软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1649−1660 [doi: 10.13328/j.cnki.jos.005741]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链跨链技术进展研究*

李 芳, 李卓然, 赵 赫

(中国科学院 合肥物质科学研究院,安徽 合肥 230031)

通讯作者: 赵赫, E-mail: zhaoh@hfcas.ac.cn

摘 要: 随着区块链技术的发展,各种具有不同特点、适用于不同应用场景的区块链如比特币、以太坊等公有链以及私有链、联盟链大量共存.由于区块链的相互独立性,现存各区块链之间的数据通信、价值转移仍面临挑战,价值孤岛现象逐渐显现.区块链的跨链技术是区块链实现互联互通、提升可扩展性的重要技术手段.对跨链技术领域的成果进行了系统总结:首先,分析了跨链技术的需求及面临的技术难点;其次,总结了正在发展的跨链技术,并介绍了 24 种主流跨链技术的原理与实现思路;然后,综合分析了跨链技术存在的安全性风险,并列举了 12 项主要问题;最后,总结探讨了跨链技术的未来发展趋势.

关键词: 区块链;跨链协议;共识算法;价值转移;数据转移

中图法分类号: TP309

中文引用格式: 李芳,李卓然,赵赫.区块链跨链技术进展研究.软件学报,2019,30(6):1649−1660. http://www.jos.org.cn/1000-9825/5741.htm

英文引用格式: Li F, Li ZR, Zhao H. Research on the progress in cross-chain technology of blockchains. Ruan Jian Xue Bao/ Journal of Software, 2019,30(6):1649−1660 (in Chinese). http://www.jos.org.cn/1000-9825/5741.htm

Research on the Progress in Cross-chain Technology of Blockchains

LI Fang, LI Zhuo-Ran, ZHAO He

(Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China)

Abstract: With the development of blockchain technology, various blockchains with different characteristics and applications such as Bitcoin, Ethereum, other public chains, as well as private and consortium chains coexist in large numbers. Due to the independence of blockchains, the data communication and value transfer between existing blockchains are still facing challenges, and the problem of value isolation gradually emerges. The cross-chain technology is an important technical means for blockchains to realize interoperability and enhance scalability. This article systematically summarizes the achievements in the cross-chain technology field. Firstly, the requirements of cross-chain technologies and the technical difficulties they face are analyzed. Secondly, the cross-chain technologies those are under development are summarized and the mechanisms and implementations of 24 mainstream cross-chain technologies are introduced. Then, the security risks of cross-chain technology are analyzed, and 12 major issues are listed. Finally, the trend of future development of cross-chain technology is summarized and discussed.

Key words: blockchain; cross-chain protocol; consensus algorithm; value transfer; data transfer

区块链(blockchain)[1]是一种去中心化(decentralized)、无需信任(trustless)的分布式数据账本,它通过密码学方法让网络中的所有节点共同拥有、管理和监督数据,系统的运转不接受任何单一节点的控制,从而具有不可

* 基金项目: 国家自然科学基金(61602435); 安徽省自然科学基金(1708085QF153)

Foundation item: National Natural Science Foundation of China (61602435); Natural Science Foundation of Anhui Province (1708085QF153)

本文由区块链与数字货币技术专题特约编辑斯雪明教授和陈文光教授推荐.

收稿时间: 2018-06-25; 修改时间: 2018-10-12; 采用时间: 2018-12-18; jos 在线出版时间: 2019-03-27

CNKI 网络优先出版: 2019-03-27 16:40:31, http://kns.cnki.net/kcms/detail/11.2560.TP.20190327.1640.007.html

伪造、不可篡改、可追溯等特点.区块链通过技术构造全新的信任体系,具有改变人类社会价值传递方式的潜力,并支持与行业应用深度融合,引起信息技术、金融、保险等多个领域的广泛关注.

以比特币(Bitcoin,简称 BTC)[1]白皮书发布作为区块链技术发展的起始点,在近 10 年期间,世界各国出现了众多区块链项目,它们有些是基于比特币代码集成了一些局部优化,有些是为适应特定应用场景而做出了功能改进,亦或为提升区块链性能与开发友好性等提出了重大创新.比特币设计中融合的非对称加密、工作量证明(proof-of-work)、链式结构(chain)、时间戳(timestamps)、Merkle 树(Merkle Tree)等相关算法、协议、机制构成了区块链技术架构的基础.但由于比特币的初衷是实现一种基于点对点技术的电子现金系统,并没有过多地考虑区块链在更广泛范围应用时所需的图灵完备、可扩展性、安全性等要求,其区块容量、区块分叉、二次开发等也面临一定的问题.人们意识到单个区块链无法解决所有技术问题,也并不能覆盖所有应用场景,各类区块链项目应运而生.

通过在共识算法、区块结构、扩展协议等方面的不断创新,区块链领域目前已形成多类项目共存的景象.以太坊(Ethereum,简称 ETH)[2]致力于将区块链拓展应用于数字货币以外的领域,并为开发者提供一个能够快速创建智能合约以及开发去中心化应用的成熟开发平台;瑞波(Ripple)[3]采用了一种新的共识算法,通过网络中有限数量的可信任节点实现共识,以减少交易确认时间;比特现金(bitcoin cash)[4]将区块大小的限制提升至 8MB 甚至更大容量的区块,在一定程度上实现了链上扩容;EOS[5]提出一种支持分布式应用开发的区块链底层平台,并计划采用并行链和委任权益证明(delegated proof of stake,简称 DPOS)实现高系统性能;IOTA[6]和 Byteball[7]等采用非线性链式结构的有向无环图(directed acyclic graph,简称 DAG)[8]实现分布式账本,提高系统的交易效率.据德勤于 2017 年 11 月出具的报告[9]显示,Github 上区块链代码项目总数约 9 万个,并呈现逐年增加的趋势,足见区块链领域的创新发展态势.

区块链项目的蓬勃发展,不可避免地引出了一个问题:链与链之间如何实现互联互通?链联网(Internet of blockchains)能否成为继互联网、物联网的下一个基础网络架构?随着区块链项目数量越来越多,价值孤岛现象也更加严重.区块链资产是否能够实现无需第三方参与的原子交换(atomic swap)?基于跨链的区块链下(off-chain)扩容技术方案存在哪些争议?区块链智能合约的应用过程中,区块链又如何与传统互联网系统实现可信任的数据交换?等等.上述问题引发了业界对跨链技术的探索实验.

