on the above-mentioned cross-chain technology,it further introduces several current mainstream cross-chain projects and applications. Finally,by comparing the similarities and differences of several cross-chain technologies in trust model,security,atomicity,scalability,etc.,the current development trend of cross-chain technology is summarized and analyzed,and the difficulties and future development direction in the field of cross-chain are discussed.

Keywords Blockchain,Cross-chain technology,Notary mechanism,Side chain relay,Hash lock,Distributed private key control

1 引言

区块链是一种由多方共同维护,使用密码学[1]来保证传输和访问安全,能够实现数据一致存储、难以篡改且防止抵赖的记账技术,也称为分布式账本技术[2-3]。区块链在近十年的发展中出现了3次重要的技术演进:1)以比特币[4]为代表的加密数字货币应用将区块链技术引入人们的视野;2)以以太坊[5]为代表的可编程区块链平台为将区块链应用于各个领域提供了可能;3)以Hyperledger Fabric[6]和Hyperchain[7]为代表的企业级区块链平台使区块链技术能够真正被应用于商业环境。

2008年中本聪针对比特币发表了题为"Bitcoin:a peer-to-peer electronic cash system"的论文。该文提出了一种电子现金系统,其实现的点对点技术使得支付双方进行交易时,可以不通过任何第三方权威金融机构的支持与验证。这篇启蒙之作使区块链和比特币系统开始迅速升值,区块链的应用

到稿日期:2021-08-16 返修日期:2022-02-04
基金项目:辽宁省重点研发计划(2020JH2/10100037);东软集团股份有限公司开放课题(NCBETOP2001)
This work was supported by the Key R&D Program of Liaoning Province(2020JH2/10100037) and Open Program of Neusoft Corporation (NCBETOP2001).
通信作者:于戈(yuge@mail.neu.edu.cn)

不仅限于金融应用，更可以应用于非金融应用，例如公共服务、信誉系统和安全性验证等。

随着区块链技术的持续发展与创新，大量基于区块链的应用不断诞生[8]，区块链所面临的问题也日益显现出来。如今的区块链系统大多是异构且不互联的，具有不同特点的大量区块链系统形成了大量的价值孤岛，链与链之间无法进行直接的价值流通，这在很大程度上限制了区块链的功能拓展与发展空间。

本文主要介绍了当前的区块链跨链技术与相关应用，总结分析了跨链技术的发展趋势与跨链领域面临的难题，为相关研究和开发人员提供了系统性的参考。本文第1节简要介绍了区块链与跨链技术的背景；第2节介绍了跨链技术的发展历程，详细介绍了4种主流的跨链技术；第3节介绍了几种有代表性的跨链项目，包括 The Interledger Protocol，Cosmos 和 Plasma 等；第4节主要分析和对比了几种典型跨链技术的性能，提出了跨链技术发展的难点问题，并对跨链技术进行了总结与展望；最后总结全文。

2 跨链技术的分类与发展

跨链技术指在不同区块链系统之间交换信息，进行必要的转换（如转换货币价值），完成交易，并对所交换的信息加以利用，实现区块链之间的互联互通与价值转移的技术[9]。跨链技术的主流方法有4种：公证人机制、侧链/中继、哈希锁定和分布式私钥控制。

在区块链发展初期，区块链技术的重点是以单链研发与优化为主[10]，直到2012年，Ripple[11]实验室提出了跨链 Interledger Protocol（ILP）协议[12-13]，两个不同的系统通过该协议可以互相自由地转换货币，而不需要信任任何个人或者机构，从此跨链技术开始进入人们的视野。2013年5月，Collado 提出原子转移[14]（也称原子交换），构建了原子式跨链交易的技术方案，该方案升级后成为了如今的哈希锁定[15]技术。2014年，Blockstream[16]首次提出侧链的概念，通过双向锚定机制，实现了主链和侧链之间的资产转移，解决了主链的性能瓶颈，达到了拓展功能的目的。2015年2月，闪电网络白皮书[17]发表，其提出哈希锁定的方法，开拓了比特币微支付通道，实现了区块链实时海量交易网络。2016年5月，以 BTC-Relay[18]为代表的中继跨链模式出现，实现了以太坊对比特币数据的跨链访问。同年6月，Tendermint 团队研究并实现了一个支持跨链交互的异构网络 Cosmos[19]，并提出了跨链通信 IBC 协议与 Tendermint[20]共识引擎。2017年8月，闪电网络的发明人 Poon 提出了 Plasma[21]的区块链扩展设计模式，所借鉴的大数据并行计算框架 MapReduce 可使区块链运算及更新效率提升至每秒10亿量级，随后 Poon 又在此基础上提出了最小可行的 Plasma 模式和修改版 Plasma Cash[21]等改进方法。

目前，许多区块链跨链平台正处于研究的初期阶段，很多技术难题亟待攻克，但链与链之间的互联互通已经成为区块链的必然发展趋势[22]。

2.1 公证人机制

公证人机制[23]是基于 Interledger[24-25]协议创造的一种技术框架，与现实世界中的中介机制类似，其假设交易双方不能互相信任，则引入交易双方共同信任的第三方充当公证人来作为中介，这个或这组受信任的团体既可以自动监听和响应来自链上的交易请求和确认信息，也可以主动对发生的事件或请求进行监听和响应。

公证人机制分为单签名公证人机制、多签名公证人机制和分布式签名公证人机制。单签名公证人机制也称为中心化公证人机制，在此机制下，公证人通常由单一指定的独立节点或者机构充当，它同时承担了数据收集、交易确认和验证的工作。中心化公证人机制的运行处理效率相对较高，这是最简单但也是单点故障风险最高的模式。此系统存在中心化的问题，中心节点的安全性是系统稳定的关键，一旦公证人本身遭受恶意攻击，交易就变得不可信，整个系统就会出现安全漏洞。因此，多签名公证人机制和分布式公证人机制应运而生。多签名公证人机制通常需要由多位公证人在各自的账本上共同签名并达成共识，交易才得以完成。在此机制下，每个节点都拥有各自的密钥[26]，对于一个交易，只有公证人的签名达到一定的数量或比例时，此交易才会被确认。多方签名虽然一定程度上解决了中心化的问题，但需要交易的每条链均支持多重签名。分布式签名公证人机制与多签名公证人机制有一定的区别，其采用多方安全计算[27-28]的思想，安全性更高，但实现难度也更大。

