



(12) 发明专利申请

(10) 申请公布号 CN 119892425 A

(43) 申请公布日 2025. 04. 25

(21) 申请号 202411949049.1

(22) 申请日 2024.12.27

(71) 申请人 公安部第一研究所

地址 100044 北京市海淀区首都体育馆南路1号

申请人 慧盾信息安全科技(苏州)股份有限公司

(72) 发明人 栗红梅 郑裕林 吴仰琦 孟斌
陈计明 周迅 沈晔

(74) 专利代理机构 北京汲智翼成知识产权代理
事务所(普通合伙) 11381
专利代理师 贾兴昌 陈曦

(51) Int. Cl.

H04L 9/40 (2022.01)

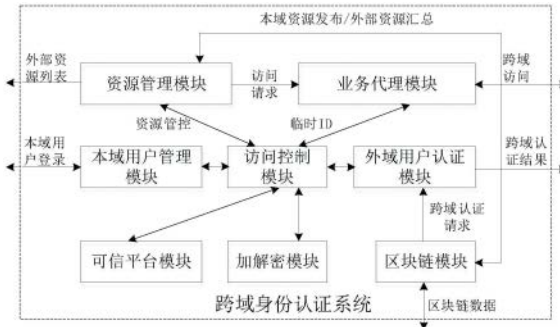
权利要求书3页 说明书9页 附图3页

(54) 发明名称

一种便捷的跨域身份认证系统及方法

(57) 摘要

本发明公开了一种便捷的跨域身份认证系统及方法,旨在提高图像和视频共享场景中的安全性和效率。该系统基于区块链技术,实现身份认证和信息共享,确保数据传输安全和身份认证可靠性。通过在区块链中开户、生成临时公私钥对、发布交易信息、验证用户临时标识等步骤,该系统实现了对用户身份的准确识别和权限控制,同时降低了存储和计算资源需求。本发明特别适合于需要高安全性的数据共享环境,为用户提供了一个安全、高效的数据共享平台。



1. 一种便捷的跨域身份认证系统,其特征在于包括:资源管理模块、业务代理模块、本域用户管理模块、访问控制模块、外域用户认证模块、可信平台模块、加解密模块和区块链模块;

其中,所述资源管理模块负责向本域用户发送外部资源列表,并与所述区块链模块交互,接收/发送本域资源信息以及外部资源汇总信息;同时,所述资源管理模块还与所述访问控制模块通信,接收/发送资源管控信息,并向前述业务代理模块发送访问请求;

所述业务代理模块处理跨域访问,接收和发起外部访问请求,并向所述访问控制模块接收/发送临时ID;

所述本域用户管理模块负责接收/发送本域用户的登录信息,并与所述访问控制模块交互,接收本域用户的权限信息并发送本域用户的登录结果;

所述外域用户认证模块与所述访问控制模块协作,接收跨域认证结果并发送跨域认证请求;所述外域用户认证模块还接收所述区块链模块发送的跨域认证请求,并向外部发送跨域认证结果;

所述可信平台模块与所述访问控制模块交换签名信息,负责接收/发送签名数据;

所述加解密模块与所述访问控制模块交互,接收/发送待加密和待解密的数据;

所述区块链模块负责与外部系统接收/发送区块链相关的数据。

2. 如权利要求1所述的跨域身份认证系统,其特征在于所述资源管理模块包括资源发布子模块和资源接收子模块;

所述资源发布子模块通过区块链系统发布本域向外部共享的资源;所述资源接收子模块通过区块链系统接收外域的资源,并结合本域用户的权限,向用户推送其可访问的所有外部资源。

3. 如权利要求1所述的跨域身份认证系统,其特征在于所述业务代理模块包括:GB/T 28181协议标准代理子模块、GA/T 1400协议标准代理子模块和业务子模块;其中,

所述业务子模块与本域用户进行交互,一方面接收并修改用户的请求,将修改后的请求消息发送到外域对等系统的业务子模块;另一方面接收外域的请求,根据请求的内容与所述GB/T 28181协议标准代理子模块或者所述GB/T 28181协议标准代理子模块进行交互;所述GB/T 28181协议标准代理子模块和所述GB/T 28181协议标准代理子模块分别与本域内的信息系统进行交互。

4. 如权利要求1所述的跨域身份认证系统,其特征在于所述本域用户管理模块包括账号管理子模块和密码策略子模块;其中,

所述账号管理子模块用于完成需访问外部资源的个体的开户和销户;所述密码策略子模块用于设置用户的密码复杂度和密码有效期策略。

5. 如权利要求1所述的跨域身份认证系统,其特征在于所述访问控制模块包括权限管理子模块和用户状态管理子模块;其中,

所述权限管理子模块为本域用户设定权限,供资源管理模块使用;所述用户状态管理子模块记录处于已登录状态的用户,并为其生成临时身份。

6. 如权利要求1所述的跨域身份认证系统,其特征在于所述外域用户认证模块包括跨域用户认证子模块;其中,

所述跨域用户认证子模块从区块链系统接收真实身份请求,对请求消息进行验证,与

所述访问控制模块交互获取真实身份,并发送应答消息。

7.如权利要求1所述的跨域身份认证系统,其特征在于所述区块链模块包括交易信息接收子模块和交易信息发送子模块;其中,

所述交易信息接收子模块周期性从区块链系统获取最新的交易信息;所述交易信息发送子模块根据交易信息的类型,将交易信息发送到资源管理模块或者外域用户认证模块,或者按照区块链系统的接口信息通过区块链系统发布交易信息。

