软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

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

基于区块链的跨部门业务材料传递机制*

肖宗水[1,2]，车正伟[1]，孔兰菊[1]，李庆忠[1,2]，闵新平[1]，闫中敏[1]

[1](山东大学软件学院 山东 济南 250101)
[2](山大地纬软件股份有限公司 山东 济南 250100)

通讯作者：孔兰菊 E-mail: klj@sdu.edu.cn

摘要：提出基于区块链技术的跨部门业务材料传递机制，确保业务材料的真实可信，解决了政务流程中材料传递成本高、风险大的问题。该方法首先建立了基于区块链的跨部门工作流协同机制，提出业务流程与区块链数据的映射算法，通过区块链在各部门间协同业务流程状态及业务材料，降低业务材料验证成本；然后，设计了基于共识算法的业务材料真实性保证机制，防止了业务材料出现“双花问题”，保证了业务材料真实性、一致性；最后，提出了业务材料授权使用机制，明确了业务材料的使用规则，确保业务材料传递过程完全可控。经过优化的区块链系统吞吐量能满足智能政务环境中的跨部门业务材料传递需求。

关键词：区块链、工作流、跨部门、共识算法、业务材料
中图法分类号：TP311

Cross-departmental Business Material Delivery Mechanism based on Blockchain

XIAO Zong-Shui[1,2]，CHE Zheng-Wei[1]，KONG Lan-Ju[1]， LI Qing-Zhong[1,2] ，MIN Xin-Ping[1]，YAN Zhong-Min[1]

[1](College of Software, Shandong University, Jinan 250101, China)

[2](Dareway Software Co., Ltd., Jinan 250100, China)

Abstract: We propose an inter-departmental business material delivery mechanism based on blockchain technology to ensure the authenticity of business materials and solve the problem of high cost and high risk of material transfer in government processes. Firstly, we establish a cross-department workflow coordination mechanism based on blockchain and propose a mapping algorithm between business process and blockchain data. The blockchain is used to coordinate business process status and business materials among departments to reduce the cost of business material verification. Then, the real-time guarantee mechanism of business materials based on consensus algorithm is designed to prevent the "double-spending problem" of business materials, and the authenticity and consistency of business materials are guaranteed. Finally, we propose an authorization mechanism of business materials and clarify the usage rules of business materials to ensure that the business material delivery process is fully controllable. The throughput of the optimized blockchain system can meet the requirements for cross-departmental business material delivery in an intelligent government environment.

Key words: Block chain; workflow; cross-departmental ; Consensus algorithm; Business materials

一个业务通常需要多部门协同完成，这就需要多份不同的业务材料在多个部门间传递，各个部门均需要保证所接受到的业务材料的真实性、一致性。但是各个部门往往相互独立，对业务材料的操作过程互不

*基金项目：国家自然科学基金资助项目(No.61772316)；山东省科技发展计划资助项(No.2016GGX101008，No.2017CXGC0702)；山东省自主创新重大专项资助项目(No.2016ZDJS01A09)；山东省泰山产业领军人才工程专项经费。

Foundation items: This project is partially supported by NSFC No.61772316; the Science and Technology Development Plan Project of Shandong Province No. 2016GGX101008, No. 2017CXGC0702; Shandong Province Independent Innovation Major Special Project No. 2016ZDJS01A09; the Taishan Industrial Experts Programme of Shandong Province.

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00

CNKI 在线出版时间: 0000-00-00

透明，即业务办理人无法感知业务部门对业务材料执行的具体操作。

各部门之间可以通过相互开放接口或建立统一的中心化平台的方式，降低业务材料验证成本，提高业务协同效率。但无论是相互开放接口或建立统一中心化平台的方式，均难以保证业务材料的真实性、一致性，同时其建设成本与维护成本高昂。中心化平台由单一的服务商管理与维护，相对封闭，业务材料所有权属于用户，业务办理人难以控制业务材料的使用过程，同时平台内部人员私自篡改数据难以发现，被篡改的数据也会被当成真实数据；若采用各部门相互开放接口的方式，业务办理人仍难以控制业务材料的使用过程，且难以防止业务办理人与业务员协同造假等问题。

区块链具有不可篡改、全网集体维护数据等特性，可保证业务材料不可篡改、真实可信[1]，明确业务材料的所有权、控制权、使用权，故可基于区块链构建跨部门的工作流协作机制。

Weber 等人基于 Ethereum 区块链平台提出了一种模型驱动的协作业务流程实现方法[2]。他们在扩展 BPMN 时引入了支付和数据转换等，业务流程中的各方通过消息交换进行交互，交换的消息以交易的形式发送到区块链上。Prybila 等人提出了一种替代方法，即通过专用令牌监视在比特币区块链上执行的业务流程[3]。这两种方法都假定协作业务流程中的各方通过消息交换进行交互，并使用区块链平台记录交换的消息，检查或强制这些交换以某种顺序发生[4]。实际上是将区块链平台作为协作过程中的一个执行组件，但是大多数组件都是脱链的，各方之间的实际交互是通过区块链之外的消息交换进行的，大文件的业务材料不能通过区块链进行传递。

