(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114338242 B
(45)授权公告日 2022.06.14

(21)申请号 202210228270.2
(22)申请日 2022.03.10
(65)同一申请的已公布的文献号
申请公布号 CN 114338242 A
(43)申请公布日 2022.04.12
(73)专利权人 广东省科技基础条件平台中心
地址 510033 广东省广州市越秀区连新路171号自编3号楼
(72)发明人 李军 周凌云 罗宇恒 刘良斌 陈晓佳 卢琰 李海威
(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 吕金金
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
审查员 刘叶

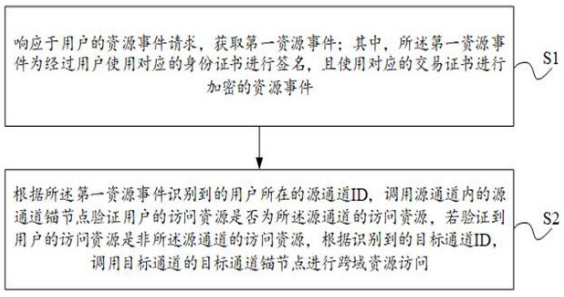
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种基于区块链技术的跨域单点登录访问方法及系统

(57)摘要

本发明公开了一种基于区块链技术的跨域单点登录访问方法及系统，包括：响应于用户的资源事件请求，获取第一资源事件；其中，所述第一资源事件为经过用户使用对应的身份证书进行签名，且使用对应的交易证书进行加密的资源事件；根据所述第一资源事件识别到的用户所在的源通道ID，调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源，若验证到用户的访问资源是非所述源通道的访问资源，根据识别到的目标通道ID，调用目标通道的目标通道锚节点进行跨域资源访问；采用本发明实施例能够减少跨域访问系统瓶颈、受入侵后跨域访问系统破坏面大的情况，同时保证了域内服务和资源的访问不受整体区块链系统的影响。



CN 114338242 B

1.一种基于区块链技术的跨域单点登录访问方法,其特征在于,包括:

响应于用户的资源事件请求,获取第一资源事件;其中,所述第一资源事件为经过用户使用对应的身份证书进行签名,且使用对应的交易证书进行加密的资源事件;

根据所述第一资源事件识别到的用户所在的源通道ID,调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源,若验证到用户的访问资源是非所述源通道的访问资源,根据识别到的目标通道ID,调用目标通道的目标通道锚节点进行跨域资源访问;

其中,所述跨域资源访问具体包括:

所述目标通道锚节点验证所述源通道锚节点发送来的第二资源事件的真实性和正确性,在验证通过后解析所述第二资源事件,获得解析后的第二资源事件;其中,所述第二资源事件为经过所述源通道锚节点使用对应的身份证书进行签名的资源事件;

所述目标通道锚节点根据解析后的第二资源事件,在全域区块链授权信息账本上检索目标域区块链授权信息账本,通过对比所述目标域区块链授权信息账本与解析后的第二资源事件,判断所述目标域区块链授权信息账本的授权信息是否符合访问策略,若符合访问策略,向所述目标通道的目标资源服务器发送服务请求,以使所述目标资源服务器生成目标域Token,并将所述目标域Token返回给所述目标通道锚节点;其中,所述全域区块链授权信息账本存储有各域区块链的授权信息账本,所述服务请求为经过所述目标通道锚节点使用对应的身份证书进行签名的服务请求,所述目标域Token为带有时间戳的Token;

所述目标通道锚节点将所述第二资源事件和所述目标域Token进行打包签名,执行部署在所述目标通道上的链码,并在经过验证、排序后提交到所述全域区块链授权信息账本,以使所述目标通道的各交易节点更新授权信息账本;

所述目标通道锚节点将所述目标域Token进行加密签名后发送给用户,以使用户通过加密签名后的目标域Token进行跨域资源访问。

2.如权利要求1所述的基于区块链技术的跨域单点登录访问方法,其特征在于,所述若验证到用户的访问资源是非所述源通道的访问资源,根据识别到的目标通道ID,调用目标通道的目标通道锚节点进行跨域资源访问,具体包括:

所述源通道锚节点若验证到用户的访问资源是非所述源通道的访问资源,生成第三资源事件;其中,所述第三资源事件为经过所述源通道锚节点使用对应的身份证书私钥进行签名,且使用对应的交易证书私钥进行加密后附上签名信息的资源事件;

所述源通道锚节点解析所述第三资源事件以验证用户的真实性,根据验证通过后的第三资源事件识别目标通道ID,向目标通道内的目标通道锚节点发送第二资源事件,以调用所述目标通道锚节点进行跨域资源访问。

3.如权利要求1所述的基于区块链技术的跨域单点登录访问方法,其特征在于,所述目标资源服务器生成目标域Token,并将所述目标域Token返回给所述目标通道锚节点,具体包括:

所述目标资源服务器验证收到的所述服务请求的真实性和正确性,在验证通过后,生成目标域Token,并将所述目标域Token返回给所述目标通道锚节点。

4.如权利要求1所述的基于区块链技术的跨域单点登录访问方法,所述基于区块链技术的跨域单点登录访问方法,还包括:

所述源通道锚节点若验证到用户的访问资源是所述源通道的访问资源，进行域内资源访问；

其中，所述域内资源访问具体包括：

所述源通道锚节点根据位于所述源通道内的源域区块链授权信息账本验证用户是否具有访问所述源通道内资源的权限，若是，向用户发送源域Token，以使用户通过所述源域Token进行域内资源访问；其中，所述源域Token为带有时间戳的Token；

