

引用格式:梁瑞岩,隋爱娜,韩鹏斌,姚广政.面向Fabric的跨链可行性方法研究[J].中国传媒大学学报(自然科学版),2023,30(01):47-52.

文章编号:1673-4793(2023)01-0047-06

面向Fabric的跨链可行性方法研究

梁瑞岩,隋爱娜*,韩鹏斌,姚广政

(中国传媒大学计算机与网络空间安全学院,北京 100024)

摘要:随着区块链技术不断地发展,Fabric框架已成为目前最主流的联盟链框架。面对不同业务需求,区块链研发人员往往为不同的应用场景构建不同的区块链,这种单链架构的业务链面临业务复杂、吞吐率低、拓展难等风险,跨链技术能帮助简单业务链完成互操作从而实现复杂的业务功能。本文综合分析了目前主流跨链技术的优缺点,提出了基于中继链与跨链中间件的跨链模型,并在此模型下基于跨链协议、背书策略交易证明、跨链事务管理实现Fabric跨链智能合约互操作。经过实验与性能分析表明本文提出的方法是可行的。

关键词:区块链;Fabric;跨链

中图分类号:TP311.13 **文献标识码:**A

Research on cross-chain feasibility method for Fabric

LIANG Ruikui, SUI Aina*, HAN Pengbin, YAO Guangzheng

(School of Computer and Cyber Sciences, Communication University of China, Beijing 100024, China)

Abstract: With the continuous development of blockchain technology, Fabric framework has become the most mainstream consortium blockchain framework. Faced with different business requirements, blockchain developers often build different blockchains for different application scenarios. This single-chain business chain faces risks such as complex business, low throughput and difficult expansion. Cross-chain technology can help simple business chains to interoperate and realize complex business functions. In this paper, the advantages and disadvantages of the current mainstream cross-chain technologies are comprehensively analyzed, and a cross-chain model based on relay chain and cross-chain middleware is proposed. Under this model, Fabric cross-chain smart contract interoperability is realized based on cross-chain protocol, endorsement policies transaction proof and cross-chain transaction management. Experiments and performance analysis show that the method proposed in this paper is feasible.

Keywords: blockchain; Fabric; cross-chain

1 引言

自十三五国家信息化规划首次将区块链纳入战略性新兴产业前沿技术范畴,区块链技术在我国金融、物流、版权保

护等领域得到加速应用和推广。BlockData 2022年企业区块链状况报告指出,Hyperledger Fabric是最受欢迎的企业级区块链解决方案,全球前100家上市公司中,有38%的公司采用了该解决方案,其中包括微软、亚马逊、

基金项目:国防基础科研计划(WDZC2022601A103)

作者简介(*为通讯作者):梁瑞岩(1998-),男,硕士研究生,主要从事区块链跨链研究。Email:476020520@qq.com;隋爱娜(1972-),女,博士,教授,主要从事网络安全与区块链研究。Email:aina@cuc.edu.cn;韩鹏斌(1995-),男,博士研究生,主要从事可搜索加密,属性基加密与区块链研究。Email:cybercommunication@163.com;姚广政(1999-),男,硕士研究生,主要从事网络与系统安全研究。Email:1013049235@qq.com

Alphabet 和 Visa^[1]。但在目前Fabric的实际应用场景中,企业或高校通常会将业务场景抽象为结构单一且复杂的区块链方案,如果之后业务或联盟体系发生改变,需要构建新的区块链,而且单链区块链存在业务复杂难以管理、区块链业务吞吐率低、存储数据多难拓展的问题。所以如何打破各单链区块链数据孤岛,实现区块链之间价值传递,成为区块链技术发展所面临的极大挑战。区块链跨链技术的提出最早出现于2012年Ripple发布的跨账本互操作协议 Interledger Protocol (ILP)中^[2],跨链技术的提出就是为了解决区块链之间信息孤岛的难题,提高区块链之间的交互性、可移植性、可扩展性。目前区块链跨链方案已初具规模,Polkadot、Cosmos等已经成为全球应用最广泛的跨链平台,通过这些平台用户可以在区块链之间以互不信任的方式传输区块链数据,但以上平台因为存在性证明机制,难以直接利用到Fabric架构中。本文通过引入中继链技术适配跨链中间件、跨链协议,设计了一套适用于Fabric联盟链的跨链方法,实现Fabric业务链之间智能合约互操作。