Garcia-Banuelos 等人提出了将 BPMN 流程模型转换为智能合约[5]。该方法使用区块链作为协调机制来维护流程的状态，并确定接下来可能发生的任务或事件。然而，这种方法并不保证业务流程中交换的消息透明、可控。

Hull 等人讨论了业务流程建模的前景，提出了以 Artifact 为中心的基于区块链的业务流程协作模型[6]。Norta 提出了将区块链技术引入到基于编排模型的业务流程协作中[7]，这种模型类似于协作图，因为它依赖于通过消息交换进行交互。这两个研究只概述了基于区块链的业务流程可行性架构的建模和执行，不提供任何实现或评估。

综上，之前的研究在整个业务流程中，区块链只用于记录和监视每个账户执行的业务流程之间的消息交互。然而，用户并不知道整个业务过程中自己的业务材料的操作过程，导致对业务材料失去控制。而且，整个业务过程也不能保证各部门对业务材料操作的真实性。

针对于现有工作流模型中在跨部门协作过程中存在的难以保证业务材料真实性、难以保证防范‘双花’问题、难以保证业务材料操作过程透明等，本文设计基于区块链的跨部门工作流协作机制，明确业务材料的所有权、控制权、使用权，保证业务材料的真实性、正确性，提高业务协同效率，杜绝人为因素引发的道德风险等问题。各部门通过区块链获取工作流所需的业务材料，业务办理人拥有业务材料的所有权，业务部门拥有业务材料的使用权；设计业务材料正确性保证机制，防止业务材料出现“双花问题”，保证业务材料的正确性；设计业务材料授权使用机制，明确业务材料的使用过程，防止违规操作等。

本章的主要研究内容如下：（1）提出一种基于区块链的跨部门工作流协同机制，通过区块链在各部门间传递业务材料，降低业务材料验证成本，提高业务协同效率，杜绝串联篡改业务材料等道德风险。（2）提出业务材料真实性保证机制，基于共识算法，防止业务材料出现“双花问题”，保证业务材料的真实性、一致性。（3）提出业务材料授权使用机制，构建授权令牌，明确业务材料的使用方与操作权限，保证业务材料的使用过程可控。（4）通过实验证明本文所提出的基于区块链的跨部门工作流协同机制可以满足跨部门业务的需求。

1. 系统模型

1.1 跨部门工作流协作机制

基于区块链的跨部门工作流协作机制，如图 1 所示，业务办理人将本次业务的相关材料（即业务材料）上传至区块链，且拥有业务材料的所有权，并可授权他人或业务部门使用或操作该业务材料；业务办理人

通过区块链将业务材料的操作权限授予指定的业务部门，业务部门通过区块链获取相应的业务材料并将操作结果写入区块链中。在区块链中业务材料的载体是交易，故业务部门或业务办理人均以交易的形式操作业务材料。

每个业务部门均需部署区块链节点，共同组成区块链网络，每个部门的区块链节点保存完整的分布式账本，即保存所有业务材料及其使用记录；业务办理人或业务部门均以交易的形式操作业务材料；通过共识算法验证交易是否正确，并保证各业务部门拥有一致的数据。

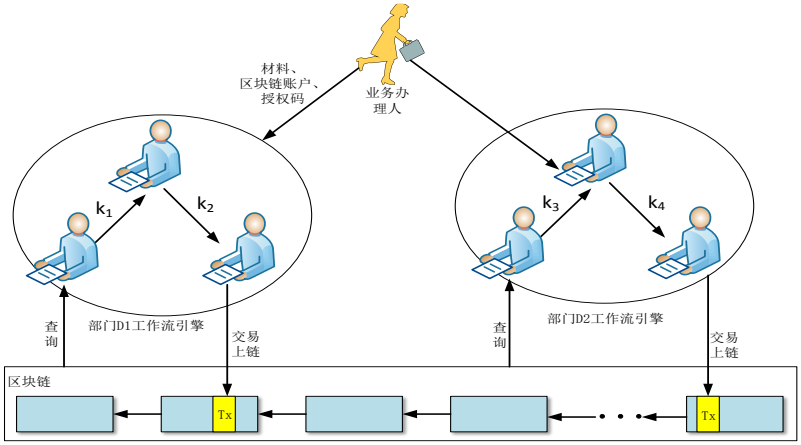

Fig.1 Blockchain-based departmental collaboration workflow mode

图 1 基于区块链的部门协作工作流模型

基于区块链的跨部门工作流协作机制中，业务材料、业务流程等在区块链中的定义如下：

定义 1：业务材料 BCM。业务材料是指业务办理工程中所需要的数据，BCM=<BCM_ID,BCM_Content,BCM_Status>，BCM_ID 表示业务材料在区块链中的唯一标识；BCM_Content 表示业务材料的具体内容，如身份信息、发票等；BCM_Status 表示业务材料在业务办理过程中的状态，如被冻结、被抵押等状态；业务部门通过交易触发业务材料的状态的变更，在交易中声明交易的发起方、接收方、业务材料以及相应的操作等。业务材料可以由业务部门产生，即业务办理中间过程中产生的新材料或者业务部门颁发的材料，如证照等；业务材料也可由业务办理人提交，经业务部门审核颁发的。