本课题组在国内较早启动了区块链技术相关研究[10,11],并长期关注跨链技术研究,通过本文的系统性梳理,期望对跨链技术的创新发展提供参考.本文第 1 节对区块链跨链存在的问题、需求以及技术难点进行分析概述.第 2 节介绍区块链发展不同阶段的跨链技术演进.第 3 节重点分析跨链技术设计与应用将面对的安全性问题.最后,在第 4 节总结跨链技术的发展和研究趋势.

1 区块链的跨链需求及技术难点

区块链技术自比特币区块链于 2008 年[1]诞生以来,已逐步发展出上千种区块链项目.根据区块链的应用场景、节点准入条件及去中心化程度,区块链被分为公有链(public blockchain)、私有链(private blockchain)以及联盟链(consortium blockchain)这 3 大类[12].其中,公有链具有高度去中心化特点,节点可自由加入或退出,并拥有读取数据、竞争记账权、实施交易等平等权限,以比特币[1]、以太坊[2]等为代表;私有链由第三方控制系统的各项权限,节点的加入、数据的读写均有一定条件限制,如摩根大通的 Quorum[13]等;联盟链由多个机构或组织共同管理,各节点通常对应不同的实体机构或组织,通过准入机制加入、退出网络,如 Corda[14],Hyperledger[15]等.

区块链的跨链技术是区块链实现互联互通(interoperability)、提升可扩展性(scalability)的重要技术手段.在网络形态上,区块链不同于互联网,后者支持一张网接入全球的节点,前者则形成了多个相互隔绝的平行网络.除了公有链的广泛共存,私有链和联盟链则支持让不同组织拥有各自的区块链,甚至让同一个组织内部同时运行多个区块链.全球区块链的数量在不断增多,而不同区块链网络的相互隔绝,导致链之间无法有效进行数字资产转移、跨链通信等操作.近年来,随着区块链应用场景的不断丰富和复杂化,越来越多的区块链项目提出跨链的需求与解决方案,跨链技术逐步得到发展.

根据目前主流跨链技术的设计研发,跨链的目的以及要解决的问题主要包括以下几点.

(1) 不同区块链之间的资产转移.尽管第三方交易平台能够提供不同区块链项目资产的转移与交换,但第三方交易平台的引入带来了新的中心化节点,不可避免地存在资产安全性、可信任性等问题.跨链确保了是用技术而非机构或人来提供安全、可靠、高效的链上资产转移途径;

(2) 实现区块链资产的留置[16].类似于金融和法律领域的财产留置,区块链资产能够实现链上锁定冻结,并设定某个区块链上的资产锁定条件、解锁条件,还可以与其他链的特定事件/行为进行关联;

(3) 读取和验证其他链的状态或事件.自以太坊区块链[2]问世以来,基于区块链的智能合约[17]得到快速发展.在某个区块链上部署的智能合约,触发其执行的条件可能需要依赖于其他链的信息和数据,跨链数据访问在该应用场景中具有关键作用;

(4) 提升区块链交易处理能力.区块链的可扩展性三难题基本法则[18]表明,区块链只能兼顾去中心性、可扩展性和安全性中的两项.区块链的吞吐量和可扩展性一直被认为是重要的瓶颈,尽管诸如 EOS[5]等区块链项目声称其 TPS(每秒处理事务数)可达百万量级,但均以设立少量验证节点为前提,降低了系统的去中心化特性.跨链通信是提供更高扩展性的技术路线之一.

区块链应用场景的不断拓展以及区块链互联互通的潜在需求,促进了跨链技术的持续创新和进步.根据跨链技术的演进和实现方式,以太坊的创始人 Buterin 曾经总结了 3 类跨链技术[16]——公证人机制(notary schemes)、侧链/中继(sidechains/relays)、哈希锁定(Hash-locking).

(1) 公证人机制.通过选举一个或多个组织作为公证人,对链 *A* 的事件进行自动或请求式监听,并在指定事件发生后,在链 *B* 执行相应动作,实现对事件的响应.公证人群体通过特定的共识算法,对事件是否发生达成共识.公证人机制又分为中心化公证人机制(centralized notary schemes)和多重签名公证人机制(multisig notary schemes),区别在于后者利用密码学技术,在每次交易验证时从公证人群体中随机选出一部分公证人,共同完成签名的签发,从而降低对公证人可靠性的依赖程度;

(2) 侧链/中继.侧链/中继以轻客户端验证技术为基础,即:在链 *B* 上执行类似区块链轻客户端功能的智能合约,通过验证链 *A* 的加密哈希树(cryptographic hash tree)以及区块头(block header)来验证链 *A* 的某项特定交易、事件或状态信息是否发生;

(3) 哈希锁定.通过在两条链上运行特定的智能合约,实现跨链交易与信息交互.用户 *A* 生成随机数 *s*,并计算出该随机数的哈希值 $h=hash(s)$发送给用户 *B*;*A* 和 *B* 通过智能合约先后锁定各自的资产;如果 *B* 在 *X* 时间内收到正确的 *s*,智能合约自动执行将 *B* 的资产将转移给 *A*,否则退回给 *B*;如果 *A* 在 2*X* 时间内收到随机数 *s*,*A* 的资产将自动转移给 *B*,否则退回给 *A*.

跨链可以分为区块链内部各个子链/主链之间以及不同区块链系统之间的互操作.从更广义的概念层面,跨链进一步涉及区块链与传统系统和协议的交互.目前,跨链技术尚未实现广泛应用,表明了跨链面临的问题复杂性.鉴于大多数区块链系统在诞生之初就缺乏互操作特性,跨链技术在设计与实现时需要重点解决如何适配各类区块链,并确保跨链操作的高效率和高安全性.

2 跨链关键技术

区块链技术自诞生以来一直具有较强的金融色彩,在早期的绝大部分时间里,比特币长期占有全球区块链项目总市值 80%以上的市场份额,处于一枝独秀的状态.随着区块链技术逐渐进入更广泛的学术界和产业界视野,越来越多的人才参与到区块链行业的创新研发.2017 年 5 月 17 日,比特币市值占比首次低于 50%[19];2017 年 8 月 14 日,以太坊交易量首次超过比特币[20].公有链、私有链、联盟链的数量不断增多,区块链的应用场景愈加丰富,行业对跨链的需求也更加明显.本文以 2017 年 5 月为分界线,分为比特币区块链时代与后比特币区块链时代两个时期,对跨链技术的发展情况分别进行介绍.