2 区块链跨链技术

2.1 跨链技术

出于改进基于区块链的应用程序的需要,区块链开发人员使用区块链分片^[3]、可附加区块链^[4]等技术来改善区块链的可扩展性、安全性和隐私,为不同应用场景创造用例并响应不同的需求,这种行为创建了不同的区块链,导致了更加混乱的区块链生态系统。基于区块链的应用有很强的隔离性,会导致区块链网络之间形成孤岛。跨链技术的主要目的是为了连接独立的区块链网络,根据跨链技术实现方法的不同分为四大类:公证人机制、哈希锁定^[5]、分布式私钥控制、侧链/中继链^[6]。

公证人机制是通过公证人监控多个链上发生的交易,与单一公证人相比一组公证人分散了协商的过程。公证人机制虽然降低了跨链交易的难度,但是这种信任机制通常放在集中方。与侧链相反,公证人机制不是区块链的扩展方法,而是第三方软件的实现方法。

哈希锁定技术通过哈希函数将资产锁定一段时间,并通过交换哈希值明文完成虚拟资产交易。哈希锁定应用场景大多限制在跨链资产转移,并不能实现跨链智能合约的互操作。

分布式私钥控制将完整的密钥分为多个密钥碎片,当发生资产转移提案时分布式节点使用密钥碎片对提案签名,当提案获得签名的数量大于签名阈值时该交易

视为有效,同样分布式私钥控制也只适用于跨链资产转移。Agentchain使用多重签名在区块链之间交换资产^[7],交易员将所拥有的资产映射到代理链,代理链将多个交易运营商合并在一个交易组中。该组成员使用多重签名生成一个帐户作为包含资产的存款池,然后锁定令牌,在出现恶意交易情况时引入仲裁机制。

侧链/中继链的核心是双向锚定^[8]。比特币网络中使用侧链实现与现有区块链互操作、扩展、升级,现有区块链将侧链作为自身的延伸,两条链之间通过跨链通信协议与侧链进行通信,侧链的设计结构由主链共识协议、侧链共识协议、跨链通信协议组成。侧链/中继链跨链技术与上述三种跨链技术相比,应用场景更加广泛,同时也是目前应用最广泛的技术。应用中继链实现跨链的平台有Polkadot与Cosmos。

Polkadot是一个连接区块链局域网到互联网的网络^[9],为并行链提供了SDK开发基础,通过SDK开发的并行链使用全球一致的数据结构,比特币网络、以太坊网络都不是通过Polkadot提供的SDK直接开发的,所以这些异构区块链不能当作并行链直接接入跨链网络。Polkadot是基于Substrate构建的,Substrate是一个用于创建加密货币和其他分散系统的框架,它保证了对WebAssembly、轻型客户端和链下工作者的跨语言支持,允许与其他技术集成。Polkadot支持基于状态转换验证的互操作性,该验证由链中继验证器完成。Parachains通过跨链消息传递协议(CROSS-CHAIN MESSAGE PASSING, XCMP)进行通信,这是一种基于Merkle树的排队通信机制。这种跨链协议通过默克尔证明保证跨链交易在多个区块链上的发生。

Cosmos网络中将独立平行区块链的分散网络称为Zone,Zone本质上是基于Tendermint共识机制的并行链^[10]。不同分区之间的通信通过链间通信(INTER-BLOCKCHAIN COMMUNICATION, IBC)协议将跨链消息路由到目标区块链,发送跨链交易时通过锁定源链的资产并传输跨链交易证明到目标链。

目前主流的跨链技术都是在公有链架构下实现,虽然Polkadot与Cosmos也支持异构联盟链接入跨链网络,但将联盟链接入公链势必导致网络隐私性变差和底层代码修改的问题。所以设计一项专门面向联盟链的跨链方法具有十分重要的意义。

2.2 Fabric联盟链跨链难点

本文结合目前已有跨链方法分析Fabric架构设计,总结出实现Fabric联盟链跨链有以下难点:

(1)业务链架构差异:不同业务的区块链具有不同的网络架构、拓扑结构、证书颁发形式、身份认证体系和共识算法等差异,这使得不同链之间进行跨链交易时面临一定的技术挑战。

(2)交易存在性验证困难:基于默克尔证明的交易存在性验证是常用的跨链认证手段。但是,Fabric使用DataHash字段标记区块内数据的变化,在区块头设计中并没有相关的默克尔根字段。因此,实现跨链交易辨认互认仍然具有一定的挑战性。

(3)安全机制差异:当涉及到联盟链和公链、平台和平台之间进行衔接时,由于安全机制的差异,如智能合约背书者不同、准入机制严格程度的差异、权限配置差异等因素,导致平台之间的互信条件不成立。

(4)联盟链跨链交易难以传递:联盟链和公链在准入机制上存在差异,因此联盟链很难直接利用公链轻节点和Merkle Proof收集区块链交易进行跨链交易传递。在联盟链架构下,跨链交易难以传递到目的链。

(5)跨链交易原子性、一致性难以保证:跨链交易类似于数据库事务,需要保证对交易来源链与交易目的链修改数据状态或交换数据的操作要么同时发生,要么同时不发生。但如果目的链因为网络延迟而超时或目的链发生故障导致跨链失败,那么跨链交易来源链上的数据状态也需要回滚至交易未发生之前。但是跨链区块链节点都是对等节点且没有高权限的管理节点,难以保证跨链交易原子性、一致性。

3 基于中继链的跨链技术方案

3.1 跨链模型

相较于其他跨链方案,中继链方案具有较高的安全性、智能合约互操作实现难度低、系统可拓展性等优势。针对Fabric框架跨链难点,本文通过中继链与跨链中间件传递跨链信息帮助联盟链完成智能合约互操作。本文设计的跨链模型如图1所示。

跨链模型最小五元组定义为 (R, M_A, C_A, M_B, C_B) 。其中 M_A 为使Fabric构建的业务链A, C_A 是为 M_A 提供跨链基础功能的跨链中间件, M_B 为使用Fabric构建的业务链B, C_B 是为 M_B 提供跨链基础功能的跨链中间件, R 为跨链消息处理核心中继链。中继链与跨链中间件的模型能提供统一、简单且拓展性高的跨链功能,相比直接交互形式的跨链方法本模型将接入新业务链 $O(n)$ 复杂度降为 $O(1)$ 。

模型中为了跨链互操作指令的传递需要为基础的

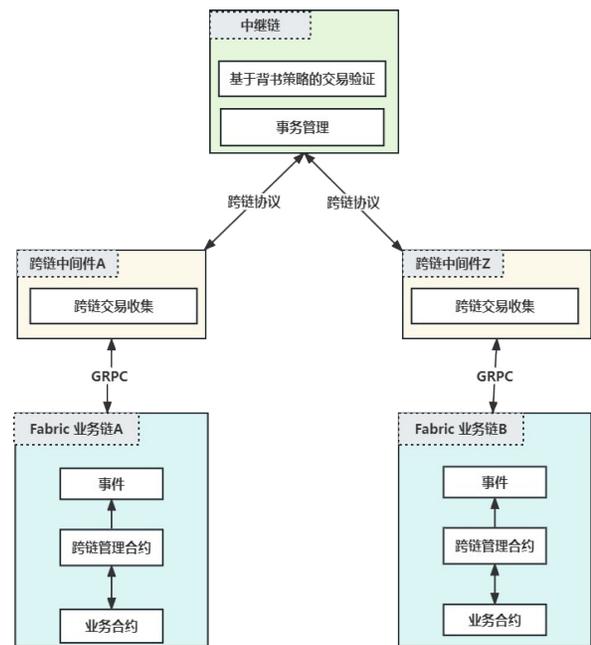


图1 跨链模型

应用链C增加功能, $C=(CC_i, S, E)$,其中 CC_i 为业务链实现业务的Fabric链码。 S 是跨链管理合约,跨链管理合约为所有需要跨链的普通合约提供一个通用的接口,除了提供接口外,跨链管理合约通过抛出Fabric事件 E 的形式将跨链交易发送到区块链系统外。