所述源通道锚节点将所述第一资源事件和所述源域Token进行打包签名，执行部署在所述源通道上的链码，并在经过验证、排序后提交到所述源域区块链授权信息账本，以使所述源通道的各交易节点更新授权信息账本。

5.如权利要求1所述的基于区块链技术的跨域单点登录访问方法，其特征在于，在所述响应于用户的资源事件请求，获取第一资源事件之前，所述基于区块链技术的跨域单点登录访问方法还包括：

响应于用户的注册请求，将经过系统管理员审核通过的注册信息及注册成功信息发送给用户，以使用户根据所述注册信息进行登录；

在判断到用户根据所述注册信息成功登录时，响应于用户的申请证书请求，返回用户身份证书、交易证书和属性证书；其中，所述属性证书包括系统管理员授予用户对资源访问的授权信息。

6.如权利要求1所述的基于区块链技术的跨域单点登录访问方法，其特征在于，通过以下步骤将授权信息存储于用户所在通道的区块链上：

用户所在通道的背书节点根据接收到的经过加密并签名的授权信息查看是否具有通道操作权限，若查看到具有通道权限，对加密并签名过的授权信息进行解密，以验证签名的正确性；

所述背书节点通过对比哈希值查看经加密并签名过的授权信息是否正确，若正确，将签名验证通过的授权信息加上背书节点的ID并使用对应的交易证书签名后提交给对应的排序节点，并反馈成功信息给用户；

所述背书节点基于背书策略，当判断到授权信息记录达到预设的背书节点数时，将交易提案的参数作为输入，在当前状态数据库上执行模拟交易，并使交易处于挂起状态，生成交易结果，以基于所述交易结果，将签名验证通过的授权信息发送给对应的排序节点；

排序节点接收到用户广播的所述交易提案和所述交易结果，按通道分类和时间戳先后顺序对所述交易提案进行排序，并为每个通道创建包含交易的区块；其中，所述交易提案中包含背书节点的签名结果和通道标识；

所述排序节点将区块发送到所述排序节点所在通道上的所有节点，以在通过共识过程后，验证节点验证交易提案，并将验证过的交易提案提交到所述排序节点所在通道的提交节点；

所述提交节点根据所述签名结果查看区块的结构是否完整或被篡改过，并确认交易是否符合背书策略，若验证到区块结构完整、区块结构未被篡改且交易符合背书策略，将新产生的授权信息区块追加到对应的提交节点所在的授权信息账本记录上，并将预设的消息广播给链上各记账节点，以使链上各记账节点进行授权信息账本的更新，并根据更新后的授权信息账本更新全域区块链授权信息账本。

7.如权利要求6所述的基于区块链技术的跨域单点登录访问方法，其特征在于，在所述将授权信息存储于用户所在通道的区块链上之前，所述基于区块链技术的跨域单点登录访问方法还包括：节点配置、通道创建和链码部署。

8.如权利要求7所述的基于区块链技术的跨域单点登录访问方法，其特征在于，所述节点配置具体包括：

调用第一系统配置文件，根据配置信息和节点的职责功能，分配通道锚节点、背书节点、验证节点、排序节点和记账节点；

基于节点发现机制，读取区块链网络中的启动节点的信息，对启动节点的列表进行遍历，经过握手阶段建立连接，向对等节点发送成员请求消息，以使所述对等节点反馈节点信息；

收到反馈的所述节点信息后，将所述节点信息加入到相应的节点列表中；其中，各节点的成员管理服务由API/SDK接口底层服务在许可的区块链网络上进行身份认证、身份授权和身份管理；

所述通道创建具体包括：

调用第二系统配置文件，生成创世块、通道的初始化配置、通道锚节点的配置，以使区块链网络中的业务通道通过获取背书节点发起配置交易给对应的排序节点来创建通道；

对每一通道的通道锚节点、背书节点、验证节点、排序节点和记账节点分配对应的证书；

所述链码部署具体包括：

根据业务需求编写链码；

根据不同域范围，创建业务域通道，并使通道与对应的通道锚节点进行绑定；

对链码进行链码打包、安装和部署。

9.一种基于区块链技术的跨域单点登录访问系统，其特征在于，包括控制器，所述控制器执行如权利要求1~8任一项所述的基于区块链技术的跨域单点登录访问方法。

一种基于区块链技术的跨域单点登录访问方法及系统

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种基于区块链技术的跨域单点登录访问方法及系统。

背景技术

[0002] 随着网络系统的规模应用不断扩大，各种服务和资源被置于不同的域中，通过域的划分和管理，可以使用户在各自的信任域中存取各自的服务和资源，在同一个域中的访问权限一般是统一的。但是越来越多的应用需要为不同域用户提供不同需求的服务和资源，这种不在同一信任域中的访问资源的方式就涉及到跨域访问。

[0003] 传统的跨域访问中，采用集中式的中介或代理来对其他域访问权进行授权，以在认证授权通过后进行跨域访问，然而，集中式认证授权容易出现跨域访问系统瓶颈、受入侵后跨域访问系统破坏面大的情况。

发明内容

[0004] 本发明实施例的目的是提供一种基于区块链技术的跨域单点登录访问方法及系统，通过将各通道的通道锚节点作为中介和代理授权服务器，能够减少跨域访问系统瓶颈、受入侵后跨域访问系统破坏面大的情况，同时保证了域内服务和资源的访问不受整体区块链系统的影响，认证和授权效率高。