2.2 侧链/中继

在侧链和中继机制中，侧链指另一个具有完全独立功能的区块链系统，它能够主动感知主链信息并采取相应的行动。侧链本质上是一种跨区块链的解决方案，可以实现数字资产从一个区块链到另一个区块链的转移。通过侧链，可以在主链的基础上进行交易监管[29]、隐私保护和智能合约等新功能的添加，在研发新型服务的同时保证了主链的工作不被影响。

侧链的概念首次出现在比特币中。一方面是为了安全地升级比特币协议以增加新功能，防止开发出的新功能在未经安全测试的环境下运行，继而发生严重事故，另一方面还考虑到拜占庭共识协议对链上大规模改动的影响。因此，比特币的核心开发者提出了侧链方案。侧链技术可以实现比特币和其他货币之间的资产转移，用户可以通过访问新的加密货币系统来使用他们已经拥有的资产。由于侧链系统与主链系统相互独立，因此在侧链上的技术创新不受阻碍，侧链上的损害不会影响到主链的性能与安全。

2014年，Back 等比特币核心开发者共同创立了 Blockstream 公司，他们在“Enabling Blockchain Innovations with Pegged Sidechains”一文中，首次提出了“侧链”一词，旨在扩大比特币协议层功能，主导研发侧链的扩展机制。根据他们的定义，这个词被用于分布式系统之间各种形式的具有互操作性的记账。BTC Relay 是在以太坊基金会支持下诞生的，是区块链的第一个侧链系统，其以以太坊网络为系统主链，比特币区块链网络作为以太坊的侧链，通过智能合约将主链与侧链连接起来，方便二者进行货币交换与信息互通，是实现

跨链通信的一次有意义的尝试。

当主链和侧链进行价值和信息交换时，中继器就相当于它们之间的交流通道。中继指将通过侧链与公证机制相结合，完成收集消息、验证消息和转发消息的功能。如果中继器本身就是区块链，那么它亦可称为中继链，中继链更加灵活且易于拓展。目标链收到数据后，进行验证并完成交易确认，此项工作不需要第三方进行认证。根据目标区块链的系统结构的不同，所使用的验证方法也有所差异。中继方法支持跨链资产交换、抵押和跨链合约实现等功能。

中继的形式有很多，Cosmos 中的 Hub、Polkadot 中的 Replay Chain 和 BTC-Relayer 中的 Replayer 等都在跨链系统中扮演着中继的角色。

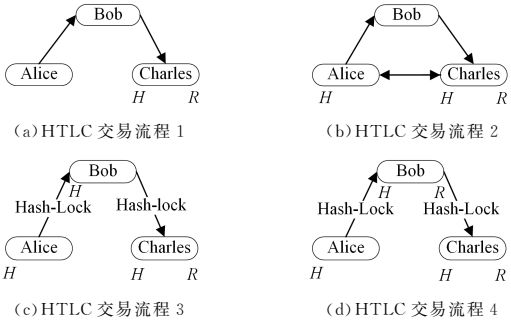
2.3　哈希锁定

哈希锁定[30]是闪电网络中提出的一种技术实现模式，其在闪电网络技术架构中已得到较广泛的应用。闪电网络是哈希锁定技术的典型应用，本质上是一种使用哈希时间锁定的智能合约来安全地进行零确认交易的机制。目前有两种精心设计的智能合约，包括到期序列可撤销合约（Revocable Sequence Maturity Contract，RSMC）以及哈希时间锁合约（Hashed Timelock Contract，HTLC）。

到期序列可撤销合约假定交易对象之间存在一个“微支付通道”，要求交易双方对每一项交易方案进行签名认证。双方均可随时提出提现要求，如果对方无法提出最新版本的交易结果，即可对其进行惩罚。通过该方法，可以限制双方对结果进行篡改。提现成功后，将一系列双方均认可的交易结果写入区块链中。

哈希时间锁定合约使用哈希锁和时间锁来确保交易接收方要么通过生成加密证明在截止日期前确认自己已经收到付款，要么丧失接受付款的能力并将款项返回给交易发起方，同时接收方生成的加密证明也可用于其他支付中的操作。哈希锁定的交易中，交易发起方拥有主动权，是更具优势的一方。

HTLC 为闪电网络等跨链互操作系统提供了微支付通道，参与方的简易交易流程如图 1 所示。



(a) HTLC 交易流程 1　(b) HTLC 交易流程 2

(c) HTLC 交易流程 3　(d) HTLC 交易流程 4

图 1　哈希时间锁定技术的交易流程图

Fig. 1　Transaction flow chart of hashed timelock contract

首先 Alice 为 Bob 打开了支付通道[31]，Bob 为 Charles 打开了支付通道，当 Alice 打算以 S 价格向 Charles 购买商品时，便要打开微支付通道。

如图 1(a)所示，Charles 首先生成一个随机数 R，并以此生成 SHA-256 的哈希散列 H。

如图 1(b)所示，Charles 将生成的哈希散列 H 发送给 Alice；Alice 将 S 价格的货币支付给 Bob，同时将 Charles 发送给她的 H 添加到附加条件中，即要求 Bob 提供生成此哈希散列 H 的数据 R。

如图 1(c)所示，此时 Bob 已经获得 Charles 生成的哈希散列，他向 Charles 支付 S 价格的货币，并将 Alice 的附加条件的副本发送给 Charles。

如图 1(d)所示，若 Charles 想要得到 Bob 的支付，便需要向他提供生成哈希散列 H 的数据 R；Bob 也因此获得了满足条件的数据，通过此 R 便可得到 Alice 的付款。此为一次完整的 HTLC 交易。