2.1 比特币区块链时代的跨链技术

2013 年 5 月,Nolan 在 BitcoinTalk 论坛提出了原子转移(atomic transfers)思路[21],构成了实现原子式跨链数

字资产交易的最初基础技术方案.原子转移也称原子交换(atomic swap),其概念类似于传统证券结算系统的货银对付(delivery versus payment,简称 DVP)或外汇交易系统的交易同步交收(payment versus payment,简称 PvP),在区块链领域,即指双方交易同时发生或同时不发生,二者不可分割.该方案通过让交易双方分别在比特币区块链和其他数字货币区块链上设定合约脚本,并利用是否获知某个哈希值的原像(preimage)作为合约触发条件.该原像由交易一方在交易之前随机产生,并结合方案设计的一系列合约锁定、解锁流程,实现跨链交易的原子性.Nolan 的技术方案经过改进升级后被称为哈希锁定,并成为跨链的一种主要技术手段.在用于 BTC 链下交易扩容方案的闪电网络(lightning network)中也运用了类似的哈希时间锁定合约(Hashed timelock contract,简称 HTLC).

侧链则是首个产生较大影响力的跨链技术.比特币核心开发者加入的 Blockstream 公司在 2014 年 10 月发布的白皮书中提出了楔入式侧链(pegged sidechains)[22]的概念,其目的是实现不同区块链资产的跨链转移,以及可以在不影响主链的情况下,实施更多的技术创新与金融创新.双向楔入(two-way peg)作为侧链的核心技术基础,定义为不同链资产的等值转换机制,并分为对称式双向楔入与非对称式双向楔入.2016 年 12 月,Blockstream 公司进一步提出强联邦侧链(sidechains with strong federations)的概念[23],在资产交换中引入由多方控制的多重签名地址,以减少延迟并提升互操作性.

业界在探索区块链间的跨链同时,针对 BTC 本身的扩容问题发展出链下交易技术.Poon 于 2015 年 2 月发布了闪电网络(lightning network)白皮书[24],该技术是通过设计一种新的支付渠道网络实现可扩展的连锁即时支付.闪电网络利用链下支付提高交易处理效率,可以被认为是区块链内部的跨链操作.随着闪电网络的实现及升级,2017 年 11 月,闪电网络在链下首次实现了测试网中 BTC 和 LTC 的跨链原子交易.

Ripple 公司在 2015 年 11 月发布的 Interledger 白皮书[25]中提出了一种用于不同支付网络或账本系统交互的协议,并计划覆盖至区块链账本及各类传统支付系统.Interledger 通过连接者(connector)传递跨系统的交易,在最终接收者收到资金前,传递线路上各个支持 Interledger 协议的系统会对各环节发送者的资金进行托管锁定.Interledger 协议的交易托管与执行分为两种方式,其中,原子模式是由参与者选出一组公证人来协调交易;通用模式无需公证人,通过参与者给予激励以及反向执行指令来确保安全支付.Interledger 最初作为公证人机制的跨链代表,在协议发展过程中,也开始逐步融入哈希锁定的理念.

2016 年 5 月,美国区块链软件技术公司 ConsenSys 设计了 BTCRelay[26],实现了以太坊对比特币区块链数据的跨链访问.BTCRelay 实质是在以太坊网络上实现的一个智能合约,通过不断接收网络中各个 Relayer 节点推送的 BTC 区块头,实现 BTC 区块头在智能合约里的存储和实时更新.由于 BTC 区块链的交易信息主要以 Merkle tree 的形式存储在区块头中,在不依赖第三方中介的情况下,BTCRelay 以一种去中心化的方式实现了以太坊智能合约对 BTC 区块链的数据访问.尽管 BTCRelay 的原理和实现并不是非常复杂,但该系统使得用户能够创建各种触发条件依赖于 BTC 区块链事件或信息的以太坊智能合约,提高了智能合约的可用性.不过,BTCRelay 仅支持 ETH 和 BTC 之间的跨链,而且并不能让 BTC 同时也能读取 ETH 区块链的信息,在这种跨链方式下,通信是单向的,具有一定局限性.

2016 年 6 月,Kwon 提出了一种支持各种区块链接入与互操作的网络架构 Cosmos[27].基于建立区块链的互联网构想,Cosmos 网络设计为由枢纽(hub)和分区(zones)组成,其中,分区由 Tendermint[28]经典拜占庭容错共识算法引擎支持运行,可接入不同区块链,并支持分区数量的扩展.分区载入区块链后,各分区之间通信必须经由枢纽,并且遵照链间通信技术规范(inter blockchain communication protocol,简称 IBC)[27].Cosmos 架构的关键在于 Tendermint 共识引擎和 IBC 协议:Tendermint 是 2014 年 Castro 和 Liskov 基于实用拜占庭容错(PBFT)[29]算法提出的权益证明 PoS(proof-of-stake)[30]共识算法改编版,通过验证者(validator)对交易区块进行多轮投票达到共识;IBC 协议则定义了区块链注册、数据包格式、交易类型、数据包交付确认流程等内容.

2016 年 11 月,Wood 在 Polkadot 白皮书[31]中介绍了一种异构的多链架构,支持不同共识系统去中心化、去信任(trustless)地进行交互操作、访问.Polkadot 通过解耦共识机制和状态转移机制两种组件来解决伸缩性问题,并将容纳的不同区块链定义为平行链.Polkadot 的参与方包括收集者(collator)、渔夫(fisherman)、提名者

(nominator)和验证者(validator)这 4 种角色,分别承担运行平行链全节点、举报及证明非法行为、拥有权益并委托资产、区块封装等工作.在跨链通信方面,Polkadot 采用中继链的方式转发各平行链的交易,同时,平行链的区块头也会被包含进中继链的区块中,以避免双花的发生.通过设计参与方角色、激励模型,Polkadot 成为可自发扩展、兼容已有区块链的异构多链网络.

以太坊的链上扩容分片技术 Sharding[18]也备受关注.2016 年 11 月发布的 Sharding 技术文档中,计划在以太坊转为权益证明(proof of stake,简称 POS)后,以太坊区块链升级为由主链(main chain)和分片链(shard chain)构成的网络结构.方案中,以太坊将首先形成约 100 个分片链,账户和交易信息均存储在分片链上,每个分片链再与主链进行通信连接.分片链主要处理交易以及存储账户与合约的状态,并支持跨分片链的消息交互;主链主要是维护验证节点的状态以及跟踪分片链区块状态.通过分片技术实现交易的并行确认,将直接提高以太坊的交易吞吐量.