[0005] 为实现上述目的，本发明实施例提供了一种基于区块链技术的跨域单点登录访问方法，包括：

[0006] 响应于用户的资源事件请求，获取第一资源事件；其中，所述第一资源事件为经过用户使用对应的身份证书进行签名，且使用对应的交易证书进行加密的资源事件；

[0007] 根据所述第一资源事件识别到的用户所在的源通道ID，调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源，若验证到用户的访问资源是非所述源通道的访问资源，根据识别到的目标通道ID，调用目标通道的目标通道锚节点进行跨域资源访问；

[0008] 其中，所述跨域资源访问具体包括：

[0009] 所述目标通道锚节点验证所述源通道锚节点发送来的第二资源事件的真实性和正确性，在验证通过后解析所述第二资源事件，获得解析后的第二资源事件；其中，所述第二资源事件为经过所述源通道锚节点使用对应的身份证书进行签名的资源事件；

[0010] 所述目标通道锚节点根据解析后的第二资源事件，在全域区块链授权信息账本上检索目标域区块链授权信息账本，通过对比所述目标域区块链授权信息账本与解析后的第二资源事件，判断所述目标域区块链授权信息账本的授权信息是否符合访问策略，若符合访问策略，向所述目标通道的目标资源服务器发送服务请求，以使所述目标资源服务器生成目标域Token，并将所述目标域Token返回给所述目标通道锚节点；其中，所述全域区块链授权信息账本存储有各域区块链的授权信息账本，所述服务请求为经过所述目标通道锚节

点使用对应的身份证书进行签名的服务请求，所述目标域Token为带有时间戳的Token；

[0011] 所述目标通道锚节点将所述第二资源事件和所述目标域Token进行打包签名，执行部署在所述目标通道上的链码，并在经过验证、排序后提交到所述全域区块链授权信息账本，以使所述目标通道的各交易节点更新授权信息账本；

[0012] 所述目标通道锚节点将所述目标域Token进行加密签名后发送给用户，以使用户通过加密签名后的目标域Token进行跨域资源访问。

[0013] 作为上述方案的改进，所述若验证到用户的访问资源是非所述源通道的访问资源，根据识别到的目标通道ID，调用目标通道的目标通道锚节点进行跨域资源访问，具体包括：

[0014] 所述源通道锚节点若验证到用户的访问资源是非所述源通道的访问资源，生成第三资源事件；其中，所述第三资源事件为经过所述源通道锚节点使用对应的身份证书私钥进行签名，且使用对应的交易证书私钥进行加密后附上签名信息的资源事件；

[0015] 所述源通道锚节点解析所述第三资源事件以验证用户的真实性，根据验证通过后的第三资源事件识别目标通道ID，向目标通道内的目标通道锚节点发送第二资源事件，以调用所述目标通道锚节点进行跨域资源访问。

[0016] 作为上述方案的改进，所述目标资源服务器生成目标域Token，并将所述目标域Token返回给所述目标通道锚节点，具体包括：

[0017] 所述目标资源服务器验证收到的所述服务请求的真实性和正确性，在验证通过后，生成目标域Token，并将所述目标域Token返回给所述目标通道锚节点。

[0018] 作为上述方案的改进，所述基于区块链技术的跨域单点登录访问方法，还包括：

[0019] 所述源通道锚节点若验证到用户的访问资源是所述源通道的访问资源，进行域内资源访问；

[0020] 其中，所述域内资源访问具体包括：

[0021] 所述源通道锚节点根据位于所述源通道内的源域区块链授权信息账本验证用户是否具有访问所述源通道内资源的权限，若是，向用户发送源域Token，以使用户通过所述源域Token进行域内资源访问；其中，所述源域Token为带有时间戳的Token；

[0022] 所述源通道锚节点将所述第一资源事件和所述源域Token进行打包签名，执行部署在所述源通道上的链码，并在经过验证、排序后提交到所述源域区块链授权信息账本，以使所述源通道的各交易节点更新授权信息账本。

[0023] 作为上述方案的改进，在所述响应于用户的资源事件请求，获取第一资源事件之前，所述基于区块链技术的跨域单点登录访问方法还包括：

[0024] 响应于用户的注册请求，将经过系统管理员审核通过的注册信息及注册成功信息发送给用户，以使用户根据所述注册信息进行登录；

[0025] 在判断到用户根据所述注册信息成功登录时，响应于用户的申请证书请求，返回用户身份证书、交易证书和属性证书；其中，所述属性证书包括系统管理员授予用户对资源访问的授权信息。

[0026] 作为上述方案的改进，通过以下步骤将授权信息存储于每个通道的区块链上：

[0027] 用户所在通道的背书节点根据接收到的经过加密并签名的授权信息查看是否具有通道操作权限，若查看到具有通道权限，对加密并签名过的授权信息进行解密，以验证签

名的正确性；

[0028] 所述背书节点通过对比哈希值查看经加密并签名过的授权信息是否正确，若正确，将签名验证通过的授权信息加上背书节点的ID并使用对应的交易证书签名后提交给对应的排序节点，并反馈成功信息给用户；

[0029] 所述背书节点基于背书策略，当判断到授权信息记录达到预设的背书节点数时，将交易提案的参数作为输入，在当前状态数据库上执行模拟交易，并使交易处于挂起状态，生成交易结果，以基于所述交易结果，将签名验证通过的授权信息发送给对应的排序节点；

[0030] 排序节点接收到用户广播的所述交易提案和所述交易结果，按通道分类和时间戳先后顺序对所述交易提案进行排序，并为每个通道创建包含交易的区块；其中，所述交易提案中包含背书节点的签名结果和通道标识；