定义 2：业务办理人 BCP。业务办理人表示业务的申请者、业务材料的拥有者，BCP=<BCP_ID,BCP_prk,BCP_pk>，BCP_ID 表示业务办理人在区块链中的唯一标识；<BCP_prk,BCP_pk>表示业务办理人的公私钥，用于业务办理人标识身份；通过使用私钥签名的方式，表明业务材料的所有权归属；区块链中，业务办理人通过交易将业务材料的操作权限授予业务部门，此交易称之为授权交易，业务部门基于授权交易操作业务材料。

定义 3：业务部门 BCD。业务部门表示具体办理业务的处理组织，每个业务部门有本部门独立的工作流引擎，用于从区块链接受业务材料并完成具体的工作流程；一个工作流引擎内各审核环节之间通过区块链传递审核信息，最后只将本部门审核的最终结果以交易的形式发送到区块链上。BCD=<BCD_ID,BCD_pk,BCD_prk>，BCD_ID 表示业务部门在区块链中的唯一标识，<BCD_pk,BCD_prk>表示业务部门的公私钥，用于在业务办理过程中表明身份；区块链中，业务部门通过交易完成相关业务办理，在交易中声明发起方、接收方、授权交易、业务材料等。

区块链上的所有交易的 Operation type 可分为六种:盖章通过交易(T_{pass})，审核未通过交易(T_{unpa})，授权交易(T_{auth})，查看记录交易(T_{review})，无效交易($T_{invalid}$)，通知交易(T_{inform})，即 $T = \{T_{pass}, T_{unpa}, T_{auth}, T_{review}, T_{invalid}, T_{inform}\}$。

区块链上交易的数据模型如图 2 所示，左侧为交易的组成内容，不同类型的交易组成内容不同；右侧图为交易 Tx=(From,To,Data,Operation type,Pre-hash)，即每条交易的数据结构都由五部分组成：From（交易发送方区块链账户地址），To（交易接收方区块链账户地址），Data（具体交易内容，可以根据 from 和to的角色不同和进行的不同操作，自定义不同的数据结构，包括时间、发送部门或企业信息等，以 JSON 格式），

Operation type（操作类型分类，如盖章通过、审核不通过、授权、查看记录等）、Pre-hash（指向该企业区块链账户的上一条交易的交易码，这样便于企业查找自己的所有交易）。