除了以上介绍的几种跨链技术以外,RootStock[32]在比特币区块链上构建智能合约系统,作为比特币区块链的侧链实现功能增强;Elements[33]通过双向锚定,提供与 BTC 的互转以及智能合约、私密交易证据分离等功能;Lisk[34]构建的分布式应用开发平台为每个应用提供一个单独的 Lisk 侧链;Factom[35]通过整合比特币和以太坊区块链,提供不可变更的数据存证功能;Corda[36]通过交易双方选择出的共同公证人作为交叉验证人,对交易数据进行验证.

2.2 后比特币区块链时代的跨链技术

以太坊创始人 Buterin 与闪电网络发明人 Poon 于 2017 年 8 月 11 日提出了 Plasma[37]区块链扩展设计模式.Plasma 设计了一种区块链树形框架,将主链作为树根、不同区块链作为主链的独立树形分支,并通过构建智能合约激励执行与强制执行框架,实现区块链的扩容计算.Plasma 包括激励层、树形链组织结构、MapReduce 计算框架、依赖于根链的共识机制和 bitmap-UTXO 结构这 5 个组件,协作实现合约持续计算、创建状态转移的欺诈证明、网络形态组织等功能.通过借鉴大数据并行计算模型 MapReduce 以及构建持续运作机制,Plasma 预期可使区块链扩容至支持每秒 10 亿量级的状态更新.

2018 年 1 月,Vitalik 在 Plasma 基础上提出了最小可行的 Plasma 实现(minimal viable plasma,简称 MVP).MVP[38]在处罚欺诈、子链依赖以及处理无效交易等方面进行了限定.2018 年 3 月,Vitalik 又提出修改版 Plasma Cash[39],在 Plasma 基础上进行了以下变更:区块链资产基本单位无法分割及合并;交易不再按照 txindex 顺序存储于 Merkle 树中,而是存储在稀疏简单的 Merkle 树或 Patricia 树中.Plasma 的跨链框架得到业界广泛关注,如 OmiseGO[40]计划使用 Plasma 支持可扩展的去中心化交易与支付平台、Lucidity[41]利用 Plasma 构建数字广告区块链协议等.

尽管以太坊因其开发友好性以及智能合约的高应用性,开发者与用户数量、市场份额均不断提升,但仍面临区块链扩展性问题,并曾因承载一款引发流行的 CryptoKitties 区块链游戏[42]出现交易严重阻塞[43].在此背景下,2017 年 11 月,Loom 项目[44]基于以太坊构建了一套支持开发、运行大型去中心化应用 DApp 的基础设施平台,并计划采用 Plasma 与以太坊实现资产转移,在保障资产安全的同时提升系统吞吐量.Loom 为开发者提供了可快速构建区块链的 SDK,并让开发的分布式应用 DApp 都单独运行在以太坊的不同侧链上,称为 DAppChain.该设计的特点在于每条 DAppChain 均可以由开发者根据需求采用不同的共识规则,具有一定的灵活性.

2017 年 8 月,Aion 项目[45]定义了一种多层次的区块链网络结构,为不同区块链系统的接入提供通信协议和标准.在 Aion 网络中,定义了“桥梁”实现区块链之间的连接和通信,桥梁也有自己独特的验证者网络.Aion 通过采用基于轻量级 BFT[46]的算法达成共识,并具有注册、竞争、交易奖励分配等功能.Aion 规定了包括发起网络、目的网络、路由信息、路由费用、Merkle 证明等在内的跨链交易格式,还设计了 Aion 虚拟机(AVM)提供对区块连逻辑的抽象以及提供运行应用程序的环境.

2017 年 8 月 29 日,Eykholt 等人在 Rchain 白皮书中[47]设计提出了一种并行的区块链多链网络,期望实现具有高扩展性的企业级区块链平台.Rchain 采用 RhoVM 虚拟机作为智能合约并发执行引擎,并通过定义命名空间(namespace),使 RhoVM 每个实例可以在命名空间中的独立区块链上并发执行智能合约.Rchain 的每个命名空

间相互独立并可相互通信,实现多链网络结构.

2017 年 11 月,Block Collider 项目[48]构建了基于多个不同区块链的分布式账本.在区块生成上,Block Collider 的区块由所接入的各个区块链的区块头组合而成,并基于中本聪共识设计了一种 Proof of Distance 的共识算法来提高计算效率.通过对不同区块链的集成,Block Collider 可提供跨链交易、跨链智能合约、交易加速等特性.Block Collider 发布时计划首先支持 BTC,ETH 等 6 种区块链的接入,并预留了扩展性,其他区块链的项目将通过投票的形式确定是否接入.

2017 年 11 月 24 日,Nano[49]技术白皮书介绍了一种基于区块晶格(block-lattice)结构的加密货币,其特色在于每个账户都有自己的区块链(账户链)来记录本账户的交易与余额历史,从而构成多链网络结构.Nano 的技术架构可认为是区块链的内部跨链,账户链之间通过收发交易以及异步确认形成网状区块晶格形态.与传统区块链采用线性增长的区块链式结构不同,Nano 实现了交易的异步更新,具有较小的数据库账本容量以及较高的交易吞吐量.

Zcash(ZEC)团队开发出 XCAT(交叉链原子交易)工具[50],实现了 ZEC 和 BTC 之间的跨链原子交易;Bancor[51]基于智能合约构建了一套跨链的去中心化流动性(liquidity)网络,实现没有对手方的区块链资产的自动估值和兑换;OneLedger[52]提供一套企业系统与区块链系统联通的解决方案,通过侧链接入各类私有链、联盟链和公有链,并通过中间协议层与企业级系统通信.

2.3 跨链技术的总结

总体而言,跨链技术还处于发展过程中,部分跨链技术目前仅公布了技术思路构想,并正在研发或在区块链测试网中开展局部实验阶段,还没有完全实现方案中所列出的各项功能指标和技术特性,因此对跨链技术的安全性、效率、性能、资源消耗等方面开展横向评估较困难.从公开的白皮书或技术报告来看,上述跨链技术有些为基础协议型,有些为开发设计模式,有些是某区块链的侧链,或仅用于有限个区块链之间互联等,各跨链技术不适于通过同一维度进行分类.表 1 汇总了各跨链技术的提出时间,并从该跨链技术是“基于 BTC 区块链/ETH 区块链/自有链”、跨链机制“公证人机制/侧链(中继)/哈希锁定/通信协议簇”、跨链范围“系统内部跨链/系统间跨链”这 3 个维度对跨链技术进行总结.