8.如权利要求1所述的跨域身份认证系统,其特征在于所述可信平台模块由CCM3310S-T芯片实现。

9.一种便捷的图像共享跨域身份认证方法,其中的共享信息包括图像数据,其特征在于包括如下步骤:

S1:使用权利要求1~8中任意一项所述的跨域身份认证系统在区块链系统中完成开户,保存区块链系统返回的认证凭证;

S2:所述跨域身份认证系统使用认证凭证登录区块链系统,生成临时公私钥对,通过区块链系统发布“公钥-交易信息”,并在区块链系统中进行数据同步;

S3:信息共享域的跨域身份认证系统通过区块链发布外部可访问的共享信息,并在区块链系统中进行数据同步;

S4:信息接收域的用户在本域的跨域身份认证系统中完成开户;

S5:信息接收域的用户登录本域的跨域身份认证系统;

S6:信息接收域的跨域身份认证系统根据用户的权限返回可访问的外域资源列表;

S7:信息接收域的用户,发起共享信息的跨域访问请求;

S8:信息接收域的跨域身份认证系统,为本域用户随机生成一个唯一的临时ID,并为临时ID标注日期、时间和有效期,形成临时标识,使用信息接收域的临时私钥对临时标识进行签名,在跨域访问请求消息中扩展头域携带临时标识和信息接收域的钱包地址,通过区块链系统发布“用户临时标识-交易信息”;

S9:信息共享域的跨域身份认证系统,根据钱包地址找到临时公钥,然后使用临时公钥对临时标识进行验签,并从中得到临时ID;

S10:判定验签是否通过;如果验签通过且跨域身份认证系统需要知道外域访问者的真实身份,则通过区块链发布特殊的交易信息;如果验签不通过,则向信息接收域返回错误报告;

S11:本域内的信息系统为信息共享域的跨域身份认证系统开通访问权限,信息共享域的跨域身份认证系统通过该访问权限按照GB/T28181协议标准或者GA/T 1400协议标准访问信息系统,请求获取相关的共享信息;

S12:信息接收域的跨域身份认证系统从区块链系统接收获取用户真实身份的请求,使用私钥从交易内容中恢复出临时ID;

S13:本域内的信息系统根据请求,向信息共享域的跨域身份认证系统返回数据

S14:信息接收域的跨域身份认证系统,使用信息共享域的跨域身份认证系统的临时公钥,对用户的账户进行加密,然后将密文通过扩展URL的方式发给信息共享域的跨域身份认证系统;

S15:信息接收域的用户接收数据。

10.一种便捷的视频共享跨域身份认证方法,其特征在于包括如下步骤:

S01:使用权利要求1~8中任意一项所述的跨域身份认证系统在区块链系统中完成开户,保存区块链系统返回的认证凭证;

S02:所述跨域身份认证系统使用认证凭证登录区块链系统,生成临时公私钥对,通过区块链系统发布“公钥-交易信息”,并在区块链系统中进行数据同步;

S03:信息共享域的跨域身份认证系统通过区块链发布外部可访问的共享信息,并在区块链系统中进行数据同步;

S04:信息接收域的用户在本域的跨域身份认证系统中完成开户;

S05:信息接收域的用户登录本域的跨域身份认证系统;

S06:信息接收域的跨域身份认证系统根据用户的权限返回可访问的外域资源列表;

S07:信息接收域的用户,发起共享信息的跨域访问请求;

S08:信息接收域的跨域身份认证系统,为本域用户随机生成一个唯一的临时ID,并为临时ID标注日期、时间和有效期,形成临时标识,然后使用信息接收域的临时私钥对临时标识进行签名,在跨域访问请求中扩展头域携带临时标识和信息接收域的钱包地址,通过区块链发布“用户临时标识-交易信息”;

S09:信息共享域的跨域身份认证系统,根据钱包地址找到临时公钥,然后使用临时公钥对临时标识进行验签,从中得到临时ID;

S010:判定验签是否通过;如果验签通过且跨域身份认证系统需要知道外域访问者的真实身份,则通过区块链发布特殊的交易信息;如果验签不通过,则向信息接收域返回错误报告;

S011:信息系统为信息共享域的跨域身份认证系统开通访问权限,信息共享域的跨域身份认证系统通过该访问权限按照GB/T 28181协议标准或者GA/T 1400协议标准访问信息系统,请求获取相关的共享信息;

S012:信息系统根据GB/T 28181协议生成应答消息,发送至信息共享域的跨域身份认证系统;