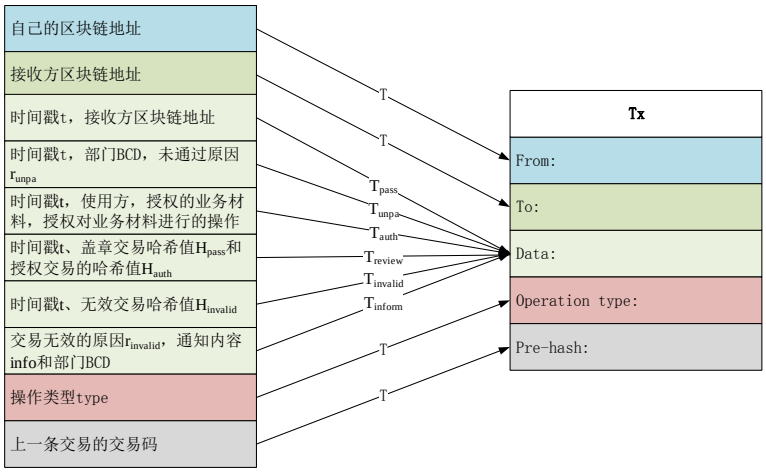

Fig.2 Blockchain transaction data structure model

图 2 区块链交易数据结构模型

下列算法实现了工作流日志中上链属性为 1 的数据、状态与区块链数据结构之间的映射。

Algorithm1 Mapping algorithm

算法 1 映射算法

1. initilize:（From,To,Data,Operation type,Pre-hash）//初始化区块链中的数据
2. (from,to)←search(MyA,A_1) //将自己的地址映射到 from，目的地址映射到 to
3. Operation type←search(type) //将日志中的 type 映射到 Operation type
4. switch Operation type //根据 type 类型的不同定义不同的 Data 结构
5. Case pass:Data←search(t,D) // $\mathbf{T_{pass}}$，将日志的时间戳 t 和部门 BCD 映射到 Data
6. Case unpa:Data←search(t,D,r_{unpa}) // $\mathbf{T_{unpa}}$，将日志的时间戳 t、部门 BCD 和未通过原因$\mathbf{r_{unpa}}$映射到 Data
7. Case auth:Data←package(t,userID,BCM,OP) // $\mathbf{T_{auth}}$，将 package(.)算法计算的时间戳**t**和使用方、业务材料 BCM、授权可以对业务材料进行的操作映射到 Data
8. Case review:Data←review(t,H_{pass},H_{auth}) // $\mathbf{T_{review}}$，将 review (.)算法计算的时间戳 t、盖章交易哈希值$\mathbf{H_{pass}}$和授权交易的哈希值$\mathbf{H_{auth}}$映射到 Data
9. Case invalid:（Data,T_{inform}）←invalid(t,$H_{invalid}$) // $\mathbf{T_{invalid}}$,输入为时间戳**t**、无效交易哈希值$\mathbf{H_{invalid}}$，使用 invalid(.)算法生成 Data 和$\mathbf{T_{inform}}$
10. Tinform Data←inform($r_{invalid}$,info,D) //输入为交易无效的原因$\mathbf{r_{invalid}}$，通知内容 info 和部门 BCD，输出为$\mathbf{T_{inform}}$的 Data
11. Pre-hash←Get hash(from)
12. Upload(From,To,Data,Operation type,Pre-hash)

1.2 业务材料真实性保证机制

基于区块链的跨部门工作流协作机制中，需要保证各部门存储一致的、正确的业务材料及其使用记录，防止各部门存储的数据不一致、不正确导致的业务无法正常办理或者业务异常办理等情况发生。业务材料真实性保证机制基于共识算法保证业务材料及其使用记录的真实性[8]，由此保证各部门的存储正确的、一致的数据。

业务材料真实性保证机制如算法 1 所示：各业务部门将本部门业务材料的验证规则封装成智能合约（包括业务材料的状态变更规则），智能合约部署到区块链中的每一个节点中；所有业务部门通过共识算法共同验证业务材料的真实性。当业务办理人或业务部门发起交易TX时，交易被广播到各个节点中；各节点验证

基于预先设定的业务材料验证规则，验证业务材料的发起方与接受方是否合法、业务材料的状态变更是否正确、交易发起方对业务材料的操作是否正确等；只有当超过 2/3 的节点认为该交易正确，该交易才会被写入到区块链中。

Algorithm 2 Business material authenticity guarantee mechanism

算法 2 业务材料真实性保证机制

```
1.  For each BCM
2.      VR <- ConstructValidationRule(BCM)
3.      DeployContract(VR)
4.  endFor
5. For each TX
6.  For each node
7.      Validate_BCD(); Validate_BCP()；Validate_Op(); Validation_Status()
8.        sendVote()
9.    If correact_note > 2/3
10.         Onchain(TX)
11.    Else
12.       Remove(TX)
13.    endIF
14.  endFor
15. endFor
```

通过业务材料真实性保证机制，保证区块链中存储的均为正确的业务材料及其使用记录，保证各业务部门获取到正确的业务材料及其历史记录。

区块链通过共识机制保证各个节点业务材料的一致性，即区块链利用“Merkle 树的根值”的哈希值来判断区块的数据是否被篡改过的。如图 3 所示，每个节点存储的区块链数据都是相同的，从而保证区块链上业务材料的一致性。

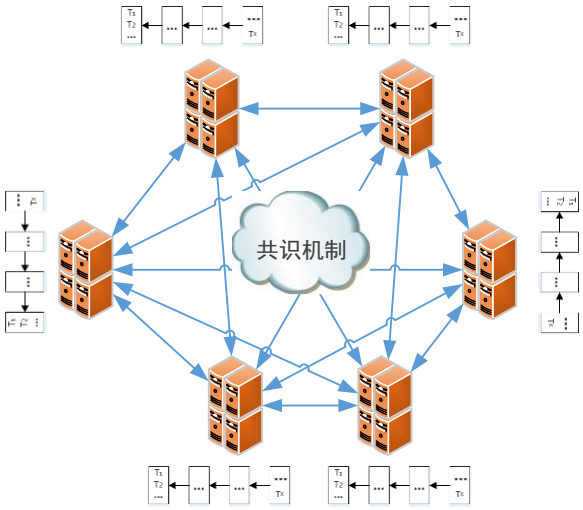

Fig.3 Business material consistency model

图 3 业务材料一致性模式

1.3 业务材料授权使用机制

现有的业务办理过程中，业务办理人对业务材料的使用过程一无所知，即当业务办理人员执行完业务后，才会将执行的具体操作告知业务办理人。在整个业务材料流通过程中，业务办理人员权限过大，因此

易造成业务材料使用不透明，从而导致业务材料违规使用等情况发生。故为保证材料的合规使用，本文构建业务材料授权使用机制，明确数据所有权，防止非法使用等情况的发生。

业务材料授权使用机制的核心思想是：业务办理方通过授权交易构建授权令牌，业务部门根据授权令牌操作业务办理方的业务材料。授权交易的发起方为业务办理人，接收方为业务部门，授权交易的内容表示具体的授权令牌，包括业务部门可操作的业务材料、可对每个业务材料执行的操作以及授权令牌的使用时间、次数等限制，授权交易的 ID 作为授权令牌的授权码。业务部门根据授权码可在区块链中检索到授权令牌，只有获取到相应的授权令牌才可操作相应的业务材料。