2.4　分布式私钥控制

分布式私钥控制是通过私钥生成与控制技术，把加密货币资产映射到基于区块链协议的内置资产模板的链上，然后根据跨链交易信息来部署新的智能合约，从而创建出新的加密货币资产的一种技术，其代表项目有 Wanchain 和 Fusion 等。

为了使原有区块链上的资产在跨链系统中仍然可以交易，分布式私钥控制技术引入了锁定和解锁两个操作。通过锁定和解锁，可以对原有区块链上的代币进行管理权的操作。锁定是对密钥控制的数字货币资产实现分布式的控制权的管理以及对资产的映射操作；解锁是利用已经掌握的分布式私钥对锁定的代币进行解锁操作，使代币由原来的不可操作状态变成现在的可转移、可操作状态。锁定和解锁互为可逆操作。

以 Fusion[32]为例，其利用密码学中的分布式密钥生成算法和门限签名技术，保证了跨链过程中资产的锁定和解锁，由系统参与共识的所有节点决定，并且在此过程中，任何节点或者少数节点联合都无法拥有资产的使用权。以比特币和 Fusion 的交互为例，在锁定阶段，节点 A 向 Fusion 发起锁定资产请求，利用分布式私钥[33-34]生成算法，将密钥碎片随机分发给 Fusion 中的不同节点。智能合约返回私钥对应的公钥地址，A 收到公钥地址之后，将资产锁定在该地址中，智能合约在确认 A 的资产锁定后更新 A 在 Fusion 中的资产信息。在解锁阶段，智能合约锁定 A 在 Fusion 中的资产信息并广播解锁交易的签名请求，持有私钥碎片的节点检查交易后签名，然后将签名后的交易广播到比特币网络，将资产输出到公钥地址。在确认了 A 解锁后，智能合约更新 Fusion 中 A 的资产信息。

3　跨链项目与应用

3.1　Interledger Protocol（ILP）

ILP 是一种用于分类账付款的协议，由 Fugger 于 2004 年启动。该协议提供了跨不同数字资产的分类账系统的路由支付方法，同时隔离发送者与接收者，使他们不需要与对方建立信任链接。拥有两个账目的账户都可以担任此连接器的工作，安全支付和自动路由使得任何发送者和接收者之间都能够被网络联通，减少了不同账目之间的交易障碍[35]。

ILP 并未创建一个统一的“账本”系统，参与交易的各方可以不信任任何第三方个人或者机构，该协议仅依靠现有的“托管”交易来保证各方的利益，避免了中介机构倒闭的风险。托管是实现分类账之间安全支付的主要方法，其可以让每个

参与者都免受支付失败或恶意行为的影响。所有的参与者都依靠自己的账本来托管资金。当一笔托管交易建立时，资金并没有发生转移，只有满足预定的条件后这些资金才会被释放。对于发送方，只有收到了接收方已收到付款的确认后，账目才会保证资金转移；对于接收方，只有在提供上述确认后，账目才会保证将资金支付给他。

ILP 交易的传输状态如图 2 所示。首先参与者提出转账请求，但不对其账目作出任何更改。当账户持有人收到涉及自己的托管操作并对此转账授权后，账目将检查资金的可用性等属性。若资金满足转账的所有规则与限制，则将此资金存放在托管处并准备转账。如果资金满足转账的执行条件，则进行资金转移；如果任何检查条件失败，或是执行被拒绝，则中止转账，账目将被托管的资金返还给发送方。同时可以为托管交易设置超时时间，若在规定时间内没有账目对被托管的交易进行确认或拒绝操作，则此次托管便被视为自动失效。

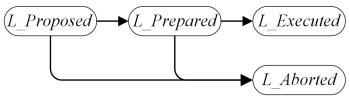


图 2 Interledger Protocol 交易的传输状态

Fig. 2 Transmission status of Interledger Protocol transaction

3.2 Cosmos

Cosmos 是一种支持异构网络的新型区块链网络架构，其使用了 Tendermint 共识算法。Tendermint core 内核为其提供了高性能、安全一致的共识协议。Cosmos 创建了第一个跨链区域 Cosmos Hub，在此区域中，不同区块链均遵守区块链间的通信协议。

Cosmos 提供 IBC(Inter-Blockchain)跨链协议和机制，IBC 通过 Cosmos Hub 为跨链系统的各区域建立相互连接，所有区域间的令牌传输都通过 Cosmos Hub 进行，同时 Cosmos Hub 可以跟踪每个区域持有的令牌总数。Cosmos 可以实现区块链之间的互操作，让资产在区块链之间的转移不依赖于受信任的第三方。

Tendermint 被认为是比特币和以太坊等高能耗 PoW 区块链最可行的替代品之一，该策略将实际的拜占庭容错共识与一种 PoS 证明技术联系起来，动态地选择节点来作为下一块的验证器。Tendermint Core 可以将任何一个应用程序黑盒转变为分布式区块链，不需要了解其具体的运行方式，只需要其有确定结果即可。通过应用程序区块链接口(ABCI)连接到区块链应用程序，用户即可使用任何语言对区块链应用程序进行编程。

Cosmos 是由 Tendermint 支持的许多区块链互联的网络，其允许这些区块链在保持互操作性的同时并发运行。Cosmos Hub 管理着许多独立的区块链，不同区域的区块链持续提交最新块的数据信息，使 Hub 的状态与各个区域保持同步；然后发布 Merkle 证明，将其作为信息发送与接收的证据，以完成信息在各个区域间的流动。这种机制也称为区块链链间通信。

图 3 给出了数据由一个区块链 Zone1 经过 Hub 转移到另一个区域中的区块链 Zone2 的通信过程。发送链可以自由管理发布的数据，发送方需要附加上其区块头信息，以便接收链对接收到的数据进行确认。