S013:信息共享域的跨域身份认证系统,向信息接收域的跨域身份认证系统转发应答消息;

S014:信息接收域的跨域身份认证系统向用户转发应答消息,用户根据应答消息中的信息准备接收视频流;

S015:信息系统将视频流发送至信息接收域的用户;

S016:信息接收域的跨域身份认证系统,使用信息共享域的跨域身份认证系统的临时公钥,对用户的账户进行加密,然后将密文发送至信息共享域的跨域身份认证系统。

一种便捷的跨域身份认证系统及方法

技术领域

[0001] 本发明涉及一种便捷的跨域身份认证系统,同时也涉及相应的图像共享跨域身份认证方法/视频共享跨域身份认证方法,属于网络身份认证技术领域。

背景技术

[0002] 在信息化和网络化的深度融合推动下,物联网、移动互联、工业互联网等技术迅猛发展,标志着人类社会已全面进入“万物互联”的信息时代。这一时代特征为信息系统带来了开放性、大规模性和复杂性等新挑战。网络安全的重要性日益凸显,它不仅关系到国家安全战略,也涉及个人数据安全,成为信息时代发展的关键支撑。在这一背景下,网络实体间信任关系的建立变得尤为关键,它是维护网络空间安全有序的基石。区块链技术以其不可篡改、不可伪造、可追溯的特点,为网络信任体系的建设提供了新的思路和解决方案。

[0003] 在公开号为CN118381635A的中国专利申请中,公开了一种基于区块链的跨域身份认证方法及系统。该技术方案通过在访问者使用的浏览器和企业内网之间建立安全的网络访问通道;对访问者输入的信息,调用部署在联盟链上的账号验证智能合约进行验证,智能合约连接数据库核验账号密码是否正确;获取访问者IP地址,判断是否为新IP地址首次登录,利用身份识别对访问者身份二次确认;服务器建立终端管控系统,提高安全跨域登录安全性;建立数据访问权限控制和审计机制;建立安全评估和漏洞扫描机制,持续评估系统安全性。

[0004] 但是,上述技术方案需要在区块链系统中记录大量的开户数据。随着时间的推移,这些数据的累积会导致存储空间的需求不断增加,同时,处理这些数据所需的计算资源也会随之增长,对区块链系统的可扩展性和性能造成不利影响。

发明内容

[0005] 本发明所要解决的首要技术问题在于提供一种便捷的跨域身份认证系统。

[0006] 本发明所要解决的另一技术问题在于提供一种便捷的图像共享跨域身份认证方法。

[0007] 本发明所要解决的又一技术问题在于提供一种便捷的视频共享跨域身份认证方法。

[0008] 为实现上述技术目的,本发明采用以下的技术方案:

[0009] 根据本发明实施例的第一方面,提供一种便捷的跨域身份认证系统,包括:资源管理模块、业务代理模块、本域用户管理模块、访问控制模块、外域用户认证模块、可信平台模块、加解密模块和区块链模块;

[0010] 其中,所述资源管理模块负责向本域用户发送外部资源列表,并与所述区块链模块交互,接收/发送本域资源信息以及外部资源汇总信息;同时,所述资源管理模块还与所述访问控制模块通信,接收/发送资源管控信息,并向前述业务代理模块发送访问请求;

[0011] 所述业务代理模块处理跨域访问,接收和发起外部访问请求,并向所述访问控制

模块接收/发送临时ID;

[0012] 所述本域用户管理模块负责接收/发送本域用户的登录信息,并与所述访问控制模块交互,接收本域用户的权限信息并发送本域用户的登录结果;

[0013] 所述外域用户认证模块与所述访问控制模块协作,接收跨域认证结果并发送跨域认证请求;所述外域用户认证模块还接收所述区块链模块发送的跨域认证请求,并向外部发送跨域认证结果;

[0014] 所述可信平台模块与所述访问控制模块交换签名信息,负责接收/发送签名数据;

[0015] 所述加解密模块与所述访问控制模块交互,接收/发送待加密和待解密的数据;

[0016] 所述区块链模块负责与外部系统接收/发送区块链相关的数据。

[0017] 其中较优地,所述资源管理模块包括资源发布子模块和资源接收子模块;

[0018] 所述资源发布子模块通过区块链系统发布本域向外部共享的资源;所述资源接收子模块通过区块链系统接收外域的资源,并结合本域用户的权限,向用户推送其可访问的所有外部资源。

[0019] 其中较优地,所述业务代理模块包括:GB/T 28181协议标准代理子模块、GA/T 1400协议标准代理子模块和业务子模块;

[0020] 所述业务子模块与本域用户进行交互,一方面接收并修改用户的请求,将修改后的请求消息发送到外域对等系统的业务子模块;另一方面接收外域的请求,根据请求的内容,与所述GB/T 28181协议标准代理子模块或者所述GB/T 28181协议标准代理子模块进行交互;所述GB/T 28181协议标准代理子模块和所述GB/T 28181协议标准代理子模块分别与本域内的信息系统进行交互。