基于 BTC 区块链是指该跨链技术在 BTC 基础上提出或开发(如 pegged sidechains)、或属于 BTC 区块链的侧链(如 rootstock,elements)、或是 BTC 区块链特性的一部分(如 lightning network);基于 ETH 区块链与之类似;自有链指该跨链技术基于或属于非 BTC/ETH 的其他区块链.基于 BTC 区块链和 ETH 区块链的跨链项目数量相当,表明公有链中这二者具有更广泛的应用基础以及更迫切的跨链需求.以自有链形式构建的跨链项目,主要以构建具有跨链特性的区块链作为项目特色,并致力于寻求实现通用的、标准化的区块链接入模型.

公证人机制/侧链(中继)/哈希锁定根据 Vitalik Buterin 的分类定义[16];通信协议簇指该跨链技术主要通过规定一系列通信数据格式与协议规范等实现区块链接入.基于公证人机制的项目中,Interledger 早期版本以公证人机制为主实现不同类型账本的连接;Corda 的特色在于提供更安全的公证人选择(交易参与方共同指定)和操作模式(运行共识机制).基于侧链(中继)的项目占比较高,其中,Pegged Sidechains 是侧链最初的技术原型,提出了双向楔入的概念;RootStock,Elements 基于 BTC 侧链提供增强式智能合约功能;BTCRelay 与 Loom 均为基于 ETH 区块链的侧链,前者提供跨 BTC 与 ETH 的资产交换及智能合约应用,后者侧重构建基于 ETH 的分布式应用 DApp 开发部署环境;Lisk 则是通过搭建自有链提供 DApp 开发平台;Plasma 及其变种 Minimal Viable Plasma,Plasma Cash 设计了集成主链与侧链的树形分层网络框架;Polkadot 和 Cosmos 则分别设计了 Relay chain-Bridges-Parachains 结构和 Hub-Zone 结构的跨链网络基础平台.基于哈希锁定机制的项目中,Nolan’s atomic transfers 为哈希锁定的技术原型;Zcash XCAT 已成功演示了 ZEC 和 BTC 的跨链交易;Lightning Network 致力于成为 BTC 主流链下扩容方案,上线版本已运行上千个主网节点和上万个通道,验证了技术的可行性.通信协议簇类跨链技术由于以定义系统结构、通信协议、数据格式、工作流程等各类标准规范为主,未来能否成为主流的跨链方案,主要取决于区块链产业界各方对该协议规范的接受度以及在协议实现层面能够获得多大范围的支持.

Table 1 Summary of cross-chain technology

表 1 跨链技术汇总表

名称	时间	基于 BTC 区块链/基于 ETH 区块链/自有链	公证人机制/侧链(中继)/哈希锁定/通信协议簇	跨链作用范围
Nolan's "atomic transfers"	2013	基于 BTC 区块链	哈希锁定	系统间
Pegged Sidechains	2014	基于 BTC 区块链	侧链	系统间
Lightning Network	2015	基于 BTC 区块链	哈希锁定	系统间
Interledger	2015	自有链	公证人机制、哈希锁定	系统间
BTCRelay	2016	基于 ETH 区块链	侧链	系统间
Cosmos	2016	自有链	中继、通信协议簇	系统间
Polkadot	2016	自有链	中继	系统间
Sharding	2016	基于 ETH 区块链	–	系统内部
RootStock	2015	基于 BTC 区块链	侧链	系统间
Elements	2016	基于 BTC 区块链	侧链	系统间
Lisk	2017	自有链	侧链	系统间
Factom	2014	基于 BTC 区块链	–	系统间
Corda	2016	自有链	公证人机制	系统间
Plasma	2017	基于 ETH 区块链	侧链	系统间
Minimal Viable Plasma	2018	基于 ETH 区块链	侧链	系统间
Plasma Cash	2018	基于 ETH 区块链	侧链	系统间
Loom	2017	基于 ETH 区块链	侧链	系统间
Aion	2017	自有链	通信协议簇	系统间
Rchain	2017	自有链	–	系统内部
Block Collider	2017	自有链	通信协议簇	系统间
Nano	2017	自有链	–	系统内部
Zcash XCAT	2017	自有链	哈希锁定	系统间
Bancor	2018	基于 ETH 区块链	–	系统间
OneLedger	2018	自有链	通信协议簇	系统间

系统内部跨链指跨链技术支持在区块链系统内部的子链(如 nano 区块链内部的账户链、ETH 区块链内部的 sharding 链、rchain 中在不同命名空间运行的独立区块链)跨链;系统间跨链指支持不同区块链项目之间的跨链(如 BTCRelay 实现 ETH 与 BTC 的跨链、cosmos 原则上支持所有符合 cosmos 协议的区块链互联等).跨链作用范围目前以区块链内部以及不同区块链之间为主,提供区块链与传统系统或协议之间交互的跨链项目较少(interledger 支持分布式和传统中心化账本互联).

跨链技术在不同时期也呈现出各自的特点.比特币区块链时代期间,主要提出了跨链的几种技术原型,并重点针对 BTC 区块链容量限制及交易手续费高等问题,发展出闪电网络、Pegged Sidechains 等项目或技术;后比特币区块链时代时期,侧重于面向更多种应用场景,例如实现链上资产互换(去中心化交易所)、增强区块链系统的互操作性和可升级性、提供小型区块链系统(包括私有链、联盟链)的安全保障和价值传递等,探索具有更强扩展性的通用跨链技术.

3 跨链安全性分析

跨链技术的重要性已被业界认可,尽管近几年跨链技术得到较迅速的发展,但目前,现有的跨链技术还没有得到大规模应用.跨链的重要应用之一原子交换尚局限在个别区块链资产之间,或处于在测试链上试用的阶段,如 BTC 与 LTC[53]、LTC 与 DCR[54]、ZEC 与 BTC[55]等的原子交换实验;区块链资产的跨类别交易仍以中心化形态为主,去中心化交易平台 Bitshares,EtherDelta 等承载的交易量相对占比极低,小于总区块链资产交易量的千分之一[56];支持跨链数据通信的各类跨链协议大部分处于研发状态,暂未获得广泛的认可和共识.跨链技术面临的问题在于:一方面,区块链技术本身日新月异的发展速度,使得区块链种类、技术复杂性、应用场景多样性都在不断提升,造成对跨链技术的更新迭代提出更高的要求;另一方面,由于区块链的某些固有特性,跨链技术目前还存在一些安全性层面的难点有待攻克.从来源与影响因素方面分析,跨链技术的安全性可以包括以下两个类别.