授权令牌按照需求分为短期、长期、一次性、重复性等四种类型，包括授权使用方、授权方、授予的权限等。业务材料的授权模型表达形式为：Auth=<AuthID,Author,Consumer,Operation,Time,Num>,Author 表示业务材料的授权方，即业务办理方，Consumer 表示授权的接收方，即业务部门，Operation 表示授予的权限，Time 表示权限的有效期，Num 表示权限使用的次数，AuthID 表示授权 ID，用授权交易的摘要值表示 AuthID。

业务材料操作模型：Used=<Consumer,BCP,Op(AuthID,operation)>，Consumer 表示使用授权的业务部门，BCP 表示业务材料的拥有方，Op 表示对业务材料执行的操作以及授权等。

业务材料的使用过程描述如下：

1、业务办理方构建授权交易，声明授权方、被授权方、授予的权限、业务材料；

2、区块链验证授权交易的合法性，判断交易的发起方、交易的接收方是否合法，判断授予的权限是否合法；

3、业务部门基于授权操作业务材料，并发起交易，声明业务材料的操作方、业务材料、业务材料的操作。

其中，使用交易的合法性验证过程包括：验证业务材料的操作是否合法，验证授权是否过期。

业务部门只能基于业务办理方授予的权限进行操作，明确了业务材料的使用过程，杜绝了业务材料的违规操作等。

2. 应用案例

如图 4 所示，企业开办主要业务流程：

1.在网上登记服务平台填写企业相关信息，等待市场监管局审核通过。市场监管局审核通过后，带上相应的资料前往工商局做登记注册，获得纸质的营业执照。

2.带着营业执照等资料，前往公安局做公章备案，再去中介窗口刻章，最后在公安分局窗口核验印章，最终获得单位公章、财务章、发票章、合同章。

3.带着营业执照、单位公章等资料，前往银行开立对工账户，获得开户许可证。

4.带着营业执照、单位公章、开户许可证等资料，前往国地税局的办税大厅办理企业纳税登记业务。

5.带着营业执照、单位公章等资料，前往人力资源与社会保障局的社保中心办理单位参保业务。

注册者需要按照注册流程到各部门去办理注册业务，其中有些流程是有先后顺序的，例如，通过第一步在登记服务平台填写信息的审核是后面所有业务的前提条件，如果第一步信息审核没有通过，后面的所有业务都无法进行办理。再比如到银行开立对工账户的业务，进行这一步业务不仅需要注册者已经在工商局获得营业执照，而且还必须完成了公安局的公章 备案及刻制业务，也就是说营业执照和单位公章都是银行对工账户业务和人力资源与社会保障局的参保业务办理的前提条件。

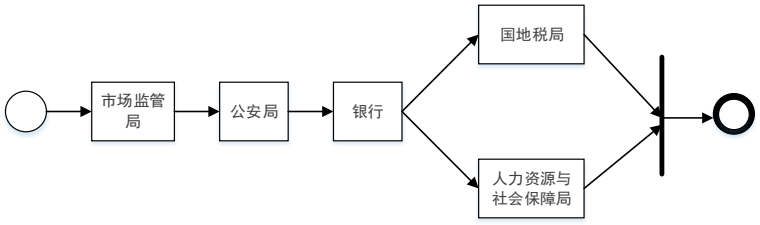

Fig.4 Business start-up business process

图 4 企业开办业务流程

在整个企业开办业务工作流过程中，部门工作流引擎与区块链系统进行交互的情况主要可分为两种：企业去各部门执行开办业务的工作流和企业业务材料信息更新工作流。

2.1 企业开办业务过程

数字证照签发后、企业签收前，企业不具使用权限，业务办结企业签收数字证照后企业才具备使用权限。业务进行中，云平台作为 holder 代理各发证部门进行授权和使用。云平台和各部门分别享有区块链账户，各部门区块链账户由云平台代管，负责数字证照的签发，并且在签发时向云平台账户赋予 holder 权限，云平台根据业务办理流程使用 holder 权限智能向后续经办部门账户发送相关数字证照的授权，下一部门办理业务时需要的数字证照通过云平台代管该部门的账户从区块链获取，且使用后发送使用交易。

运用云平台智能流水线将业务智能推送到下一经办机构，各经办机构通过云平台代管部门区块链账户，并获取数字证照，办理业务。

在企业执行开办业务过程中，若当前部门节点的执行依赖于一个或几个已执行的节点，则当前正在执行的部门节点称为 Cur-node，被依赖的已执行节点称为 Pre-node。例如，注册者在工商局办理完营业执照后，才可去公安局办理印章刻制业务，工商局部门节点与公安局部门节点的业务过程执行存在严格的先后顺序，在此业务场景下工商局为 Pre-node，公安局为 Cur-node。