[0021] 其中较优地,所述本域用户管理模块包括账号管理子模块和密码策略子模块;

[0022] 所述账号管理子模块用于完成需访问外部资源的个体的开户和销户;所述密码策略子模块用于设置用户的密码复杂度和密码有效期策略。

[0023] 其中较优地,所述访问控制模块包括权限管理子模块和用户状态管理子模块;

[0024] 所述权限管理子模块为本域用户设定权限,供资源管理模块使用;所述用户状态管理子模块记录处于已登录状态的用户,并为其生成临时身份。

[0025] 其中较优地,所述外域用户认证模块包括跨域用户认证子模块;

[0026] 所述跨域用户认证子模块从区块链系统接收真实身份请求,对请求消息进行验证,与所述访问控制模块交互获取真实身份,并发送应答消息。

[0027] 其中较优地,所述区块链模块包括交易信息接收子模块和交易信息发送子模块;

[0028] 所述交易信息接收子模块周期性从区块链系统获取最新的交易信息;所述交易信息发送子模块根据交易信息的类型,将交易信息发送到资源管理模块或者外域用户认证模块,或者按照区块链系统的接口信息通过区块链系统发布交易信息。

[0029] 其中较优地,所述可信平台模块由CCM3310S-T芯片实现。

[0030] 根据本发明实施例的第二方面,提供一种便捷的图像共享跨域身份认证方法,其中的共享信息包括图像数据,包括如下步骤:

[0031] S1:使用上述跨域身份认证系统在区块链系统中完成开户,保存区块链系统返回的认证凭证;

[0032] S2:所述跨域身份认证系统使用认证凭证登录区块链系统,生成临时公私钥对,通

过区块链系统发布“公钥-交易信息”,并在区块链系统中进行数据同步;

[0033] S3:信息共享域的跨域身份认证系统通过区块链发布外部可访问的共享信息,并在区块链系统中进行数据同步;

[0034] S4:信息接收域的用户在本域的跨域身份认证系统中完成开户;

[0035] S5:信息接收域的用户登录本域的跨域身份认证系统;

[0036] S6:信息接收域的跨域身份认证系统根据用户的权限返回可访问的外域资源列表;

[0037] S7:信息接收域的用户,发起共享信息的跨域访问请求;

[0038] S8:信息接收域的跨域身份认证系统,为本域用户随机生成一个唯一的临时ID,并为临时ID标注日期、时间和有效期,形成临时标识,使用信息接收域的临时私钥对临时标识进行签名,在跨域访问请求消息中扩展头域携带临时标识和信息接收域的钱包地址,通过区块链系统发布“用户临时标识-交易信息”;

[0039] S9:信息共享域的跨域身份认证系统,根据钱包地址找到临时公钥,然后使用临时公钥对临时标识进行验签,并从中得到临时ID;

[0040] S10:判定验签是否通过;如果验签通过且跨域身份认证系统需要知道外域访问者的真实身份,则通过区块链发布特殊的交易信息;如果验签不通过,则向信息接收域返回错误报告;

[0041] S11:本域内的信息系统为信息共享域的跨域身份认证系统开通访问权限,信息共享域的跨域身份认证系统通过该访问权限按照GB/T28181协议标准或者GA/T 1400协议标准访问信息系统,请求获取相关的共享信息;

[0042] S12:信息接收域的跨域身份认证系统从区块链系统接收获取用户真实身份的请求,使用私钥从交易内容中恢复出临时ID;

[0043] S13:本域内的信息系统根据请求,向信息共享域的跨域身份认证系统返回数据

[0044] S14:信息接收域的跨域身份认证系统,使用信息共享域的跨域身份认证系统的临时公钥,对用户的账户进行加密,然后将密文通过扩展URL的方式发给信息共享域的跨域身份认证系统;

[0045] S15:信息接收域的用户接收数据。

[0046] 根据本发明实施例的第三方面,提供一种便捷的视频共享跨域身份认证方法,包括如下步骤:

[0047] S01:使用上述跨域身份认证系统在区块链系统中完成开户,保存区块链系统返回的认证凭证;

[0048] S02:所述跨域身份认证系统使用认证凭证登录区块链系统,生成临时公私钥对,通过区块链系统发布“公钥-交易信息”,并在区块链系统中进行数据同步;

[0049] S03:信息共享域的跨域身份认证系统通过区块链发布外部可访问的共享信息,并在区块链系统中进行数据同步;

[0050] S04:信息接收域的用户在本域的跨域身份认证系统中完成开户;

[0051] S05:信息接收域的用户登录本域的跨域身份认证系统;

[0052] S06:信息接收域的跨域身份认证系统根据用户的权限返回可访问的外域资源列表;