(1) 跨链的技术原理与实现机制本身存在的安全性缺陷.伴随着区块链技术的快速发展,跨链技术仍处于演进过程中,在设计与实现上还存在信任依赖、恶意交易等安全性问题;

(2) 区块链系统的结构及特点对跨链安全性造成的影响.由于区块链的分布式账本架构与传统软件系统具有显著差异,相比于一般信息系统之间的互联互通,现有各类跨链技术还将面临一些共性的安全性挑战.

以下分析总结了 12 种主要的跨链安全性问题(其中,1~3 项属于第 1 类别,4~12 项属于第 2 类别),以期为相关领域学者研究现有跨链技术以及设计新的跨链技术提供一些参考.

(1) 公证人信任问题.公证人机制由于引入了第三方机构或组织,尽管有成熟的选举策略,但价值转移或信息交换主要依赖于公证人的诚实性,因此中心化程度较高.公证人多重签名通过随机选择在一定程度上增强了安全性,但并未完全消除相关依赖,仍然存在共谋风险.基于公证人机制的一些跨链项目也在寻求与其他技术的结合,如公证人机制的代表——Interledger 项目,在其最新协议中融合了哈希锁定机制,以提供更完备的安全保障;

(2) 侧链/中继的安全性问题.由于侧链/中继机制主要通过读取区块头来实现对事件或支付的验证,无法像主链全节点获知网络上所有交易的全貌,因此难以实现交易的全面验证,如追溯所有历史交易的 UTXO(unspent transaction output)数据、判断是否存在双重支付等.侧链/中继机制依赖于矿工的诚实性,在链失效(chain fail)或 51%攻击情况下,将导致跨链系统无法正常工作;

(3) 哈希锁定的安全性问题.根据哈希锁定的设计原理,其技术安全性主要与资金锁定机制以及锁定时间超时相关.例如,基于哈希锁定的闪电网络在系统设计时就预见到如下安全风险[24]:恶意参与者创建大量交易通道并让所有通道同时超时,导致垃圾交易信息在网络中广播并造成阻塞,从而影响正常交易;交易通道开启阶段必须保证定量的资金处于锁定状态,即用户需要采用“热钱包”保持较长时间连接到区块链网络以便能签名交易,而非“冷钱包”或离线存储等更安全的方式,因而将增加黑客盗取用户私钥的风险;交易一方如果发生数据丢失或者没有在正确的时间内广播交易,将可能存在被另一方盗取资金的风险;

(4) 孤块(orphan block)问题.在采用工作量证明(PoW)[1]为共识算法的区块链网络中,不同矿工可能在相近时间内挖出了两个或多个区块,它们均符合区块链基础协议且工作量足够,因此都属于合法区块.但由于网络传输等问题,网络中的各个节点可能会以不同的顺序接受这些区块,并在最早接收的区块基础上继续计算下一个区块.最终,这些区块中只有一个存在于最长链中,其他区块则被丢弃成为孤块.因此,当跨链网络读取所接入区块链的最新区块信息后,会出现包含相关交易数据的区块先被确认有效,随后又成为孤块的情况,从而导致跨链网络实际传递了错误的区块信息(该区块内的交易和相关数据均已被原始区块链丢弃);

(5) 长距离攻击(long range attack).在采用权益证明(PoS)[30]共识算法的区块链网络中,恶意的节点可能会预先计算出大量区块再一次性放出,导致对应的原始区块链出现重组(block reorganization).基于替换前的区块完成的跨链交易将均被撤销,跨链网络中的交易因此会被双花(double-spend),智能合约则可能出现满足触发条件并执行结束,但随后触发条件被回滚的情况.应对此类攻击较好的方法之一是设立确定性检查点[57];

(6) 阻塞超时问题.某些跨链技术通过设置延迟时间以确保跨链交易或交互数据得到区块链的确认,这在一定程度上可以避免孤块和长距离攻击问题.鉴于区块链目前有限的交易处理速度,垃圾交易(spam transactions)或短期内过多的交易数量会导致区块链网络阻塞.在当前影响力最大的公有链系统比特币和以太坊中,均出现过多次交易阻塞超过数小时甚至几天未被确认的情况.跨链形成的链联网,可能会因为跨链网络一侧的区块链阻塞而导致跨链交易超时且无法及时取消,甚至存在大面积跨链交互阻塞的风险;

(7) 竞争条件攻击(race condition attack).在原子交换类的跨链系统中,尤其容易遭受此类攻击[16].举例来

说,*A*,*B* 双方通过跨链系统提供的智能合约,尝试交换 *A* 的 1 个 BTC 和 *B* 的 10 个 ETH 资产.*A* 发送 1 个 BTC 给合约规定的地址,*B* 此时也发送同样数量的 BTC 到相同地址,并且试图取回自己的 10 个 ETH.这两笔交易均有一定概率被先确认,从而导致 *B* 同时得到 *A* 的 BTC 并取回自己的 ETH 而 *A* 一无所获的情况;

(8) 日蚀攻击(eclipse attack).区块链以及跨链网络均是以 P2P 网络为基础,由于 P2P 网络单个节点连接至其他节点数量受 TCP 连接限制,攻击者通过控制足够多的地址,可以屏蔽受害节点的所有输入和输出节点,从而使受害节点无法获得真实的网络信息.相较于节点全球分散、数量庞大的大型公有链区块链网络,组成跨链网络的节点数相对更少,更易遭受类似的日蚀攻击;

(9) 区块肿胀(block bloat)问题.通过存储跨链交易相关区块链的区块头实现数据访问是跨链技术的一种主流做法,由于区块链交易记录的不断累积,截至本文撰写时(2018 年 10 月),比特币区块链大小已达 220GB,以太坊区块链为 108GB(fast sync 模式),并在继续快速增长中.尽管区块头的容量占比较低,但跨链接入的区块链越多,需要存储的容量也会相应增多,使得跨链也会面临相同的区块膨胀问题;

(10) 失效蔓延问题.跨链形成的链联网结构中,如果其中一部分区块链因共识失败或 51%攻击[1]成功等,使这些区块链被恶意势力掌控或完全无法正常运转,链联网中错综复杂的跨链通信则会因为部分死链导致连锁式的交互失败,从而使跨链失效在链联网中大面积蔓延.2018 年以来,有 BTG,Verge 等多种区块链遭受了 51%攻击[58],造成重大的区块链资产双花问题,如跨链系统连接了这类区块链网络且未采取相应的安全防护措施,可能导致与它们相联的其他区块链网络受到影响,并造成经济损失等后果;

(11) 跨链重放攻击(cross-chain replay attacks).区块链网络发生硬分叉(hard fork)后,由于原始链和分叉链的交易地址、交易格式、密钥算法等均可能完全相同,其中一条链上的交易被恶意传送到另外一条或多条链重新广播,该交易也可能得到确认,即重放攻击(replay attacks).硬分叉是区块链中并不少见,一般出现在区块链系统升级、共识失败,或开发人员将代码进行一定程度修改后另行启动新的区块链系统.跨链重放攻击会导致跨链交易在分叉的区块链同时成立,造成用户区块链资产的损失;

(12) 升级兼容性问题.大多数区块链项目在上线后均会通过持续升级更新特性,特别是大版本升级时会影响一些关键特性,如区块大小、共识算法切换、新增功能等.当跨链接入众多区块链时,各链版本升级后对跨链协议、跨链机制的兼容,以及跨链如何应对与自适应,都是需要关注的问题.