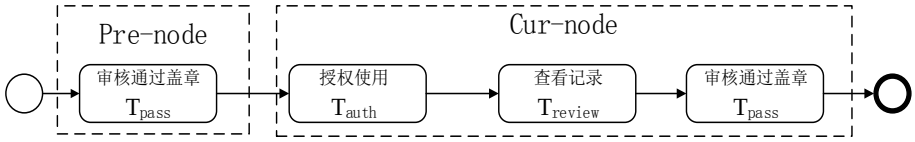

Fig.5 Business start-up transaction process

图 5 企业开办交易流程

云平台启动业务流程，开始受理业务。企业录入信息，并提交业务材料。云平台获取企业区块链账户，向下一部门推送业务。下一部门通过云平台受理业务，生成业务材料，并发送到区块链上。

云平台代理企业身份账户在区块链上发送一条授权交易T_{auth}，目的是让当前部门节点 Cur-node 可以在区块链上查看 Pre-node 的盖章通过交易和业务材料，确认是否已经通过 Pre-node 的审核，若 Cur-node 有多个 Pre-node，则需要对应的发送多条T_{auth}。

接下来，Cur-node 根据企业发送来的授权码，解析出其中所包含的盖章交易的哈希值H_{pass}，根据哈希值在区块链上找到所需要的T_{pass}，并需要在区块链上发送T_{review}，以便对所有查看交易的部门进行记录，以保护企业的信息安全和对自己信息的自由掌控的权利。

最后，Cur-node 在本部门的系统中对该企业进行一系列审核，若该注册者通过这些审核，那么 Cur-node 就可以给其办理本部门的企业开办业务。之后，Cur-node 为了向之后的部门证明已给该企业办理了企业开办业务，需在区块链上发送交易T_{pass}。

如果该企业在 Cur-node 的审核环节没有通过，Cur-node 就需要在区块链上发送交易T_{unpa}。

2.2 信息更新业务过程

一条交易信息的更新，不仅引起本条交易信息的更新，还导致其他部门的交易信息的无效或更新，这时，被引起信息更新的部门称之为 Rel-node。例如：公司法人的变更，引起的营业执照、税务登记证、银行开户许可证等一系列证照信息的变更。

区块链上的交易是不可以直接修改的，当某条交易的信息需要更新时，需要先发送一条失效交易，使旧的或错误的信息标记为无效交易，然后再发送一条新的交易，将更新后的信息写入这条新交易中。

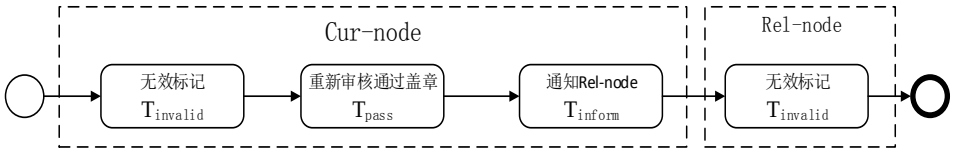

Fig.6 Information update transaction process model

图 6 信息更新交易流程模型

图 6 为信息更新的交易模型，由于 Cur-node 的信息更改导致 Rel-node 的相关信息也需要更改。首先，Cur-node 先在区块链上发送交易$T_{invalid}$，将之前发送到区块链上的盖章交易标记为无效交易，data 里存放要失效交易的哈希值，和盖章交易无效的声明，以及让其失效的原因；service type 为无效。然后，经过对更改信息的重新审核，通过后 Cur-node 再发送交易T_{pass}，该修改交易的发送方为 Cur-node，接收方为企业区块链账户，data 里存放该企业证照更新后的信息，service type 仍然为盖章通过。同时 Cur-node 还要在区块链上向 Rel-node 发送一条该部门盖章交易无效的通知交易T_{inform}，即通过这条交易来通知 Rel-node 该企业的信息有更改，通知交易的 data 为具体的更改信息。Rel-node 的工作流引擎捕捉到这种类型的消息后，会在区块链上通过发送交易$T_{invalid}$将引起更改的盖章交易标记为无效交易，等待企业重新去 Rel-node 完成开办业务。

2.3 工作流日志到区块链的映射

表 1 是从市场监管局的工作流日志中提取的重要字段。每一条记录代表一个事件e，由表 1 中的属性组成，即$e = （e_{user}, e_{start}, e_{end}, e_{type}, e_{bc}）$。上链属性中 0 代表不需要发送到区块链的信息，1 代表需要跨部门传递的信息，要发送到区块链上。所以工作流日志与区块链的数据结构之间存在映射。

Table1 Market supervision bureau workflow event log

表 1 市场监管局工作流事件日志

事件 ID	注册者	开始时间	结束时间	操作类型	上链
1	Johnny	2018/09/0709:27:00	2018/09/0709:30:00	内部审核	0
2	Johnny	2018/09/0709:32:00	2018/09/0709:35:00	内部审核	0
3	Johnny	2018/09/0709:38:00	2018/09/0709:43:00	盖章通过	1
4	Betty	2018/09/0813:52:00	2018/09/0813:57:00	查看记录	1
5	Anderson	2018/10/1510:07:00	2018/10/1510:11:00	无效标记	1