- [0053] S07:信息接收域的用户,发起共享信息的跨域访问请求;
- [0054] S08:信息接收域的跨域身份认证系统,为本域用户随机生成一个唯一的临时ID,并为临时ID标注日期、时间和有效期,形成临时标识,然后使用信息接收域的临时私钥对临时标识进行签名,在跨域访问请求中扩展头域携带临时标识和信息接收域的钱包地址,通过区块链发布“用户临时标识-交易信息”;
- [0055] S09:信息共享域的跨域身份认证系统,根据钱包地址找到临时公钥,然后使用临时公钥对临时标识进行验签,并从中得到临时ID;
- [0056] S010:判定验签是否通过;如果验签通过且跨域身份认证系统需要知道外域访问者的真实身份,则通过区块链发布特殊的交易信息;如果验签不通过,则向信息接收域返回错误报告;
- [0057] S011:信息系统为信息共享域的跨域身份认证系统开通访问权限,信息共享域的跨域身份认证系统通过该访问权限按照GB/T 28181协议标准或者GA/T 1400协议标准访问信息系统,请求获取相关的共享信息;
- [0058] S012:信息系统根据GB/T 28181协议生成应答消息,发送至信息共享域的跨域身份认证系统;
- [0059] S013:信息共享域的跨域身份认证系统,向信息接收域的跨域身份认证系统转发应答消息;
- [0060] S014:信息接收域的跨域身份认证系统向用户转发应答消息,用户根据应答消息中的信息准备接收视频流;
- [0061] S015:信息系统将视频流发送至信息接收域的用户;
- [0062] S016:信息接收域的跨域身份认证系统,使用信息共享域的跨域身份认证系统的临时公钥,对用户的账户进行加密,然后将密文发送至信息共享域的跨域身份认证系统。
- [0063] 与现有技术相比较,本发明通过构建一个基于区块链的跨域身份认证系统,实现了一种高效、安全的身份认证机制,特别优化了图像和视频数据的共享流程。该系统利用区块链的不可篡改和透明性特点,为跨域身份认证提供了坚实的信任基础,并通过生成临时公私钥对、发布交易信息、以及通过区块链验证用户临时标识等步骤,确保了用户身份的真实性和访问权限的合理控制。本发明不仅增强了数据共享的安全性,还通过减少区块链上的必要信息存储,有效降低了区块链系统的存储和计算负担。

附图说明

- [0064] 图1为用于实施本发明的系统部署图;
- [0065] 图2为本发明实施例提供的跨域身份认证系统的结构示意图;
- [0066] 图3为本发明实施例提供的图像共享跨域身份认证方法的信息交互图;
- [0067] 图4为本发明实施例提供的视频共享跨域身份认证方法的信息交互图。

具体实施方式

- [0068] 下面结合附图和具体实施例对本发明的技术内容进行详细具体的说明。
- [0069] 本发明提供了一种便捷且安全的跨域身份认证系统及方法,特别适用于图像和视频共享的场景。该系统通过区块链技术实现身份认证和信息共享,确保了数据传输的安全

性和身份认证的可靠性。如图1所示,该系统包括信息接收域、信息共享域和区块链三个主要部分,它们通过网络相互连接。其中,在信息接收域,跨域身份认证系统直接与用户网络连接,负责处理用户的身份验证和信息请求。该域向信息共享域发送真实身份应答,并向区块链发送钱包地址和公钥,同时接收来自区块链的钱包地址和公钥,以确保交易的安全性。信息共享域包括跨域身份认证系统和信息系统,其中跨域身份认证系统通过网络与信息系统连接,获取信息系统中的数据。此外,信息共享域向区块链发送钱包地址、公钥和真实身份请求,并接收来自区块链的相应信息。

[0070] 与现有技术相比较,本发明的主要技术构思在于利用区块链的不可篡改性和透明性,为跨域身份认证提供一个去中心化的信任基础。相应的跨域身份认证系统采用了模块化设计,包括资源管理模块、业务代理模块、本域用户管理模块、访问控制模块、外域用户认证模块、可信平台模块和加解密模块等,每个模块都有特定的功能和责任,共同协作完成跨域身份认证和信息共享。

[0071] 此外,可信平台模块可以采用CCM3310S-T、CCM3310S-H和CCM3320S等芯片实现,以提供硬件级别的安全保护,包括密钥管理、系统完整性验证、数字签名和身份认证等功能,增强了整个跨域身份认证系统的安全性。通过这种设计,本发明不仅提高了跨域身份认证的效率和安全性,还减少了区块链系统的性能开销,因为区块链系统只保存最少的必要信息。本发明特别适用于需要高安全性和可靠性的图像和视频共享应用场景,可以为用户提供了一个便捷、安全的数据共享平台。

[0072] 第一实施例

[0073] 如图2所示,本发明第一实施例提供的一种便捷的跨域身份认证系统,包括:资源管理模块、业务代理模块、本域用户管理模块、访问控制模块、外域用户认证模块、可信平台模块、加解密模块和区块链模块。