[0031] 所述排序节点将区块发送到所述排序节点所在通道上的所有节点，以在通过共识过程后，验证节点验证交易提案，并将验证过的交易提案提交到所述排序节点所在通道的提交节点；

[0032] 所述提交节点根据所述签名结果查看区块的结构是否完整或被篡改过，并确认交易是否符合背书策略，若验证到区块结构完整、区块结构未被篡改且交易符合背书策略，将新产生的授权信息区块追加到对应的提交节点所在的授权信息账本记录上，并将预设的消息广播给链上各记账节点，以使链上各记账节点进行授权信息账本的更新，并根据更新后的授权信息账本更新全域区块链授权信息账本。

[0033] 作为上述方案的改进，在所述将授权信息存储于用户所在通道的区块链上之前，所述基于区块链技术的跨域单点登录访问方法还包括：节点配置、通道创建和链码部署。

[0034] 作为上述方案的改进，所述节点配置具体包括：

[0035] 调用第一系统配置文件，根据配置信息和节点的职责功能，分配通道锚节点、背书节点、验证节点、排序节点和记账节点；

[0036] 基于节点发现机制，读取区块链网络中的启动节点的信息，对启动节点的列表进行遍历，经过握手阶段建立连接，向对等节点发送成员请求消息，以使所述对等节点反馈节点信息；

[0037] 收到反馈的所述节点信息后，将所述节点信息加入到相应的节点列表中；其中，各节点的成员管理服务由API/SDK接口底层服务在许可的区块链网络上进行身份认证、身份授权和身份管理；

[0038] 所述通道创建具体包括：

[0039] 调用第二系统配置文件，生成创世块、通道的初始化配置、通道锚节点的配置，以使区块链网络中的业务通道通过获取背书节点发起配置交易给对应的排序节点来创建通道；

[0040] 对每一通道的通道锚节点、背书节点、验证节点、排序节点和记账节点分配对应的证书；

[0041] 所述链码部署具体包括：

[0042] 根据业务需求编写链码；

[0043] 根据不同域范围，创建业务域通道，并使通道与对应的通道锚节点进行绑定；

[0044] 对链码进行链码打包、安装和部署。

[0045] 为实现上述目的,本发明实施例还提供了一种基于区块链技术的跨域单点登录访问系统,包括控制器,所述控制器执行如上述所述的基于区块链技术的跨域单点登录访问方法。

[0046] 与现有技术相比,本发明实施例提供的一种基于区块链技术的跨域单点登录访问方法及系统,通过响应于用户的资源事件请求,获取第一资源事件;其中,所述第一资源事件为经过用户使用对应的身份证书进行签名,且使用对应的交易证书进行加密的资源事件;根据所述第一资源事件识别到的用户所在的源通道ID,调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源,若验证到用户的访问资源是非所述源通道的访问资源,根据识别到的目标通道ID,调用目标通道的目标通道锚节点进行跨域资源访问,实现了将各通道的通道锚节点作为中介和代理授权服务器的跨域单点登录访问,能够减少跨域访问系统瓶颈、受入侵后跨域访问系统破坏面大的情况,同时保证了域内服务和资源的访问不受整体区块链系统的影响,认证和授权效率高。除此之外,本发明实施例通过单点登录的方式减少了用户名、密码的维护成本,通过减少授权次数,提高了认证和授权的效率,并且通过引入时间戳信息,进一步保障了授权信息的安全性和可靠性,同时记录了授权信息的访问记录,可作为安全日志用于安全审计。

附图说明

[0047] 图1是本发明实施例提供的一种基于区块链技术的跨域单点登录访问方法的流程图;

[0048] 图2是本发明实施例提供的通道A和通道B的示例图。

具体实施方式

[0049] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0050] 值得说明的是,在本发明实施例中,域即为通道。

[0051] 参见图1,图1是本发明实施例提供的一种基于区块链技术的跨域单点登录访问方法的流程图,所述基于区块链技术的跨域单点登录访问方法,包括:

[0052] S1、响应于用户的资源事件请求,获取第一资源事件;其中,所述第一资源事件为经过用户使用对应的身份证书进行签名,且使用对应的交易证书进行加密的资源事件;

[0053] 具体地,所述资源事件包括源域ID(源通道ID)、目标域ID(目标通道ID)、源IP、目标IP、目标资源和所需的操作;

[0054] 可以理解的是,用户使用自己的身份证书进行签名,且使用对应的交易证书进行加密的资源事件。

[0055] S2、根据所述第一资源事件识别到的用户所在的源通道ID,调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源,若验证到用户的访问资源是非所述源通道的访问资源,根据识别到的目标通道ID,调用目标通道的目标通道锚节点进行跨域资源访问;

[0056] 其中，所述跨域资源访问具体包括：

[0057] 所述目标通道锚节点验证所述源通道锚节点发送来的第二资源事件的真实性和正确性，在验证通过后解析所述第二资源事件，获得解析后的第二资源事件；其中，所述第二资源事件为经过所述源通道锚节点使用对应的身份证书进行签名的资源事件；

[0058] 可以理解的是，所述第二资源事件为所述源通道锚节点使用自己的身份证书进行签名的资源事件，通过解析所述第二资源事件，确定所要访问源、目标资源和所需的操作。

[0059] 所述目标通道锚节点根据解析后的第二资源事件，在全域区块链授权信息账本上检索目标域区块链授权信息账本，通过对比所述目标域区块链授权信息账本与解析后的第二资源事件，判断所述目标域区块链授权信息账本的授权信息是否符合访问策略，若符合访问策略，向所述目标通道的目标资源服务器发送服务请求，以使所述目标资源服务器生成目标域Token，并将所述目标域Token返回给所述目标通道锚节点；其中，所述全域区块链授权信息账本存储有各域区块链的授权信息账本，所述服务请求为经过所述目标通道锚节点使用对应的身份证书进行签名的服务请求，所述目标域Token为带有时间戳的Token；