通过算法 1 将表 1 中市场监管局工作流事件日志映射到区块链上的交易如表 2 所示，事件 3、4、5 映射为区块链上的交易。

Table2 The example of blockchain transaction

表 2 区块链交易示例

From	To	Data	Operation type
市场监管局区块链地址	Johnny	2018/09/0709:38:00 A：“0x44989dd66d80adaebe05a8f48c02d60f165314c6”	T_{pass}
市场监管局区块链地址	Betty	2018/09/0813:52:00 T_{pass}”0x4c0a13e35c82841714680b4cd45dcc6e66f362c76d1ac06d635547e2cd921092” **T_{auth}**“0x893316b0e56d7a303154ce24fade669d5e89c177481a23e9c97cff565ba638ce”	T_{review}
市场监管局区块链地址	Anderson	2018/10/1510:07:00 $T_{invalid}$：“0xca50cb1d72d3bc7ebbae43afb8451064b0beae66”	$T_{invalid}$

市场监管局区块链地址	公安局区块链地址	2018/10/1510:07:00 $r_{invalid}$：“0x43afb8451064b0beae66ca50cb1d72d3bc7ebbae” A:“0x05a8f48c02d60f165314c644989dd66d80adaebe”	T_{inform}

3.实验分析

以太坊已经实现了去中心化的分布式存储，保持使用者匿名，交易无法撤销等特点，但仍有一些技术问题有待解决，比如延展性攻击、区块容量限制、区块分叉、扩展性等[9]。本文参考以太坊开发实现上述所提出的数字资产交易模型，修改了以太坊的交易格式、共识机制等。实验服务器环境为 E5-2609@2.40GHz, 12GB 内存，操作系统版本 Ubuntu14.04。

根据企业开办业务的需求分析，所有部门的最高流程并发量之和达到 8000/s，每个流程之间最佳时间间隔为 5s。以太坊区块链的吞吐量每秒能达到 200 笔交易，交易延迟为 15s[10]，并不能满足目前业务的需求。为此我们将以太坊的共识模块进行了修改，交易延迟缩短到 5s[11]，并针对吞吐量和交易延迟做实验。

区块链吞吐量=单位时间内交易上链的数目/单位时间；单位时间=交易传播时间+区块构建时间+区块传播时间[12]。根据公式，传播时间越短，则单位时间越短，区块链的吞吐量会增大。区块的大小是影响传播时间的关键因素，区块越小，区块构建时间和区块传播时间越短。但是区块太小，每个区块承载的交易就会减少，交易堆积在交易池中不能及时上链，造成交易堵塞；当区块过大，而交易数量相对较少时，则会造成区块浪费。所以找到与业务量相匹配的区块大小，不仅能解决交易堆积，减少区块浪费，还能提高区块链的吞吐量。

业务材料的大小与区块上能容纳的交易数量紧密相关。当业务材料过大，每个区块上容纳的交易相对减少，进而影响区块链的吞吐量，使吞吐量降低；当业务材料过小时，会影响图片的清晰度，不能满足业务办理时的使用需求。最后经过反复对比发现，业务材料大小为 100k 较为适中，清晰度基本能够满足办理业务时的需求。但当业务材料为 100k 时，每个区块存储的交易数量会很少，区块链的吞吐量并不能满足当前业务需求。

为此，我们将 IPFS 和区块链结合，可以使用 IPFS 来处理大量数据，然后把对应的加密哈希存储到区块链中并打上时间戳。这样就无需将数据本身放在链上，不但可以节省区块链的网络带宽，还可以对其进行有效保护[13]。

将 IPFS 和区块链结合后，现在每笔交易的大小约为 20～30B，测试区块大小对区块链吞吐量的影响。我们在 64k～6M 之间选取几个值，测试区块大小对吞吐量的影响，实验结果如图 7 所示，区块大小为 2M 时，区块链的吞吐量达到最大。

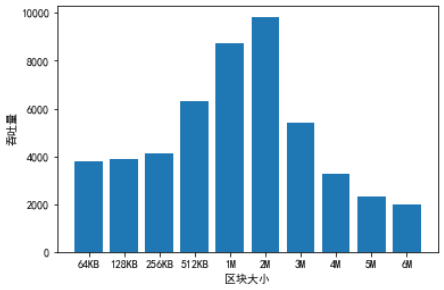

Fig.7 Block size and throughput diagram

图 7 区块大小与吞吐量关系图

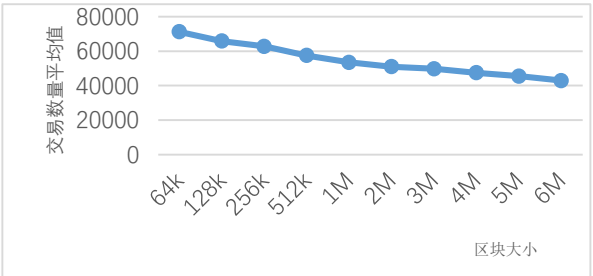

Fig.8 variation of trading average with block size

图 8 交易平均值随区块大小变化图

针对不同区块大小的区块链，做交易数量平均值的实验。如图 8 所示，将区块大小范围设置在 64k~6M，每种大小的区块都等距抽取 20 个块计算区块交易数量的平均值。根据实验结果发现，区块大小为 2M 时，区块上的交易数量约为 20000 笔，基本能满足目前业务量的需求。