[0074] 其中,资源管理模块负责向本域用户发送外部资源列表,并与区块链模块交互,接收/发送本域资源信息以及外部资源汇总信息;同时,资源管理模块还与访问控制模块通信,接收/发送资源管控信息,并向前述业务代理模块发送访问请求;业务代理模块处理跨域访问,接收和发起外部访问请求,并向访问控制模块接收/发送临时ID;本域用户管理模块负责接收/发送本域用户的登录信息,并与访问控制模块交互,接收本域用户的权限信息并发送本域用户的登录结果;外域用户认证模块与访问控制模块协作,接收跨域认证结果并发送跨域认证请求;外域用户认证模块还接收区块链模块发送的跨域认证请求,并向外部发送跨域认证结果;可信平台模块与访问控制模块交换签名信息,负责接收/发送签名数据;加解密模块与访问控制模块交互,接收/发送待加密和待解密的数据;区块链模块负责与外部系统接收/发送区块链相关的数据。

[0075] 在本发明的一个实施例中,资源管理模块包括:资源发布子模块和资源接收子模块。其中,资源发布子模块通过区块链系统发布本域向外部共享的资源。资源接收子模块通过区块链系统接收外域的资源,并结合本域用户的权限,向用户推送其可访问的所有外部资源。

[0076] 在本发明的一个实施例中,业务代理模块包括:GB/T 28181协议标准代理子模块、GA/T 1400协议标准代理子模块和业务子模块。其中,业务子模块与本域用户进行交互,一方面接收用户的请求,在请求消息中添加必要的信息,将修改后的请求消息发送到外域对

等系统的业务子模块。另一方面接收外域的请求,根据请求的内容,与GB/T 28181协议标准代理子模块或者GB/T 28181协议标准代理子模块进行交互。GB/T 28181协议标准代理子模块和GB/T 28181协议标准代理子模块分别与本域内的信息系统进行交互。

[0077] 在本发明的一个实施例中,本域用户管理模块包括:账号管理子模块和密码策略子模块。其中,账号管理子模块用于完成需访问外部资源的个体的开户和销户。密码策略子模块用于设置用户的密码复杂度和密码有效期策略。

[0078] 在本发明的一个实施例中,访问控制模块包括:权限管理子模块和用户状态管理子模块。其中,权限管理子模块为本域用户设定权限,供资源管理模块使用。用户状态管理子模块记录处于已登录状态的用户,并为其生成临时身份。

[0079] 在本发明的一个实施例中,外域用户认证模块包括:跨域用户认证子模块,其作用在于从区块链系统接收真实身份请求,对请求消息进行验证,与访问控制模块交互获取真实身份,并发送应答消息。

[0080] 可信平台模块是一种嵌入在计算机主板等硬件设备中的微芯片。它旨在通过提供安全相关的功能,增强整个计算机系统的安全性,能为系统中的敏感数据、密钥等信息提供硬件层面的保护,并且可以用于验证系统启动过程的完整性等。在本发明的一个实施例中,该微芯片的型号为CCM3310S-T(或CCM3310S-H、CCM3320S等,但不限于此)。CCM3310S-T是一款由国芯科技自主研发的车规级安全芯片,其采用具有自主知识产权的32位CPU安全内核CS0,拥有32K字节SRAM、16K字节ROM和256K字节EFLASH的存储资源,以及DMA/EDMA、2个定时器、看门狗和计时器模块。关于CCM3310S-T的进一步说明,可以参阅如下链接:<http://www.fai thi ot.com/content s/11/179.html>,在此不予赘述。

[0081] 该可信平台模块的主要功能包括:密钥管理、系统完整性验证、数字签名和身份认证。

[0082] 其中,密钥管理是指:可信平台模块内部可以安全地生成、存储和管理加密密钥。例如,它可以生成用于加密硬盘数据的对称密钥,或者用于数字签名、身份验证的非对称密钥对(公钥和私钥)。由于密钥存储在硬件内部受保护的区域,相比存储在软件层面,更不容易被窃取或篡改,从而提高了密钥的安全性。

[0083] 系统完整性验证是指:在计算机启动时,可信平台模块可以对启动过程中的各个关键组件(如BIOS、引导加载程序、操作系统内核等)进行哈希运算,并将得到的哈希值与预先存储在芯片内的合法哈希值进行对比。如果出现不一致的情况,就意味着系统可能遭到了篡改,可信平台模块可以采取相应措施,比如阻止系统启动或者向管理员发出警告,以此来确保系统是按照可信的配置启动的。

[0084] 数字签名是指:利用其存储的私钥,可信平台模块能够对数据、文件等进行数字签名,以证明数据的来源和完整性。比如在一些需要保证文档真实性的场景中,通过可信平台模块签名后的文档,接收方可以利用对应的公钥来验证签名,确认文档是否来自可信的源头且未被篡改。

[0085] 身份认证是指:可以基于存储在其中的密钥等信息,协助进行用户或设备的身份认证。例如,在企业网络环境中,计算机接入网络时,借助可信平台模块中的相关信息,向服务器证明自身的合法性,实现更安全可靠的网络接入。