[0060] 可以理解的是，全域区块链授权信息账本中保存了各个域区块链的授权信息账本，其是通过一定排序后生成的，具体地，各个域区块链的授权信息账本包括授权信息及访问记录；所述服务请求为经过所述目标通道锚节点使用自己的身份证书进行签名的服务请求。

[0061] 可以理解的是，若不符合访问策略，目标通道锚节点向源通道锚节点反馈不成功消息。

[0062] 所述目标通道锚节点将所述第二资源事件和所述目标域Token进行打包签名，执行部署在所述目标通道上的链码，并在经过验证、排序后提交到所述全域区块链授权信息账本，以使所述目标通道的各交易节点更新授权信息账本；

[0063] 值得说明的是，所述目标通道锚节点在利用自己的身份证书对所述第二资源事件和所述目标域Token进行加密签名后，通过调用API/SDK接口的链码服务执行部署在目标通道的链码。

[0064] 所述目标通道锚节点将所述目标域Token进行加密签名后发送给用户，以使用户通过加密签名后的目标域Token进行跨域资源访问。

[0065] 值得说明的是，为了防止时间或重放攻击，采取了对目标域Token采用用户公钥加密签名再发放的方法。在本发明实施例中，用户利用目标域Token进行资源的访问，在时间戳范围内实现单点登录访问。

[0066] 在本发明实施例中，利用Hyperledger区块链架构构建分布式授权信息的分布式存储即将授权信息分别建立各个域的区块链授权账本和全域区块链授权信息账本的方式、利用区块链加密功能、数字证书功能、链码机制和共识机制，保证授权信息的自动可信判决，同时保障授权信息的机密性、完整性和安全性；同时，本发明实施例采用单点登录方式能够减少用户名、密码的维护成本，通过减少授权次数，能够提高认证和授权的效率，并且通过引入时间戳信息，进一步保障了授权信息的安全性和可靠性，同时记录了授权信息的访问记录，可作为安全日志用于安全审计。

[0067] 具体地，在步骤S1所述响应于用户的资源事件请求，获取第一资源事件之前，所述基于区块链技术的跨域单点登录访问方法还包括：

[0068] 响应于用户的注册请求，将经过系统管理员审核通过的注册信息及注册成功信息发送给用户，以使用户根据所述注册信息进行登录；

[0069] 在判断到用户根据所述注册信息成功登录时，响应于用户的申请证书请求，返回用户身份证书、交易证书和属性证书；其中，所述属性证书包括系统管理员授予用户对资源访问的授权信息。

[0070] 值得说明的是，系统管理员根据用户业务需求和抵御对资源的非法访问的要求即根据决策表或库，授予用户对资源访问的授权信息；通过决策表或库决定用户是都能够访问某个域、进行某项操作、获得某项服务；授权的结果用许可权来描述，许可权的描述采用<域ID|主体|资源|权限>四元组的格式；

[0071] 可以理解的是，通过调用Hyperledger的API/SDK接口响应的申请证书请求，申请成功则返回用户身份证书、交易证书和属性证书；身份证书是用户的唯一标识，代表用户的真实性和唯一性；交易证书用于在系统中进行操作(查询、提交、交易等)使用的证书，保障操作的安全性，其包含了在交易和信息传递中使用了非对称加密算法生成的公钥和私钥对；属性证书是可修改和编辑的证书，其中保存了用户的域信息、权限、拥有的资源和可操作的资源，其包含了系统管理员授予用户对资源访问的授权信息，在本发明实时例中，通过属性证书方式方便信息交换。

[0072] 在本发明实施例中，除了采用身份证书来识别用户，采用交易证书来保证敏感数据的私密性之外，还建立了适用于跨域授权的属性证书，通过灵活的属性证书来高效交换授权信息，能够避免授权次数频繁和共识算法的频繁调用。

[0073] 具体地，通过以下步骤将授权信息存储于每个通道的区块链上：

[0074] 用户所在通道的背书节点根据接收到的经过加密并签名的授权信息查看是否具有通道操作权限，若查看到具有通道权限，对加密并签名过的授权信息进行解密，以验证签名的正确性；

[0075] 可以理解的是，节点在将授权信息存储在区块链之前，先采用颁发的交易证书加密并签名该授权信息，用户将经过加密并签名的授权信息广播到所在域的背书节点。

[0076] 所述背书节点通过对比哈希值查看经加密并签名过的授权信息是否正确，若正确，将签名验证通过的授权信息加上背书节点的ID并使用对应的交易证书签名后提交给对应的排序节点，并反馈成功信息给用户；

[0077] 可以理解的是，若不正确即信息有误或被篡改过，则丢弃该授权信息并把错误信息反馈给用户；若正确，将授权信息经过签名后提交给对应通道的排序节点，并反馈成功信息(状态为：已提交到排序节点)给用户。

[0078] 所述背书节点基于背书策略，当判断到授权信息记录达到预设的背书节点数时，将交易提案的参数作为输入，在当前状态数据库上执行模拟交易，并使交易处于挂起状态，生成交易结果，以基于所述交易结果，将签名验证通过的授权信息发送给对应的排序节点；