综上,当多个区块链系统通过跨链系统相互连接后,系统的整体复杂度将大幅增加,特别是跨链系统所对接的多条区块链,在设计之初一般并未考虑跨链应用的场景,并缺乏对应的保护机制,由此引入的安全性问题需要跨链系统的设计者谨慎分析和应对.

4 总结与展望

跨链技术被认为是区块链领域发展的圣杯[59],是实现链联网的核心关键技术.本文对目前主流的跨链技术进行了系统性的介绍和对比.由于区块链领域的发展日新月异,一些新的跨链技术也在不断涌现.现有的跨链技术从形态上来看,有些是在已有区块链项目基础上的改进,实现有限的数据互联;有些是提出了一套通信协议,实现区块链间的通信;有些是提出了新的系统架构和运行模式,支持不同区块链的接入.总的来看,跨链技术仍处于初期发展过程中,跨链的推广应用需要达成更广泛的共识.

基于区块链的分布式账本技术通过区块封装、共识算法、时间戳等机制,提供了去中心化、不可篡改、无需信任等优秀特性,并结合行业需求逐步开展了各类应用开发[60];同时,系统容量、资源消耗、运行效率等技术指标也在不断提升[61,62],为实现无处不在的价值流通与交换提供了可能.跨链是实现无界价值互联的关键,其技术突破将有助于推动跨链资产转移/抵押、跨链数据共享、中心化资产交易平台、分布式应用 DApp 的跨平台开发/部署/配置、跨链智能合约应用、垂直行业私有链价值交互等应用领域的发展.开放的公有链与访问受限的私有链、联盟链之间,区块链与传统软件系统之间,也存在价值拓展和交换的应用需求,未来跨链技术有可能演变为支撑更广泛应用的网络基础设施.

跨链的初衷在于构建链联网、实现各个区块链的无缝互联,但基于区块链的本质特性以及面对愈加丰富的应用形态时,未来也可能并不会统一成一种通用的跨链技术来满足各类需求.可以预见:随着跨链技术研究的深入和应用的普及,将发展出类似当前互联网中标准化的数据接口通讯技术,各种不同的区块链系统将尽可能地提供出多种标准跨链通信接口,并抽象出典型的互操作服务供其他系统调用.在区块链系统的内部,不同的分片、子链,或支链之间,也将通过系统内部高速跨链机制实现局部信息与全局信息之间的同步与更新.除了各类线性链式区块结构,业界还发展出有向无环图(directed acyclic graph,简称 DAG)[6−8]、哈希图(Hashgraph)[63]等结构的分布式账本系统,跨链技术面临的场景更加复杂.跨链技术最终能否形成链联网的 TCP/IP 协议、实现全球区块链的广泛互联,亦或成为多种跨链技术长期共存、实现不同层次的数据连接,将与区块链自身的技术形态、应用模式发展密切相关,也有待跨链技术研究者持续探索实践.

References:

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

[2] Buterin V. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper

[3] Schwartz D, Youngs N, Britto A. The Ripple protocol consensus algorithm. https://ripple.com/files/ripple_consensus_whitepaper.pdf

[4] Bitcoin cash FAQ. https://www.bitcoincash.org/faq.html

[5] Larimer D. EOS.IO technical white paper. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

[6] Popov S. The tangle. https://iotatoken.com/IOTA_Whitepaper.pdf

[7] Churyumov A. Byteball: A decentralized system for storage and transfer of value. https://byteball.org/Byteball.pdf

[8] Arumugam S, Brandstadt A, Nishizeki T. Handbook of Graph Theory, Combinatorial Optimization, and Algorithms. 1st ed. New York: Chapman and Hall, 2016.

[9] Trujillo JL, Fromhart S, Srinivas V. Evolution of blockchain technology. https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html

[10] Li XF, Zhao H, Li F, Tan HB, Sun YN, Liu B. Electronic document anti-tampering method. Chinese Patent ZL201410436231.7, 2014-08-29 (in Chinese).

[11] Zhao H, Li XF, Zhan LQ, Wu ZC. Data integrity protection method for microorganism sampling robots based on blockchain technology. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015,43(s1):216−219 (in Chinese with English abstract). [doi: 10.13245/j.hust.15S1052]

[12] Buterin V. On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains

[13] JPMorgan Chase & Co. Quorum whitepaper. https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum%20Whitepaper%20v0.2.pdf

[14] Brown RG, Carlyle J, Grigg I, Hearn, M. Corda: An introduction. https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

[15] Cachin C. Architecture of the hyperledger blockchain fabric. In: Proc. of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.

[16] Buterin V. Chain interoperability. https://www.r3.com/download/chain-interoperability

[17] Szabo N. Smart contracts: Building blocks for digital markets. http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf

[18] Buterin V. Sharding FAQ. https://github.com/ethereum/wiki/wiki/Sharding-FAQs

[19] CoinMarketCap. Percentage of total market capitalization (dominance). https://coinmarketcap.com/charts

[20] Bjoroy TV. Ethereum sets new transaction record, outperforming Bitcoin. https://venturebeat.com/2017/08/15/ethereum-sets-new-transaction-record-outperforms-bitcoin

[21] Nolan T. Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.0

[22] Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, Poelstra A, Timón J, Wuille P. Enabling blockchain innovations with pegged sidechains. https://blockstream.com/sidechains.pdf

[23] Johnny D, Andrew P, Jonathan W, Marta P, Ben G, Mark F. Strong federations: An interoperable blockchain solution to centralized third party risks. https://arxiv.org/pdf/1612.05491.pdf

[24] Poon J, Dryja T. The Bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf

[25] Thomas S, Schwartz E. A protocol for interledger payments. https://interledger.org/interledger.pdf

[26] ConsenSys. BTC Relay's documentation. http://btc-relay.readthedocs.io/en/latest/