[0086] 在本发明的一个实施例中,加解密模块包括:加密子模块和解密子模块,其作用在

于将明文数据进行加密或者将密文数据进行解密。区块链模块包括：交易信息接收子模块和交易信息发送子模块。其中，交易信息接收子模块周期性从区块链系统获取最新的交易信息。交易信息发送子模块根据交易信息的类型，将交易信息发送到资源管理模块或者外域用户认证模块，或者按照区块链系统的接口信息通过区块链系统发布交易信息。

[0087] 第二实施例

[0088] 如图3所示，本发明第二实施例提供一种便捷的图像共享跨域身份认证方法，使用图像数据作为共享信息，具体包括如下步骤：

[0089] S1：使用上述跨域身份认证系统在区块链系统中完成开户，保存区块链系统返回的认证凭证，即证书和私钥。

[0090] S2：跨域身份认证系统使用认证凭证登录区块链系统，生成临时公私钥对，通过区块链系统发布“公钥-交易信息”，并在区块链系统中进行数据同步。

[0091] 在步骤S2中，当跨域身份认证系统首次尝试登录区块链系统时，它必须通过创建并发布一笔交易来公布自己的钱包地址和一对临时的公私钥。在这笔交易中，发布者和接收者都指的是同一个实体，即进行登录的跨域身份认证系统本身。

[0092] S3：信息共享域的跨域身份认证系统通过区块链发布外部可访问的共享信息，并在区块链系统中进行数据同步。

[0093] S4：信息接收域的用户在本域的跨域身份认证系统中完成开户。

[0094] S5：信息接收域的用户登录本域的跨域身份认证系统。

[0095] 步骤S5描述了用户登录跨域身份认证系统的过程。在这一步骤中，认证方式不局限于某一种特定的机制，而是可以采用任何现有的认证方式。例如，可以使用传统的账号加密码的方式进行认证，也可以采用基于生物特征的认证方式，如指纹识别。

[0096] S6：信息接收域的跨域身份认证系统根据用户的权限返回可访问的外域资源列表。

[0097] S7：信息接收域的用户，发起共享信息的跨域访问请求。

[0098] S8：信息接收域的跨域身份认证系统，为本域用户随机生成一个唯一的临时ID，并为临时ID标注日期、时间和有效期，形成临时标识，使用信息接收域的临时私钥对临时标识进行签名，在跨域访问请求消息中扩展头域携带临时标识和信息接收域的钱包地址，通过区块链系统发布“用户临时标识-交易信息”。

[0099] S9：信息共享域的跨域身份认证系统，根据钱包地址找到临时公钥，使用临时公钥对临时标识进行验签，并从中得到临时ID。

[0100] S10：判定验签是否通过。如果验签通过且跨域身份认证系统需要知道外域访问者的真实身份，则通过区块链发布特殊的交易信息。如果验签不通过，则向信息接收域返回错误报告。

[0101] 步骤S10涉及到一种特殊的交易信息处理方式。在这步骤中，信息共享域作为发送者，向信息接收域发送特殊的交易信息。这笔交易的内容是使用信息接收域的临时公钥加密后的临时ID。这样的设计确保了信息的安全性和隐私性，因为只有拥有相应私钥的信息接收域才能解密并识别出真实的临时ID。

[0102] S11：本域内的信息系统为信息共享域的跨域身份认证系统开通访问权限，信息共享域的跨域身份认证系统通过该访问权限按照GB/T28181协议标准或者GA/T 1400协议标

准访问信息系统,请求获取相关的共享信息。

[0103] S12:信息接收域的跨域身份认证系统从区块链系统接收获取用户真实身份的请求,使用私钥从交易内容中恢复出临时ID。

[0104] S13:本域内的信息系统根据请求,向信息共享域的跨域身份认证系统返回数据。

[0105] S14:信息接收域的跨域身份认证系统,使用信息共享域的跨域身份认证系统的临时公钥,对用户的账户进行加密,然后将密文通过扩展URL的方式发给信息共享域的跨域身份认证系统。

[0106] S15:信息接收域的用户接收数据。

[0107] 综上所述,本发明第二实施例提供的图像共享跨域身份认证方法,通过创建临时密钥对、发布共享信息、生成并验证临时ID等步骤,确保了图像数据在跨域传输过程中的安全性和认证的可靠性,同时降低了系统性能开销,提高了认证效率和数据共享的便捷性。

[0108] 第三实施例

[0109] 如图4所示,本发明第三实施例提供的一种便捷的视频共享跨域身份认证方法,使用视频数据作为共享信息,具体包括如下步骤:

[0110] S01:使用上述跨域身份认证系统在区块链系统中完成开户,保存区块链系统返回的认证凭证,即证书和私钥。

[0111] S02:跨域身份认证系统使用认证凭证登录区块链系统,生成临时公私钥对,通过区块链系统发布“公钥-交易信息”,并在区块链系统中进行数据同步。

[0112] 步骤S02详细描述了跨域身份认证系统与区块链系统的首次交互流程。具体来说,当跨域身份认证系统首次登录区块链系统时,它需要通过创建并发布一笔交易来公布自己的钱包地址和一对临时的公私钥。在这笔交易中,发布者和接收者的身份都是指同一个实体,即进行登录操作的跨域身份认证系统本身。