当区块大小一定时，（我们以 2M 为例），统计每个区块上交易的数量。在整个区块链上每隔 10 个区块抽取一个区块，共抽取了 20 个区块，对区块上交易数量进行统计，最终结果如图 6-12 所示，算得平均每

个区块上大约能容纳有 50000 笔交易。

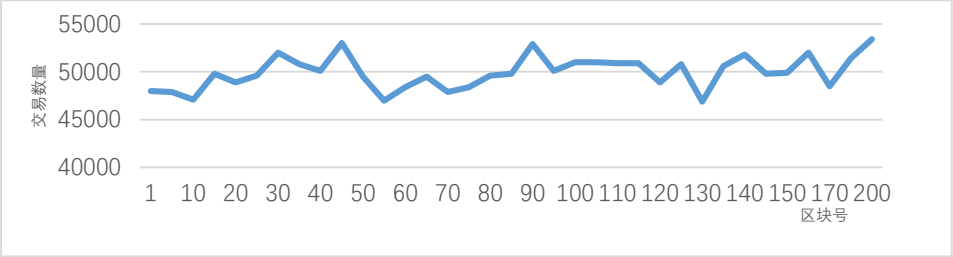

Fig.9 the number of transactions with block size of 2M

图 9 区块大小为 2M 的交易数量统计图

经过上述实验，我们发现当区块大小为 2M 时，区块链的吞吐量最大，约为 10000 笔/s。这时，区块上能容纳的交易数量约为 50000 笔，完全能够满足企业开办业务的最高流程并发 8000/s 的需求。

结束语

涉及企业开办业务的所有部门和企业通过认证后加入区块链系统，各部门工作流引擎间利用区块链在企业开办业务的分布式工作流系统中进行数据保存和信息传递，用户可以通过客户端随时查看自己的业务办理进程和结果。利用区块链上的数据不可篡改的特性，保证了信息的可靠性和安全性；通过区块链进行信息传递来代替跨部门调用接口传递信息，消除了原有的单一中心化依赖问题；区块链上的信息都以交易的形式存在，写作部门可以根据需要查看到材料的历史纪录及当前状态，极大的提高了部门审核效率。

References:

[1] Wang XG.Overview of block chain technology consensus algorithm . China Computer & Communication.2017(9):72-74(in Chinese with English abstract).

[2] Weber I, Xu X, Riveret R, et al. Untrusted Business Process Monitoring and Execution Using Blockchain. International Conference on Business Process Management. Springer International Publishing.2016:329-347.

[3] Prybila C, Schulte S, Hochreiner C, Weber I. Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain. Future Generation Computer Systems (FGCS). 2017.

[4] Mendling J, Weber I, Aalst W.M.P, et al. Blockchains for Business Process Management - Challenges and Opportunities. ACM Trans. Management Inf. Syst. 2018, 9(1):4:1–4:16.

[5] Garc á-Ba ñuelos L, Ponomarev A, Dumas M, et al. Optimized Execution of Business Processes on Blockchain.International Conference on Business Process Management. Springer, Cham. 2017:130-146.

[6] Hull R, Batra V S, Chen Y M, et al. Towards a Shared Ledger Business Collaboration Language Based on Data-Aware Processes. Service-Oriented Computing. Springer International Publishing.2016:18-36.

[7] Norta A. Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations.International Conference on Business Informatics Research. Springer, Cham.2015:3-17.

[8] Watanabe H, Fujimura S, Nakadaira A, et al. Blockchain contract: A complete consensus using blockchain. Consumer Electronics. IEEE.2016:577-578.

[9] Staples Mark, Chen Shiping, Falamaki Sara, et al. Risks and opportunities for systems using blockchain and smart contracts. : Data61(CSIRO)Sydney.2017.

[10] G. Wood, Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper.2014:1–32.

[11] Min X, Li Q, Liu L, et al. A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size.Trustcom/bigdatase/ispa. IEEE.2017:90-96.

[12] Pilkington M. Blockchain Technology: Principles and Applications. Social Science Electronic Publishing.2015.

[13] Chen Y, Li H, Li K, et al. An improved P2P file system scheme based on IPFS and Blockchain. IEEE International Conference on Big Data. IEEE.2018:2652-2657.

附中文参考文献:

[1]王晓光. 区块链技术共识算法综述[J]. 信息与电脑(理论版), 2017(9):72-74.