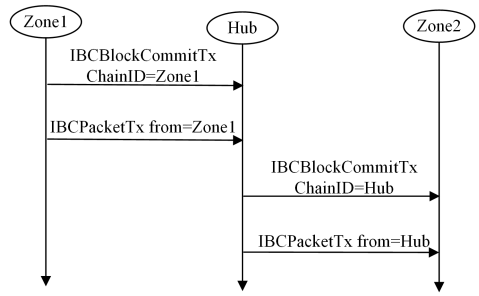


图 3 Cosmos 中各个区域与 Hub 互联的通信过程

Fig. 3 Communication process between each region in Cosmos and Hub interconnection

通过 IBC 机制，将此过程拆分为两个独立的事务：

(1)IBCBlockCommitTx 事务，允许区块链向任何观察者证明其最近的哈希值。

(2)IBCPacketTx 事务，允许区块链向任何观察者证明给定的数据是由发送人的应用程序发布的，此过程可以通过最近块哈希的 Merkle 证明来完成。

3.3 Plasma

Plasma 是一种用于激励和强制执行智能合约的提议框架，其结构是创建经济激励机制，无须合约创建者主动管理，而是通过激励节点本身来自主且持久地运行合约。其每秒 10 亿量级的运算效率使区块链能够高效完成大量的状态更新。Plasma 将区块链与 MapReduce[36] 框架相结合，将所有区块链操作重新划分为一组 MapReduce 函数，此结构可以绑定智能合约以强制执行可伸缩计算。

Plasma 由 5 个关键部分组成：

(1)激励层。使 Plasma 能够以经济高效的方式持续地进行合约计算。

(2)树状结构。通过树状结构排列子链，最大限度地降低成本和提高净交易值。

(3)MapReduce 计算框架。在链中构建状态转移的欺诈证明，使框架与树状结构兼容，并重新定义链上状态，使其高度可扩展。

(4)共识机制。在现有的区块链基础上进行权益证明(PoS)的共识方法，要求维持中本聪提出的共识原则，不进行区块扣留。

(5)Bitmap-UTXO 结构。Plasma 通过此结构确保区块链进行准确的状态转换，同时最大程度地降低批量出口成本。

Plasma 链是区块链中的一条链，该链并不展示区块内容，而是将区块头的哈希提交给根链。根链上存在一系列欺诈证明的智能合约，以减少欺诈行为或非拜占庭行为。如果根链上收到了欺诈证明，则回滚该块并进行处罚。如图 4 所示，灰色方块表示旧块，白色方块表示已经传播并落实到根链上的最新块。Alice 在根链上没有账目余额，只在 Plasma 链上有余额。通过此方法可以达到在 Plasma 链上进行大量交易的同时保证根区块链接收到最少的数据。

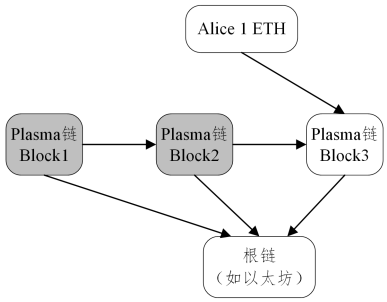


图 4　Plasma 系统中资金在链上的转移过程

Fig. 4　Transfer process of funds on the chain in Plasma system

3.4　Horizon

Horizon 是一种高效的跨链桥协议，其将资产从 BFT 区块链转移到另一个区块链（如以太链），支持基本的智能合约执行。跨链桥协议允许链上交换加密货币、链上资产转移到边缘以及对分割区块链中事件的交叉碎片进行验证，且大多依赖拜占庭容错协议（BFT）来实现可扩展性。遗憾的是，现有的可以从 BFT 区块链转移资金的桥式协议在目标区块链上产生了巨大的计算开销，导致智能合同验证的成本高昂。

如图 5 所示，一个跨链交易 $A \rightarrow B$ 想要将货币从区块链 A 转移到区块链 B（如以太坊区块链）。Horizon 跨链桥协议包括部署在区块链 B 上的智能合约 S 及一个中继节点 R，R 定期与来自 A 的元块头同步。Horizon 由两个关键部分组成：

（1）中继/合约同步。在每个周期结束时（即每 24 h），R 将最近的块头发送给合约，此块包含足够多的信息，以允许合约之后对 A 上包含的任何交易进行验证。在跨链桥协议中，合约验证由 T_{burn} 表示，由客户提交。T_{burn} 的本质是将 A 上的货币转移到一个空地址，即永久删除货币。

（2）跨链交易。Horizon[37] 协议的跨链交易由客户端 C 在向区块链提交 T_{burn} 时发起 A，一旦在 A 上确认事务，C 即向一个完整节点 F 发送请求，该节点始终保持 A 链的完整最新副本。F 收到请求后找到包括 T_{burn} 的块 Bk 并对其 merkle 树根进行检查与验证。最后，F 将验证后的数据发送给 C，C 创建解锁事务并将其提交到区块链 B 中。由于整个节点不受信任，因此此事务可能会失败。在这种情况下，客户端用另一个完整节点来替换 F 并重复该过程。

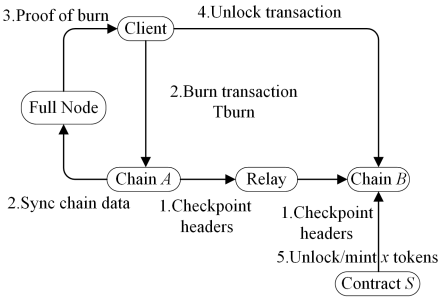


图 5　Horizon 跨链协议示意图

Fig. 5　Horizon cross chain protocol

3.5　Zendoo

Zendoo[38] 是一种可验证的跨链传输协议，数据与资产进行正向传输，即将资产从原始区块链 A（主链）移动到目标侧链 B 的操作。主链生成一个特殊类型的操作，删除相应的货币数量并为侧链提供相应货币的元数据。与此同时，侧链接受元数据并据此发行相应数量的货币，通过这种方法实现跨链的资产转移工作。正向转移的过程可以由元组表示，元组中包括 3 部分内容。