[0079] 排序节点接收到用户广播的所述交易提案和所述交易结果，按通道分类和时间戳先后顺序对所述交易提案进行排序，并为每个通道创建包含交易的区块；其中，所述交易提案中包含背书节点的签名结果和通道标识；

[0080] 所述排序节点将区块发送到所述排序节点所在通道上的所有节点，以在通过共识过程后，所有节点各自验证交易提案，并将验证过的交易提案提交到所述排序节点所在通

道的提交节点；

[0081] 可以理解的是，共识过程为使用PBFT等共识机制达成共识的环节。

[0082] 所述提交节点根据所述签名结果查看区块的结构是否完整或被篡改过，并确认交易是否符合背书策略，若验证到区块结构完整、区块结构未被篡改且交易符合背书策略，将新产生的授权信息区块追加到对应的提交节点所在的授权信息账本记录上，并将预设的消息广播给链上各记账节点，以使链上各记账节点进行授权信息账本的更新，并根据更新后的授权信息账本更新全域区块链授权信息账本。

[0083] 具体地，所述预设的消息为有新的授权信息区块追加到区块链上。

[0084] 在本发明实施例中，每个信任域(通道)中都有独立的本地区块链授权信息账本，通道的隔离特性为数据的安全提供了保障，同时使得域内服务和资源的访问不受整体区块链的影响，认证和授权效率高；

[0085] 同时，通过构建存储有全域授权信息的全域区块链授权信息账本、将各通道的共享通道锚节点来作为中介和代理授权服务器，能够减少跨域访问系统瓶颈、受入侵后跨域访问系统破坏面大的情况，同时使用链码功能自动判决授权策略来实施交易，减少人工干预。

[0086] 具体地，在所述将授权信息存储于用户所在通道的区块链上之前，所述基于区块链技术的跨域单点登录访问方法还包括：节点配置、通道创建和链码部署。

[0087] 具体地，所述节点配置具体包括：

[0088] 调用第一系统配置文件，根据配置信息和节点的职责功能，分配通道锚节点、背书节点、验证节点、排序节点和记账节点；

[0089] 可以理解的是，所述第一系统配置文件包括网络的拓扑结构和组织结构；所述配置信息包括IP地址；这些节点之间采用Gossip协议进行广播通信。

[0090] 基于节点发现机制，读取区块链网络中的启动节点的信息，对启动节点的列表进行遍历，经过握手阶段建立连接，向对等节点发送成员请求消息，以使所述对等节点反馈节点信息；

[0091] 收到反馈的所述节点信息后，将所述节点信息加入到相应的节点列表中；其中，各节点的成员管理服务由API/SDK接口底层服务在许可的区块链网络上进行身份认证、身份授权和身份管理；

[0092] 可以理解的是，在通道锚节点和排序节点中运行的代码都需经过认证和授权才能进行区块链操作，成员管理服务是基于Hyperledger的MSP实现。

[0093] 具体地，所述通道创建具体包括：

[0094] 调用第二系统配置文件，生成创世块、通道的初始化配置、通道锚节点的配置，以使区块链网络中的业务通道通过获取背书节点发起配置交易给对应的排序节点来创建通道；

[0095] 可以理解的是，第二系统配置文件包括创世纪块、成员管理服务等信息；

[0096] 在本发明实施例中，利用区块链通道机制来区分信任域，以将授权信息存储于信任域中，使得每个信任域中都有独立的本地区块链授权信息账本，即将授权信息存储于每个通道的区块链上。

[0097] 业务通道创建通道时，通道也会检查创世区块，包括检查区块中的配置交易的背

书。如果一切正确，调用在通道上的接口来开始接收本域的授权信息账本。若通道已经存在，则参与者列表将被替换，同时排序节点自动替换订阅者并且将该交易与该通道上的其他交易一起发送给新成员，新成员将会同步完整的区块授权信息账本，其中，新成员为同一通道内注册为新节点的成员。

[0098] 对每一通道的通道锚节点、背书节点、验证节点、排序节点和记账节点分配对应的证书；

[0099] 在本发明实施例中，通过输入通道名称、交易名、通道描述等基本信息加载第二系统配置文件运行批处理脚本完成通道的创建；同时通过可视化方式查看通道列表；其中通道查询结果包括通道名称、通道所属的服务名、加入通道的节点等信息。

[0100] 具体地，所述链码部署具体包括：

[0101] 根据业务需求编写链码；

[0102] 根据不同域范围，创建业务域通道，并使通道与对应的通道锚节点进行绑定；

[0103] 对链码进行链码打包、安装和部署。

[0104] 可以理解的是，可采用Go、Java 等语言来编写链码，链码经过编译后进行签名验证，验证通过之后才能将链码提交并运行；在本发明实施例中，链码部署指把编译后的源码安装到指定节点的过程，在部署会检查是否符合链码节点部署的策略和通道的写入策略。当完成链码打包、安装和部署后，链码即与通道关联，完成了实例化。

[0105] 具体地，在步骤S2中，所述若验证到用户的访问资源是非所述源通道的访问资源，根据识别到的目标通道ID，调用目标通道的目标通道锚节点进行跨域资源访问，具体包括：

[0106] 所述源通道锚节点若验证到用户的访问资源是非所述源通道的访问资源，生成第三资源事件；其中，所述第三资源事件为经过所述源通道锚节点使用对应的身份证书私钥进行签名，且使用对应的交易证书私钥进行加密后附上签名信息的资源事件；

[0107] 所述源通道锚节点解析所述第三资源事件以验证用户的真实性，根据验证通过后的第三资源事件识别目标通道ID，向目标通道内的目标通道锚节点发送第二资源事件，以调用所述目标通道锚节点进行跨域资源访问。