3.2 跨链架构

本文根据跨链业务需求将跨链系统分层设计,并根据内聚性高、耦合性低的原则,实现应用链管理、跨链合约管理、跨链交易存在性证明、跨链事务、跨链交易收集等功能。跨链模型的架构如图2所示。

其中,第一层为协议层,第二层为跨链服务层,第三层为中继链网络基础层。协议层定义了各个跨链消息字段的含义;跨链服务层提供跨链交易的基本组成功能;基础层则为中继链提供基本的运行环境。跨链模型的各个层次相互配合,实现跨链交易的有效性验证、跨链交易的收集以及跨链交易的事务管理等功能。

3.3 跨链协议

由于不同区块链之间存在底层结构和共识协议等方面的差异,因此区块链之间的交互通常较为困难。为此,本文设计了一套区块链信息交互协议,以实现区块链之间的信息交互。协议采用灵活、统一、可靠的设计方式,实现了跨链消息的传递。跨链协议中涉及到的字段偏多,其中最主要的几个字段设计如表1所示。

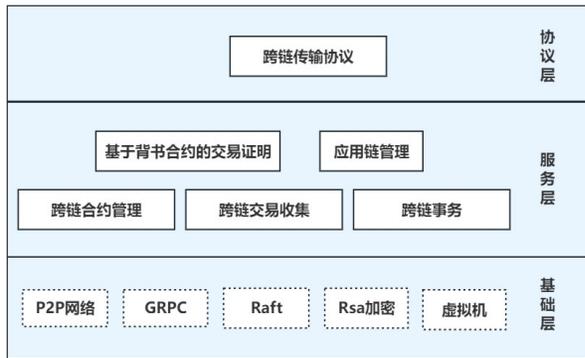


图 2 跨链模型架构图

表 1 跨链协议描述表

参数	描述
From-Contract	定位跨链交易发起智能合约
From-Function	定位跨链交易发起函数
From-Args	跨链交易发起方调用函数的传入参数
To-Contract	定位跨链交易接收智能合约
To-Function	定位跨链交易接收方函数
To-Args	跨链交易接收方调用函数的传入参数
Payload	跨链调用的内容字段(主要包含回调函数、回调参数、交易证明等)

3.4 跨链交易收集

针对业务更加复杂的联盟链跨链场景中,轻节点维护账本状态难以记录智能合约互操作的问题,本文提出一种适用于Fabric的跨链交易收集方案。

业务链中普通的业务合约需要首先调用跨链管理合约,调用方法采用Fabric的InvokeChaincode方法,在Fabric开放文档中描述该函数是在本地使用相同的交易上下文调用指定链码的invoke方法,这个方法是Fabric预留的跨链接口,但该方法只局限于跨通道不能实现跨组织。InvokeChaincode方法可以实现在一个智能合约中调用另一个通道或相同通道的智能合约,在分布式身份认证场景中身份链Query Certificate链码通过该方法调用跨链合约抛出跨链事件。跨链中间件以DAPP的形式提供给业务链使用,中间件通过Fabric SDK注册交易监听事件,同时跨链中间件还需要监听主链上的区块高度,将需要跨链的交易信息收集起来,组装成跨链协议消息包。在跨链交易打包时,中间件需要进行一定的筛选,筛选条件主要包括跨链交易是否合法、跨链交易是否过期、跨链交易是否存在重复交易等。在筛选完成后,跨链交易会被打包成一个新的块,并通过跨链协议广播到整个中继链网络中。跨链交易收集时序图如图3所示。