（1）账本 ID。在交易和资产转移之前，需要先明确目标侧链的唯一标识符。

（2）货币数量。主链和侧链之间需要转移的货币数量。

（3）元数据。其结构并不固定于主链中，它的语义含义是，基于不同侧链构造的预定义类型的不同变量组成，因此主链并不需要了解它的语义结构即可完成元数据的构造。

与正向传输相对应，反向传输协议允许货币从侧链移动到主链，它依赖于批转移的想法[39-40]。这意味着，如果在某一时期提交给副链的所有要求都向后转移，则称该时期为“撤回时期”。撤回的信息都收集在特殊撤回证书中，并将信息发送至主链进行处理。

撤回证书不仅是反向传输的一个容器，也是侧链的一种心跳机制，其将反馈定期提交给主链，以帮助主链确认各个侧链的状态。而且，不同侧链的退出时间不对齐，可能有不同的长度，因此整个系统异步运行。

3.6　WeCross

WeCross[41] 是一款由微众银行区块链团队自主研发并完全开源的国产区块链跨链协作平台。该平台从底层的平台架构设计开始，旨在探寻出可信融合连通所需的“最小化”抽象设计，同时充分考虑了跨链交互的安全性、扩展性与可用性问题，总结提出了跨链方案需要遵循的 4S 原则。

为保证异构区块链实现无阻的互联互通，需要设计统一的体系结构抽象。WeCross 在核心数据结构、区块链交互模式和事务管理上提取应用较广泛的主流区块链的产品核心和必需的公共子集，对区块链平台进行多层抽象。

Wecross 具有 3 层抽象体系结构，即事务层、交互层和数据层。数据层提炼了通用的区块数据结构，将交易、合约和消息等抽象成资源类型；又为资源设计通用的寻址协议，实现了数据在异构链上的流动。交互层为不同业务场景提供跨链交互模型，建立了适配于路由的中继网络，同时也提供了网络协议和交易验证机制，实现了跨链交互层的抽象设计。事务层基于数据层的数据结构和交互层的抽象，在事务级别上实现了跨链交互，目前其仅支持两阶段事务和哈希时间锁定事务，未来也会依据不同需求有针对性地设计更多跨链事务。

此 3 层结构中的任意一层都是可替换的，底层的技术实现并会不影响上层的逻辑运行，反之也是如此。其系统架构主要包括跨链分区、跨链路由、跨地域互联、灵活独立的部署架构，以及可自由定制的适配器和跨链资源等。

为了实现跨链交互的高效性与安全性，WeCross 通过 4 项技术实现了跨链的核心功能。

（1）UBI（通用区块链接口）。其解决了异构区块链的 API 与交互调用逻辑各异的问题，为交易、智能合约与资产等数据设计了统一的资源样式，以“求同存异”和“最大公约数”为基本思路，对主流区块链的关键数据结构进行提炼，将核心接口归纳为数据、调用和事件 3 类固定的接口，设计了普适的

跨链抽象区块数据结构，用户无须关心底层架构，只需要传入参数并规定返回值即可。

(2)HIP(异构链互联模型)。其定义了一种区块链接入范式，只需要获取“资源”和“信息”的接口便可连接入一条区块链，而无须对原有结构进行修改。该模型支持单分区单路由、单分区多路由和多分区多路由等多种场景。跨链路由作为整个交互模型的核心模块，采用分层设计的理念，共分为4层，以TCP[42]长连接保证双向通信，路由间会自动同步各自区块链的区块高度、共识等多种状态。

(3)TTM(可信事务机制)。其使用了多维度的默克尔证明作为跨链互信技术的基本算法，在保证对用户的完全透明的同时，既检验了交易的存在性，也能够验证交易结果的正确性，为跨链交易的可信执行提供了基础。

(4)MIG(多边跨链治理)。其是一套完整的区块链多边治理方案，通过协商和投票的方式进行机构的准入、区块链治理与有效的监管仲裁工作。通过在治理链上部署权限管理智能合约，将跨链操作的权限控制细化到分区、机构、区块链甚至资源的具体接口。而接入到此链的跨链路由将实时同步于执行合约中的策略，以保障跨链业务中的多边治理与跨链信息安全。

3.7 区块链跨链项目对比

表1列出了8种跨链技术在技术实现、共识机制等不同方面的对比情况。

表1 8种区块链跨链项目对比

Table 1 Comparison of eight blockchain cross-chain projects

	跨链技术	交易类型	共识机制
ILP	公证人机制	以转账为主	托管机制
Cosmos	中继	支持智能合约	改进的PoS方法
Plasma	侧链	支持智能合约	PoS
Horizon	中继	支持智能合约	PBFT
Zendoo	侧链	支持智能合约	改进的PoS方法
Lightning Network	哈希锁定	以转账为主	哈希算法
Fusion	分布式私钥控制	以转账为主	分布式私钥与门限签名
WeCross	中继	二阶段提交、哈希时间锁定	默克尔证明机制

由表1可知，目前的区块链跨链项目主要以4种跨链技术为主要技术支持。其中侧链/中继技术的应用频度更高，如早期以Tendermint core内核为共识协议的较为完善的Cosmos网络架构，到近年来的Horizon和Zendoo等新研发的跨链协议，以及由中国企业自主研发的区块链跨链平台WeCross，均是侧链/中继技术的体现；公证人机制是基于ILP协议创造的技术框架；哈希锁定技术在Lightning Network架构中得以充分利用；Fusion则是分布式私钥控制的代表项目之一。

在支持智能合约的角度上，ILP，Lightning Network和Fusion均支持以转账为主的交易类型；Cosmos，Plasma，Horizon和Zendoo均支持智能合约等多种类型的交易；WeCross平台目前支持二阶段提交与哈希时间锁定的事务，未来将根据应用场景的不同有针对性地设计事务类型。项目在共识机制上也存在差异，如Horizon依赖PBFT技术实现节点之间的共识；Plasma使用PoS证明作为共识技术；Cosmos和Zendoo使用经过改进的PoS证明技术；而Fusion通过分布式密钥与门限签名[43-44]的方式，来保证参与共识的每一个节点都能够参与到跨链交易的资产锁定与解锁中；WeCross则使用默克尔验证的方式来验证交易的存在性与交易结果的正确性。