[0108] 具体地，所述目标资源服务器生成目标域Token，并将所述目标域Token返回给所述目标通道锚节点，具体包括：

[0109] 所述目标资源服务器验证收到的所述服务请求的真实性和正确性，在验证通过后，生成目标域Token，并将所述目标域Token返回给所述目标通道锚节点。

[0110] 值得说明的是，所述目标资源服务器通过调用API/SDK接口的Token服务请求生成目标域Token。

[0111] 可选地，所述基于区块链技术的跨域单点登录访问方法，还包括：

[0112] 所述源通道锚节点若验证到用户的访问资源是所述源通道的访问资源，进行域内资源访问；

[0113] 其中，所述域内资源访问具体包括：

[0114] 所述源通道锚节点根据位于所述源通道内的源域区块链授权信息账本验证用户是否具有访问所述源通道内资源的权限，若是，向用户发送源域Token，以使用户通过所述源域Token进行域内资源访问；其中，所述源域Token为带有时间戳的Token；

[0115] 值得说明的是，所述源通道锚节点通过调用API/SDK接口的Token服务生成源域

Token。

[0116] 所述源通道锚节点将所述第一资源事件和所述源域Token进行打包签名，执行部署在所述源通道上的链码，并在经过验证、排序后提交到所述源域区块链授权信息账本，以使所述源通道各交易节点更新授权信息账本。

[0117] 值得说明的是，所述源通道锚节点在利用自己的身份证书对所述第一资源事件和所述源域Token进行加密签名后，通过调用API/SDK接口的链码服务执行部署在源通道的链码。

[0118] 在本发明实施例中，用户利用源域Token进行资源的访问，在时间戳范围内实现单点登录访问。

[0119] 示例性，如图2所示，本发明实施例创建了通道A(源通道)和通道B(目标通道)，在通道A和通道B中实施本发明实施例，具体流程如上述实施例所述，在此不再赘述。

[0120] 本发明实施例提供的一种基于区块链技术的跨域单点登录访问系统，包括控制器，所述控制器执行如上述实施例的基于区块链技术的跨域单点登录访问方法。

[0121] 值得说明的是，本发明实施例所述的基于区块链技术的跨域单点登录访问系统的工作过程可参考上述实施例所述的基于区块链技术的跨域单点登录访问方法的工作过程，在此不再赘述。

[0122] 与现有技术相比，本发明实施例提供的一种基于区块链技术的跨域单点登录访问方法及系统，通过响应于用户的资源事件请求，获取第一资源事件；其中，所述第一资源事件为经过用户使用对应的身份证书进行签名，且使用对应的交易证书进行加密的资源事件；根据所述第一资源事件识别到的用户所在的源通道ID，调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源，若验证到用户的访问资源是非所述源通道的访问资源，根据识别到的目标通道ID，调用目标通道的目标通道锚节点进行跨域资源访问，实现了将各通道的通道锚节点作为中介和代理授权服务器的跨域单点登录访问，能够减少跨域访问系统瓶颈、受入侵后跨域访问系统破坏面大的情况，同时保证了域内服务和资源的访问不受整体区块链系统的影响，认证和授权效率高。除此之外，本发明实施例通过单点登录的方式减少了用户名、密码的维护成本，通过减少授权次数，提高了认证和授权的效率，并且通过引入时间戳信息，进一步保障了授权信息的安全性和可靠性，同时记录了授权信息的访问记录，可作为安全日志用于安全审计。