[27] Kwon J, Buchman E. Cosmos: A network of distributed ledgers. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md

[28] Kwon J. Tendermint: Consensus without mining. https://tendermint.com/static/docs/tendermint.pdf

[29] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. on Computer Systems, 2002,20(4): 398−461. [doi: 10.1145/571637.571640]

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

[31] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework. https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf

[32] Lerner SD. RSK white paper overview. https://bravenewcoin.com/assets/Whitepapers/RootstockWhitePaperv9-Overview.pdf

[33] How Elements works and the roles of network participants. https://elementsproject.org/how-it-works

[34] Lisk Developer Hub. Lisk's consensus algorithm. https://lisk.io/documentation/the-lisk-protocol/consensus

[35] Snow P, Deery B, Lu J, Johnston D, Kirby P. Factom: Business processes secured by immutable audit trails on the blockchain. https://www.factom.com/devs/docs/guide/factom-white-paper-1-0

[36] Hearn M. Corda: A distributed ledger. https://docs.corda.net/_static/corda-technical-whitepaper.pdf

[37] Poon J, Buterin V. Plasma: Scalable autonomous smart contracts. https://plasma.io/plasma.pdf

[38] Buterin V. Minimal viable plasma. https://ethresear.ch/t/minimal-viable-plasma/426

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

[40] OmiseGO official guide. https://cdn.omise.co/omg/officialguide.pdf

[41] Lucidity: The blockchain advertising protocol for complete data transparency. https://lucidity.tech/wp-content/uploads/2018/06/Lucidity-Whitepaper-v1.2-060618.pdf

[42] CryptoKitties: Collectible and breedable cats empowered by blockchain technology. http://upyun-assets.ethfans.org/uploads/doc/file/25583a966d374e30a24262dc5b4c45cd.pdf?_upd=CryptoKitties_WhitePapurr_V2.pdf

[43] CryptoKitties craze slows down transactions on Ethereum. https://www.bbc.com/news/technology-42237162

[44] Duffy JM. Everything you need to know about loom network. https://medium.com/loom-network/everything-you-need-to-know-about-loom-network-all-in-one-place-updated-regularly-64742bd839fe

[45] Spoke M, Nuco Engineering Team. Aion: Enabling the decentralized Internet. https://aion.network/media/en-aion-network-technical-introduction.pdf

[46] Miller A, Xia Y, Croman K, Shi E, Song D. The honey badger of BFT protocol. In: Weippl E, ed. Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security (CCS 2016). New York: ACM Press, 2016. 31−42. [doi: 10.1145/2976749.2978399]

[47] Eykholt E, Meredith LG, Denman J. RChain architecture documentation. https://media.readthedocs.org/pdf/rchain-architecture/stable/rchain-architecture.pdf

[48] Block Collider Team. Block collider whitepaper. https://www.blockcollider.org/bc_whitepaper_zh.pdf

[49] LeMahieu C. Nano: A feeless distributed cryptocurrency network. https://nano.org/en/whitepaper

[50] Davies J. Web-Based XCAT tool for easy ZEC/BTC atomic trading. https://github.com/ZcashFoundation/GrantProposals-2017Q4/files/1363993/29.pdf

[51] Hertzog E, Benartzi G, Benartzi G. Bancor protocol white paper. https://about.bancor.network/static/bancor_protocol_whitepaper_en.pdf

[52] OneLedger. A universal blockchain protocol enabling cross-ledger access through business modularization. https://oneledger.io/wp-content/uploads/2018/04/oneledger-whitepaper.pdf

[53] Fromknecht C. Connecting blockchains: Instant cross-chain transactions on lightning. https://blog.lightning.engineering/announcement/2017/11/16/ln-swap.html

[54] Young J. First-ever atomic cross-blockchain swap between litecoin and decred completed. https://btcmanager.com/first-atomic-swap-between-litecoin-decred-complete/

[55] Redman J. Engineers demonstrate Zcash/Bitcoin atomic swaps. https://news.bitcoin.com/engineers-demonstrate-zcashbitcoin-atomic-swaps/

[56] CoinMarketCap. 24 hour volume rankings (all exchanges). https://coinmarketcap.com/exchanges/volume/24-hour/all/

[57] Buterin V, Griffith V. Casper the friendly finality gadget. https://arxiv.org/abs/1710.09437

[58] Duncan C. Verge, Bitcoin gold, what's next? The 51% attacks are just beginning. https://cryptoinsider.21mil.com/verge-bitcoin-gold-xvg-btg-51-attacks-just-beginning/

[59] Deichler A. Interoperability: the holy grail of blockchain. https://www.afponline.org/trends-topics/topics/articles/Details/interoperability-the-holy-grail-of-blockchain

[60] Tsai WT, Yu L, Wang R, Liu N, Deng EY. Blockchain application development techniques. Ruan Jian Xue Bao/Journal of Software, 2017,28(6):1474−1487 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[61] Yu H, Zhang ZY, Liu JW. Research on scaling technology of Bitcoin blockchain. Journal of Computer Research and Development, 2017,54(10):2390−2403 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2017.20170416]

[62] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):482−494 (in Chinese with English abstract). [doi: 10.16383/j.aas.2016.c160158]

[63] Baird L. The swirlds hashgraph consensus algorithm: Fair, fast, Byzantine fault tolerance. https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

附中文参考文献:

[10] 李晓风,赵赫,李芳,谭海波,孙怡宁,刘冰.一种电子文件防篡改方法.ZL201410436231.7.2014-08-29.

[11] 赵赫,李晓风,占礼葵,吴仲城.基于区块链技术的采样机器人数据保护方法.华中科技大学学报(自然科学版),2015,43(s1):216−219. [doi: 10.13245/j.hust.15S1052]

[60] 蔡维德,郁莲,王荣,刘娜,邓恩艳.基于区块链的应用系统开发方法研究.软件学报,2017,28(6):1474−1487. http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[61] 喻辉,张宗洋,刘建伟.比特币区块链扩容技术研究.计算机研究与发展,2017,54(10):2390−2403. [doi: 10.7544/issn1000-1239.2017.20170416]

[62] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):482−494. [doi: 10.16383/j.aas.2016.c160158]

李芳(1985－),女,湖北恩施人,博士,工程师,主要研究领域为物联网,区块链技术,测量与控制.

李卓然(1994－),女,硕士,主要研究领域为空间分析,区块链技术.

赵赫(1984－),男,博士,高级工程师,主要研究领域为区块链技术,计算机应用技术,网络安全.