4 讨论

4.1 发展现状与趋势

表2列出了4种区块链跨链技术在不同特性方面的对比。目前的跨链技术均以转账交易作为主要支持的交易类型，侧链/中继技术也支持合约调用的交易类型，而公证人机制则由公证人决定跨链系统能够支持的交易类型。相比其他3种技术仅需要确保链不会失效并解决51%的攻击问题，公证人技术需要较高的信任基础，即需要满足多数公证人诚实这一条件。在公证人的共同担保与互信的条件下，才能保证整个跨链系统的性能正常。在此项跨链技术中，公证人起到了至关重要的作用。

表2 4种区块链跨链技术的对比

Table 2 Comparison of four blockchain cross-chain technologies

	公证人机制	侧链/中继	哈希锁定	分布式私钥控制
互操作性	公证人决定所支持的互操作交易类型	支持转账、合约调用等交易	主要支持转账类型交易	主要支持转账类型交易
信任模型	多数公证人诚实	链不会失效 不会受到“51%攻击”	链不会失效 不会受到“51%攻击”	链不会失效 不会受到“51%攻击”
使用跨链交换	支持	支持	支持	支持
使用跨链资产转移	支持(需要长期公证人信任)	支持	不支持	支持
适用跨链原语	支持	支持	不直接支持	支持
适用跨链资产抵押	支持(需要长期公证人信任)	支持	大多数支持但存在一定难度	支持
多种币智能合约	困难	困难	不支持	支持
实现难度	中等	难	容易	中等
原子性	公证人担保	合约实现	哈希锁定和超时机制实现	多签算法实现
通用性	公证人决定支持的平台类型	侧链/中继链决定支持的平台类型	闪电网络支持比特币，雷电网络支持以太坊	底层链支持脚本机制和签名校验，支持主流公有链、联盟链
安全性	公证人互信机制	Merkle证明	哈希算法	多签名算法
是否需要信任基础	需要	不需要	不需要	不需要
可扩展性	公证人决定	可平行扩展	可平行扩展	可平行扩展

几种技术均支持跨链交换，除了哈希锁定技术外，其余的跨链技术均适用于跨链原语并支持跨链资产转移和抵押；哈希锁定技术则是不直接支持或实现起来存在一定难度。但相比其他3种技术，哈希锁定的实现难度最低，其次为公证人机制和分布式私钥控制，实现难度最高的是侧链和中继技术。4种技术均以不同的方法保证了系统的原子性、通用性和安全性，并且除公证人技术的扩展技术由公证人决定外，其他3种技术均支持可平行扩展。

4.2　跨链技术的难点

4.2.1　跨链事务管理问题

一个完整的跨链交易可以拆分为若干个子交易，这些子交易构成事务，跨链交易需要保证事务的ACID。在保证事务的一致性问题上，不同区块链的共识机制大都不同[45-46]，常见的共识算法包括PoW[47]共识、PoS[48]共识、DBFT共识和XBFT共识等。为保持交易的最终一致性，不同区块链需要在共识机制上达成互信。在保证事务的原子性的问题上，事务只有发生和不发生两种状态，子交易可以发生在不同的区块链系统中，跨链系统需要保证子交易间的独立性，以保障交易双方信息一致和同步。若后续的子交易失败，之前的子交易也可以撤回，以避免双花[49]问题等漏洞。

4.2.2　多链兼容与验证问题

为实现不同区块链之间的互联互通，首先需要解决多链之间的兼容性问题，使得区块链之间的交易可以被互相接收。已有的区块链大部分是异构的，需要一一进行兼容性对接；尚未开发完毕的区块链则需要进行兼容性研发，做好与其他异构链互联互通的准备。在一个区块链可以接收另一个区块链上的交易之后，需要考虑交易的确认与验证问题：1）确认交易的执行并写入区块链；2）验证交易是否已经满足共识机制。跨链的双方需要验证彼此交易的合法性和有效性，以及在完成确认和验证后如何将信息成功广播到链上。

4.2.3　跨链安全与监管问题

区块链由于其本身的设计机制以及针对智能合约和共识算法等的恶意攻击，存在很多安全漏洞，可能会引发双花[49]攻击、密钥泄漏、DoS等问题，这些漏洞会对用户及区块链上的交易产生严重的安全隐患，可能会造成巨大的经济损失。在区块链跨链系统上，如果链与链之间交易的独立性较差，且没有做好安全保障，在出现恶意攻击时，跨链会导致更加严重的损失。

同时，为解决区块链系统的安全问题，设置监管系统对智能合约及分类账等进行安全性检测。在多链互联的状况下，监管系统的存在能够为不同区块链系统提供监管检测服务。在两条链交互的过程中，做好适度的隔离和安全检测工作，防止当一条链产生安全问题时，对整个跨链网络产生不必要的影响。

4.2.4　隐私保护问题

区块链系统采用一系列密码学算法在节点之间建立共识机制，但为了保证当前交易的一些敏感数据以及交易中涉及的用户隐私信息不被泄漏给恶意节点，需要提高系统的隐私性[50]。攻击者可能会对区块链网络中的节点进行攻击，而区块链交易的公开性便于攻击者针对其关联性对交易敏感信息进行推测，而且在区块链发展初期，区块链系统还存在很多安全缺陷，这些都可能成为攻击者窃取信息的目标。跨链系统对隐私保护的要求更高，隐私丢失带来的后果也更严重。

4.2.5　事务并发执行问题

在比特币、以太坊等区块链中，交易的执行都是按照链上的顺序决定的，这样的串行执行在一定程度上影响了矿工和验证者的工作效率，大大降低了区块链事务处理的吞吐量[51]。在区块链跨链系统中，事务被分散到不同链上，进行事务的并行化处理的难度也变得更大。