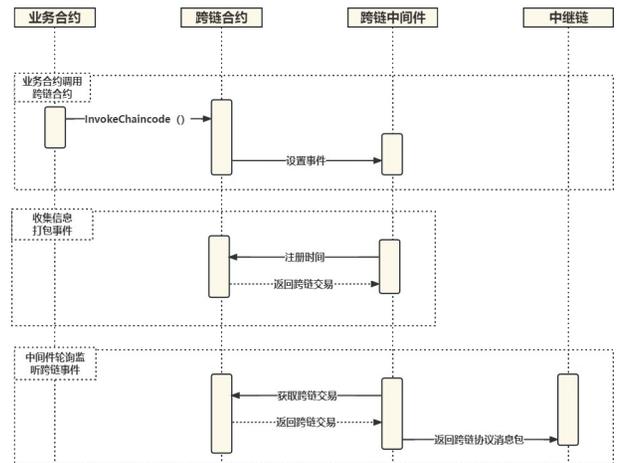


图 3 跨链交易收集时序图

3.5 基于背书策略的交易证明与验证

交易证明是保证跨链交易原子性的核心,但Fabric架构底层区块数据结构中没有默克尔树,无法通过跨链中间件构造SPV证明。在Fabric交易过程中,客户端节点发起交易请求后,由链码背书节点接收交易请求并根据请求信息执行链码生成交易读写集,最终链码对交易读写集签名结果被发送给客户端节点,普通节点收到区块后验证交易有效性与交易存在性的凭据,完成交易背书。通过对Fabric交易流程的分析,本文设计基于Fabric背书策略并构造交易存在性证明,具体证明构造流程如图4所示。

基于背书合约的交易证明构建分为两个流程:获取交易与获取交易背书。获取交易流程中,通过Fabric SDK可以直接查询区块链存储在交易数据库中数据,通过交易ID查询跨链交易数据。TransactionAction=(Header, Payload, Unrecognized, sizecache),通过解析Payload字段可以得到链码执行结果的相关数据。获取交易背书流程中,将跨链交易中涉及交易请求的ChaincodeActionPayload解析为交易回执与背书信息,其中背书信息包含对读写集的签名和背书策略组。

当跨链的区块链接入跨链系统时,业务链将底层联盟、客户端、成员、管理员等的证书与Msp Id发送到中继链,中继链采用键值对的形式将每一个Msp实体与其对应的证书存储起来。在交易证明验证阶段每当需要验证交易存在性时,中继链首先使用跨链中间件发送跨链协议数据包中的证书与键值对进行匹配,如果失败表明该交易是伪造的,如果成功继续使用跨链协议数据包中的公钥尝试解签背书策略中的密文,如果成功则验证跨链交易已在跨链来源链上发生。

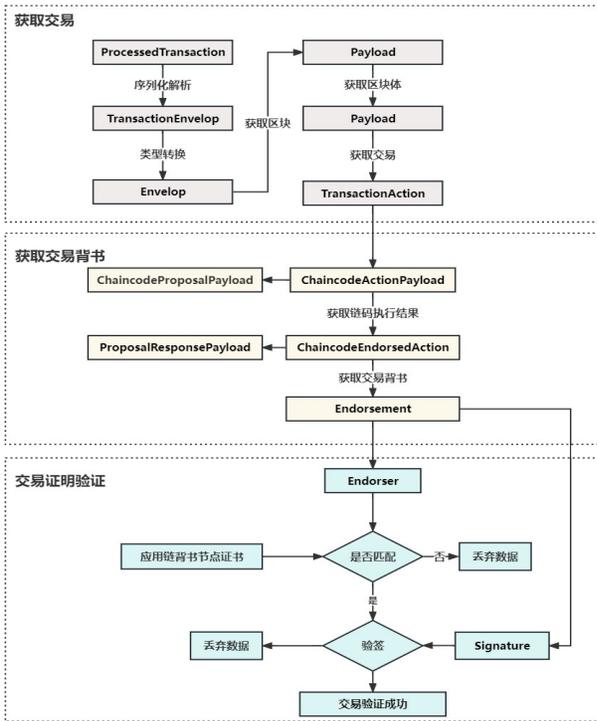


图4 基于背书合约的交易证明与验证流程

3.6 跨链事务管理

跨链事务指跨链交易需要保证原子性、一致性,传统分布式系统一般采用两阶段提交或三阶段提交来实现系统的一致性,而区块链系统一般保证事务性的技术有哈希锁定与分布式私钥控制等,哈希锁定与分布式私钥控制更适合用于资产转移的跨链场景,并不适合智能合约互操作场景。跨链事务方案设计使用提交与回滚技术来实现跨链交易的原子性。

跨链事务流程如图5所示。



图5 跨链事务流程

中继链收到跨链交易后将跨链交易分为多个子交易,其中包括跨链发起子交易、跨链调用子交易、跨链回滚子交易、跨链回调子交易。跨链发起子交易与跨链调用子交易分别由来源链与目的链完成,跨链回滚子交易与跨链回调子交易由中继链根据前两阶段子交易完成情况发起。