[0123] 以上所述是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本发明的保护范围。

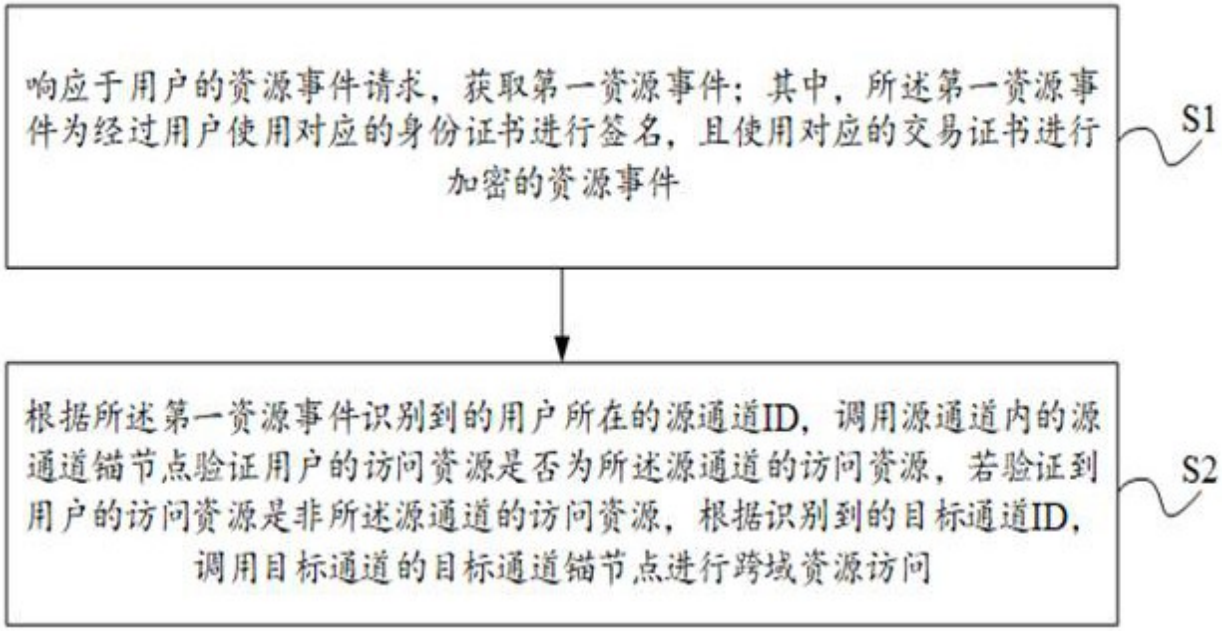

响应于用户的资源事件请求，获取第一资源事件；其中，所述第一资源事件为经过用户使用对应的身份证书进行签名，且使用对应的交易证书进行加密的资源事件
S1
根据所述第一资源事件识别到的用户所在的源通道ID，调用源通道内的源通道锚节点验证用户的访问资源是否为所述源通道的访问资源，若验证到用户的访问资源是非所述源通道的访问资源，根据识别到的目标通道ID，调用目标通道的目标通道锚节点进行跨域资源访问
S2

图1

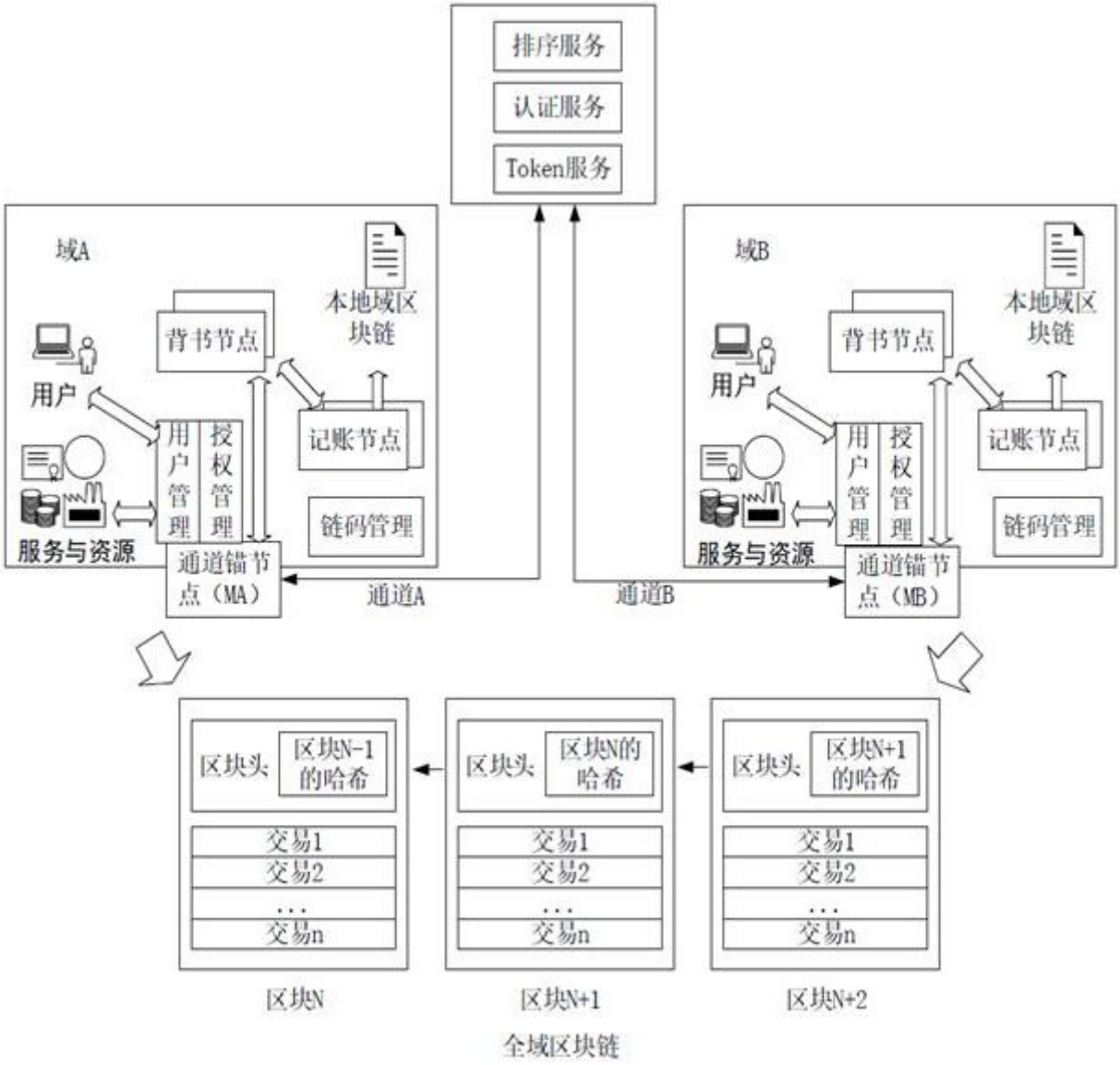

排序服务
认证服务
Token服务
域A
本地域区块链
背书节点
用户
记账节点
用户管理
授权管理
链码管理
服务与资源
通道锚节点（MA）
通道A
域B
本地域区块链
背书节点
用户
记账节点
用户管理
授权管理
链码管理
服务与资源
通道锚节点（MB）
通道B
区块头
区块N-1的哈希
交易1
交易2
...
交易n
区块N
区块头
区块N的哈希
交易1
交易2
...
交易n
区块N+1
区块头
区块N+1的哈希
交易1
交易2
...
交易n
区块N+2
全域区块链

图2