4.2.6　技术实现难度问题

跨链系统已经成为区块链技术的一个重点研究方向，但其技术实现难度较大，交易涉及两条甚至多条链之间的价值流通，对上述几个方面都有较高的要求，因此需要针对不同区块链系统的特性进行有针对性的开发。在跨链平台建立完成后，可以考虑基于此平台进行新型区块链系统的开发，目前有许多跨链项目正处于研发过程中，如Cosmos和Plasma等，这些项目虽然取得了一定的进展，但仍处于初期阶段，若要达到跨链平台商业化，还有很多技术问题亟需解决。

4.3　跨链技术总结与展望

综上所述，跨链技术需要满足系统的原子性、通用性和安全性，需要有良好的可扩展性，除了转账交易，还需要设计并实现对更多类型交易的支持，可以考虑引入智能合约来完成更复杂的交易。目前的跨链技术对多种币的智能合约的支持性较差，多链之间的兼容性依然很难满足，如何更好地验证彼此交易的合法性和有效性，可以作为未来的研究方向之一。同时，跨链技术存在安全漏洞，在信任模型上还有较大的提升空间，可以考虑引入拜占庭模型或其他较完善的共识机制，来提高系统的安全性和健壮性。

结束语　区块链具有多方共识、分布式存储、不可篡改和可追溯等特性，在数字货币领域、供应链管理领域、事务监管与溯源和征信安全等方面具有广阔的应用前景。随着区块链技术的持续发展与不断创新，大量区块链项目如雨后春笋般问世，为使不同领域不同功能区块链之间能够更好地实现互联互通与价值流动，跨链技术成为了区块链行业的一个关注焦点。

区块链跨链存在事务管理、交易验证、共识机制、安全监管等问题，这些难题极大地限制了区块链的网络边界与应用范围，其在阻碍区块链赋能数字经济的进程的同时，也为研究人员们提出了挑战并指明了研究的方向。目前主流的区块链互操作方法有公证人机制、侧链/中继、哈希锁定和分布式私钥控制4种，本文详细介绍了这4种方案的理念并进行了特性对比，另外还讨论了几种较完善的区块链跨链项目。

要推进区块链跨链技术的发展，需要技术提供方、行业需求方和监管机构等多方齐心协力共同参与，促进跨链技术的研究及跨链平台的搭建，区块链技术也会随之演进与成熟，共同构建互联互通、安全可信的区块链跨链生态体系。在对

现有技术进行更新与优化的同时，应进一步探索异构链之间因底层架构、数据结构、接口协议和共识机制等多维异构性，而导致的无法很好互联互通的问题的解决方案，研究一种并行高效、安全可信和可拓展性强的跨链机制，使其能够在更多创新应用的场景中服务更多更广的群体，以应对未来形式多样的跨链应用场景。而为不断扩展的跨链平台与大量事务提供更完善的监管工作也是跨链技术的一个重要研究方向。

参 考 文 献

[1] LONE A H, NAAZ R. Demystifying Cryptography behind Blockchains and a Vision for Post-Quantum Blockchains[C]// 2020 IEEE International Conference for Innovation in Technology (INOCON). 2020: 1-6.

[2] YU G, NIE T Z, LI X H, et al. The Challenge and Prospect of Distributed Data Management Techniques in Blockchain Systems[J]. Chinese Journal of Computers, 2021, 44(1): 28-54.

[3] HE P, YU G, ZHANG Y F, et al. Survey on Blockchain Technology and Its Application Prospect [J]. Computer Science, 2017, 44(4): 1-7.

[4] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[J/OL]. Consulted. https://courses. cs. washington. edu/courses/csep552/18wi/papers/nakamoto-bitcoin. pdf.

[5] KÖLVART M, POOLA M, RULL A. Smart Contracts[M]. Springer International Publishing, 2016.

[6] HUA S, ZHANG S, PI B, et al. Reasonableness discussion and analysis for Hyperledger Fabric configuration[C]// 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). 2020: 1-3.

[7] ZHU L, YU H, ZHAN S X, et al. Research on high-performance consortium blockchain technology[J]. Ruan Jian Xue Bao: Journal of Software, 2019, 30(6): 1577-1593.

[8] WANG X L, LIU X F, ZHAO G S, et al. Overview of Blockchain: Technology and Challenges [J]. Radio Communications Technology, 2018, 44(6)531-537.

[9] LU A T, ZHAO K, YANG J Y, et al. Research on Cross-chain Technology of Blockchain [J]. Netinfo Security, 2019(8): 83-90.

[10] GUO Z, GUO S Y, ZHANG S L, et al. Analysis of blockchain cross chain technology[J]. Journal of Internet of Things, 2020, 4(2): 36-49.

[11] SUN Y, FAN L J, HONG X H. Technology Development and Application of Blockchain: Current Status and Challenges[J]. Engineering Science, 2018, 20(2): 35-40.

[12] SCHWARTZ D, YOUNGS N, BRITTO A. The Ripple protocol consensus algorithm[EB/OL]. https://ripple. com/files /ripple_consensus_whitepaper. Pdf.

[13] THOMAS S, SCHWARTZ E. A protocol for interledger payments[EB/OL]. https://interledger. org/interledger. pdf.

[14] COLLADO A, GÓMEZ-SUÁREZ A, OONISHI Y, et al. Synthesis, characterisation, and oxygen atom transfer reactions involving the first gold(I)-alkylperoxo complexes[J]. Chemical Communications, 2013, 49(91): 10745-10747.

[15] LI C L, CHEN Y. Merkle Hash Tree Based Deduplication in Cloud Storage[J]. Applied Mechanics and Materials, 2014, 556: 6223-6227.

[16] Blockstream[EB/OL]. [2019-04-12]. https://blockstream. com/.

[17] POON J, DRYJA T. The bitcoin lightning network: Scalable off-chain instant payments[J/OL]. https://www. mianshigee. com/ppt/17915exz/.