4 实验结果分析

本文的实现测试环境如表2所示。

表2 软硬件测试环境

名称	版本型号
系统	Ubuntu 20.04
CPU	Intel(R)_Core(TM)_i7-7700_CPU_@_3.60GHz
内存	4GB 2133MHz
fabric	V1.4.3
fabric-sdk-go	V1.0.0
go	1.15.6
docker	20.10.7
docker-compose	1.23.2

本文跨链区块链网络配置如表3所示。

表3 跨链区块链网络配置

区块链网络	网络拓扑	共识算法
中继链	Org1.Peer0 Org1.Peer1 Org1.Peer2 Org1.Peer3	Solo
交易来源链	Org2.Peer0 Org2.Peer1 Org3.Peer0 Org3.Peer1	4节点 Raft
交易目的链	Org4.Peer0 Org4.Peer1 Org5.Peer0 Org5.Peer1	4节点 Raft

目前区块链系统还没有一个统一的测试标准,本文通过 Caliper 测试框架测试两条 Fabric 链的智能合约性能,结果如图6与图7所示。

Caliper report

Summary of performance metrics

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
UavRegister	5000	0	18.8	2.07	0.04	0.35	18.7
UavUpdate	638	0	21.6	2.14	0.06	0.30	20.6
UavQuery	3772	0	129.8	0.19	0.01	0.04	129.6

图6 目的链压力测试报告

Caliper report

Summary of performance metrics

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
TaskRegister	5000	0	9.6	2.13	0.04	0.55	9.6
TaskUpdate	423	0	14.2	2.04	0.04	0.42	13.5
TaskQuery	2854	0	98.3	0.30	0.01	0.05	98.1
RemoteQueryCa	2576	0	88.7	0.39	0.01	0.06	88.5

图7 来源链压力测试报告

从图中可以分析出普通查询合约每秒钟业务吞吐量大约都有100笔左右。这个结果受限于实验机器硬件配置与 Caliper 测试节点数。

Caliper 只能对普通智能合约进行压力测试,但跨链业务分为跨链调用和跨链回调,本文通过 Fabric SDK 进行跨链合约压力测试,测试结果如图8所示。

```

[frabsd/fab] 2023/02/22 01:18:57 UTC - msp. (*identity).Verify -> DEBU Verify: digest = 00000000 74
81 30 ba a8 fc 82 1b 89 21 8a bc b9 24 a0 ef [t.0.....!..$..]
00000010 eb 03 2c a2 f4 ee 4d d9 77 d9 32 b1 5e e0 3d 2e [.....M.W.2.^..]
[frabsd/fab] 2023/02/22 01:18:57 UTC - msp. (*identity).Verify -> DEBU Verify: stg = 00000000 30 45
02 21 00 b5 09 4c 5f 07 01 0f 0f de c0 84 [E...L.g.o....]
00000010 96 e2 fb 2f 5d 29 e3 ad b2 8d b4 bc ba 11 9f fc [.....]
00000020 16 0e 07 8f f7 02 20 28 0f 05 aa e4 88 a3 77 8b [.....(.....W.]
00000030 c0 6c 1f 1d fe 1c 64 5c 21 56 d0 d9 6d f9 b1 13 [.....d\IV..n...]
00000040 35 05 c5 b6 72 c1 81 [5.....]
2023/02/22 09:18:57 *****Remote Verify END*****
2023/02/22 09:18:57 Cross-chain Start At 2023-02-22 09:17:57.06249775 +0800 CST m=+4.354368080_End
At 2023-02-22 09:18:57.06249775 +0800 CST m=+64.354368080,Nums:5135,tline duration:1m0s

```

图 8 跨链压力测试

测试中跨链调用为 RemoteQueryCa 调用 UvaQuery, 调用成功之后 UvaQuery 回调 TaskUpdate。测试结果显示一分钟内可以完成 5135 次跨链业务, 跨链业务 TPS 为 85.6, 跨链对于普通合约的影响为 33%。