[18] KWON J, BUCHMAN E. Cosmos: A network of distributed ledgers[EB/OL]. https://github. com/cosmos/cosmos /blob/master/WHITEPAPER. md.

[19] CONSENSYS. BTC Relay's documentation [EB/OL]. http://btc-relay. readthedocs. io/en/latest/.

[20] KWON J. Tendermint: Consensus without mining[EB/OL]. https://tendermint. com/static/docs/tendermint. pdf.

[21] POON J, BUTERIN V. Plasma: Scalable autonomous smart contracts[EB/OL]. https://plasma. io/plasma. pdf.

[22] LI F, LI Z R, ZHAO H. Research on the progress of blockchain cross chain technology[J]. Journal of Software, 2019, 30(6): 1649-1660.

[23] DAI B R, JIANG S M, LI D W, et al. Evaluation Model of Cross-chain Notary Mechanism Based on Improved PageRank Algorithm[J]. Computer Engineering, 2021, 47(2): 26-31.

[24] NEISSE R. An Interledger Blockchain Platform for Cross-Border Management of Cybersecurity Information[J]. IEEE Internet Computing, 2020, 24(3): 19-29.

[25] THOMAS S, SCHARRTZ E. Interledger whitepaper[EB/OL]. https://interledger. org/.

[26] RIVEST R, SHAMIR A, ADLEMAN L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems (1978)[M/OL]. 2021. https://www. researchgate. net/publication/349073609_A_Method_for_Obtaining_Digital_Signatures_and_Public-Key_Cryptosystems_1978.

[27] YU C F, WANG L, ZHOU A H, et al. Method and apparatus for performing multi-party secure computing based-on issuing certificate: US2021067347[P]. 2021-03-04.

[28] YU C F, WANG L, ZHOU A H, et al. Method and apparatus for performing multi-party secure computing based-on issuing certificate: US2021250183[P]. 2021-08-12.

[29] ZHANG Q N, ZHU J M, GAO S, et al. A Smart Service Transaction and Supervision System Based on Blockchain: CN113313592A[P]. 2021-08-27.

[30] KANG J S, CHOI Y S, SUNG M Y, et al. A Study of Security and Privacy in USN Environment using HASH LOCK Approach [C]// International Conference on Future Information & Communication Engineering. 2007.

[31] ZHONG P, MA W, WANG B, et al. A Cryptocurrency Multi-channel Payment Method Based on Smart Contracts: CN113011878A[P]. 2021-06-22.

[32] Fusion[EB/OL]. [2019-04-15]. https://www. fusion. org/.

[33] PATIN A. Technologies for private key recovery in distributed ledger systems: US11025423[P]. 2021-06-01.

[34] ZHAO Z, WU G, SUSILO W, et al. Accountable identity-based

encryption with distributed private key generators[J]. Information Sciences，2019，505(10)：352-366.

[35] HOPEBAILIE A，THOMAS S. Interledger：Creating a Standard for Payments [C] // International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee，2016.

[36] HASSAN A O，HASAN A A. Simplified Data Processing for Large Cluster：A MapReduce and Hadoop Based Study[J]. Advances in Applied Sciences，2021，6(3)：43.

[37] LAN R，UPADHYAYA G，TSE S，et al. Horizon：A Gas-Efficient，Trustless Bridge for Cross-Chain Transactions[J]. arXiv：2101.06000，2021.

[38] GAROFFOLO A，KAIDALOV D，OLIYNYKOV R. Zendoo：a zk-snark verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains[C]// 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). IEEE，2020：1257-1262.

[39] GAROFFOLO A，VIGLIONE R. Sidechains：Decoupled consensus between chains[J]. arXiv：1812.05441，2018.

[40] GAZI P，KIAYIAS A，ZINDROS D. Proof-of-stake sidechains [C]// 2019 IEEE Symposium on Security and Privacy (SP). IEEE，2019：139-156.

[41] WeCross Technical White Paper [EB/OL]. http://fintech.webank.com/wecross.

[42] LI K，CHEN Q H，LU J X. Summary of Research on HTTP Protocol[J]. China CIO News，2021(5)：126-129.

[43] LIAO H M，WANG D，XUAN J X，et al. Threshold Signature and Decryption Scheme Based on Domestic Public Key Cryptographic Algorithm [J]. Computer Applications and Software，2021，38(6)：313-317.

[44] RIVEST R L，SHAMIR A，ADLEMAN L. A method for obtaining digital signatures and public key cryptosystems[M]. Routledge，2019.

[45] JIN S X，ZHANG X D，GE J G，et al. Review of Blockchain Consensus Algorithm Research[J]. Journal of Information Security，2021，6(2)：85-100.

[46] KING S. PPCoin：Peer-to-peer crypto-currency with proof-of-stake[EB/OL]. http://www.peercoin.net/assets /paper/peercoin-paper.pdf.

[47] GERVAIS A，KARAME G O，WÜST K，et al. On the Security and Performance of Proof of Work Blockchains[C]// the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM，2016.

[48] BUTERIN V. Plasma cash：Plasma with much less per-user data checking [OL]. https://ethresear.ch/t/plasma-cash-plasma-with-much-less per-user-data-checking/1298.

[49] KARAME G O，ANDROULAKI E，CAPKUN S. Double spending Fast Payments in Bitcoin[C]// The 2012 ACM Conference on Computer & Communications Security. New York：ACM，2012：906-917.

[50] KANG H Y，DENG J. Summary of Research on Blockchain Data Privacy Protection[J]. Journal of Shandong University (Science Edition)，2021，56(5)：92-110.

[51] DICKERSON T，GAZZILLO P，HERLIHY M，et al. Adding Concurrency to Smart Contracts：US20190087793A1[P]. 2019-03-21.

SUN Hao，born in 1997，postgraduate，is a student member of China Computer Federation. Her main research interests include query processing and blockchain technology.

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

（责任编辑：喻藜）