通过 Caliper 性能测试结果显示跨链来源链的跨链调用成功, 同时证明了通过本文设计的跨链方法能完成区块链之间信息的传递。

5 结论

本文通过引入中继链技术, 设计了一套适用于 Fabric 联盟链的跨链方法。在跨链互操作性方面, 与只能实现简单的跨链资产转移的其他跨链方法相比, 本方法基于 Fabric 数据结构特点设计了基于背书策略的交易证明、跨链交易收集方案与跨链事务管理, 实现了 Fabric 业务链之间的智能合约互操作。与其他跨链方法相比, 本方法在不牺牲安全性的前提下无需修改代码匹配安全机制, 只需在业务链中添加跨链合约管理链码。本文设计的跨链方法, 跨链性能受限于中继链与跨链中间件交易存在性验证的速度, 这将是未来的工作重点。

参考文献 (References):

[1] The State of Enterprise Blockchain in 2022[EB/OL].https://www.blockdata.tech/blog/general/the-state-of-enterprise-

blockchain-in-2022/, 2022-11-16.

- [2] Hope-Bailie A, Thomas S. Interledger: Creating a standard for payments [C]//Proceedings of the 25th International Conference Companion on World Wide Web. 2016: 281-282.
- [3] Wang G, Shi Z J, Nixon M, et al. Sok: Sharding on blockchain [C]//Proceedings of the 1st ACM Conference on Advances in Financial Technologies. 2019: 41-61.
- [4] Nunes H C, Lunardi R C, Zorzo A F, et al. Context-based smart contracts for appendable-block blockchains [C]//2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020: 1-9.
- [5] Deng L, Chen H, Zeng J, et al. Research on cross-chain technology based on sidechain and hash-locking [C]//Edge Computing-EDGE 2018: Second International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 2. Springer International Publishing, 2018: 144-151.
- [6] Back A, Corallo M, Dashjr L, et al. Enabling blockchain innovations with pegged sidechains[J]. 2014.
- [7] Li D, Liu J, Tang Z, et al. Agentchain: A decentralized cross-chain exchange system [C]//2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (Trustcom/BigdataSE). IEEE, 2019: 491-498.
- [8] Teutsch J, Straka M, Boneh D. Retrofitting a two-way peg between blockchains[J]. arXiv preprint arXiv:1908.03999, 2019.
- [9] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework[J]. White paper, 2016, 21(2327): 4662.
- [10] CosmosNetwork [EB/OL]. https://cosmos.network/, 2019-11-15.

(上接第 14 页)

2020:495-499.

- [35] T Shitomi, T Nakatogawa, A Sato, K Furuya and M Okano. Spectral Efficiency Evaluation of an NR-Based 5G Terrestrial Broadcast System for Fixed Reception[C]. in IEEE Transactions on Broadcasting, 2022,68(2):487-500 .
- [36] L Richter and U H Reimers.A 5G New Radio-Based Terrestrial Broadcast Mode: System Design and Field Trial[C]. in IEEE Transactions on Broadcasting, 2022, 68(2) : 475-486.
- [37] 3GPP R1-1913259.On the performance evaluation of HARQ-based time-interleaving for LTE-based 5G terrestrial broadcast [C]. TSG RAN WG1 #99, Reno, USA, 2019.
- [38] 3GPP R1-1913439.On time and frequency interleaving for terrestrial broadcast[C]. TSG RAN WG1 #99, Reno, USA,

2019.

- [39] 3GPP R1-1913095.Information on Time Interleaving in State-of-the-Art Terrestrial Broadcast Systems[C]. TSG RAN WG1 #99, Reno, USA, 2019.
- [40] 3GPP R1-1912331.CRBI-based interleaver for 5G terrestrial broadcasting[C]. TSG RAN WG1 #99, Reno, USA, 2019.
- [41] 3GPP S2-2106434.Rel-18 Proposal to support LTE-based 5G Terrestrial Broadcast (Rel-16 EnTV) connected to 5GC[C]. TSG-SA WG2 #146-e, Elbonia, 2021.
- [42] Success for the Nakolos team at the International Broadcasting Convention 2022 (IBC) in Amsterdam [EB/OL]. [2022-09-22]. https://www.nakolos.com/2022/09/15/world-premier-at-ibc/.

编辑:龙学锋