[0113] S03:信息共享域的跨域身份认证系统通过区块链发布外部可访问的共享信息,并在区块链系统中进行数据同步。

[0114] S04:信息接收域的用户在本域的跨域身份认证系统中完成开户。

[0115] S05:信息接收域的用户登录本域的跨域身份认证系统。

[0116] 步骤S05涉及到用户登录跨域身份认证系统的过程。在这一步骤中,认证方式不局限于某一种特定的机制,而是可以采用任何现有的认证方式。例如,用户可以选择使用传统的账号加密码的方式进行认证,也可以采用基于生物特征的认证方式,如指纹识别等。

[0117] S06:信息接收域的跨域身份认证系统根据用户的权限返回可访问的外域资源列表。

[0118] S07:信息接收域的用户,发起共享信息的跨域访问请求。

[0119] S08:信息接收域的跨域身份认证系统,为本域用户随机生成一个唯一的临时ID,并为临时ID标注日期、时间和有效期,形成临时标识,然后使用信息接收域的临时私钥对临时标识进行签名,在跨域访问请求中扩展头域携带临时标识和信息接收域的钱包地址,通过区块链发布“用户临时标识-交易信息”。

[0120] S09:信息共享域的跨域身份认证系统,根据钱包地址找到临时公钥,然后使用临时公钥对临时标识进行验签,并从中得到临时ID。

[0121] S010:判定验签是否通过。如果验签通过且跨域身份认证系统需要知道外域访问

者的真实身份,则通过区块链发布特殊的交易信息。如果验签不通过,则向信息接收域返回错误报告。

[0122] 步骤S010描述了一种特殊的交易信息处理方式。在这步骤中,信息共享域作为发送者,向信息接收域发送特殊的交易信息。这笔交易的请求内容是使用信息接收域的临时公钥加密后的临时ID。这样的设计确保了信息的安全性和隐私性,因为只有拥有相应私钥的信息接收域才能解密并识别出真实的临时ID。

[0123] S011:信息系统为信息共享域的跨域身份认证系统开通访问权限,信息共享域的跨域身份认证系统通过该访问权限按照GB/T 28181协议标准或者GA/T 1400协议标准访问信息系统,请求获取相关的共享信息。

[0124] S012:信息系统根据GB/T 28181协议生成应答消息,发送至信息共享域的跨域身份认证系统。

[0125] S013:信息共享域的跨域身份认证系统,向信息接收域的跨域身份认证系统转发应答消息。

[0126] S014:信息接收域的跨域身份认证系统向用户转发应答消息,用户根据应答消息中的信息准备接收视频流。

[0127] S015:信息系统将视频流发送至信息接收域的用户。

[0128] S016:信息接收域的跨域身份认证系统,使用信息共享域的跨域身份认证系统的临时公钥,对用户的账户进行加密,然后将密文发送至信息共享域的跨域身份认证系统。

[0129] 综上所述,本发明第三实施例提供的视频共享跨域身份认证方法,通过区块链技术实现用户开户、生成临时公私钥对、发布可访问的视频信息、处理跨域访问请求、验证用户临时ID等步骤,确保了视频数据在跨域传输中的安全性和认证的可靠性,同时通过加密技术保护用户账户信息,降低了区块链系统的性能开销,提高了视频共享的效率和安全性。

[0130] 需要说明的是,上述多个实施例只是举例说明。各个实施例的技术方案之间可以进行组合,均在本发明的保护范围内。

[0131] 上面对本发明提供的跨域身份认证方法及系统进行了详细的说明。对本领域的一般技术人员而言,在不背离本发明实质内容的前提下对它所做的任何显而易见的改动,都将构成对本发明专利权的侵犯,将承担相应的法律责任。

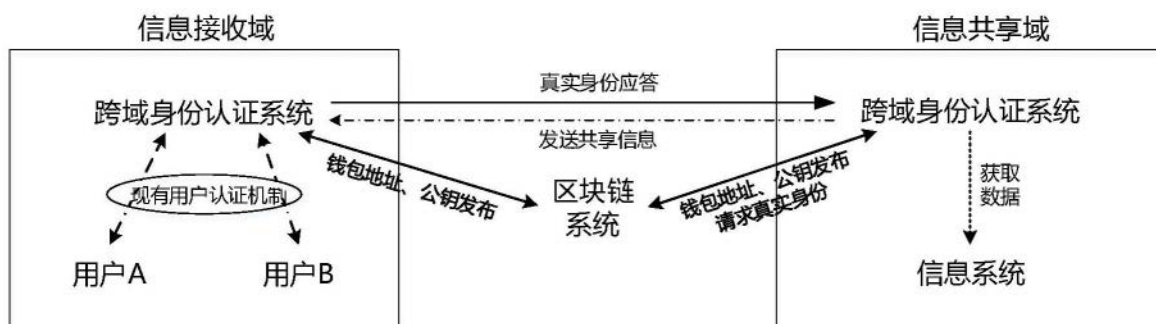


图1

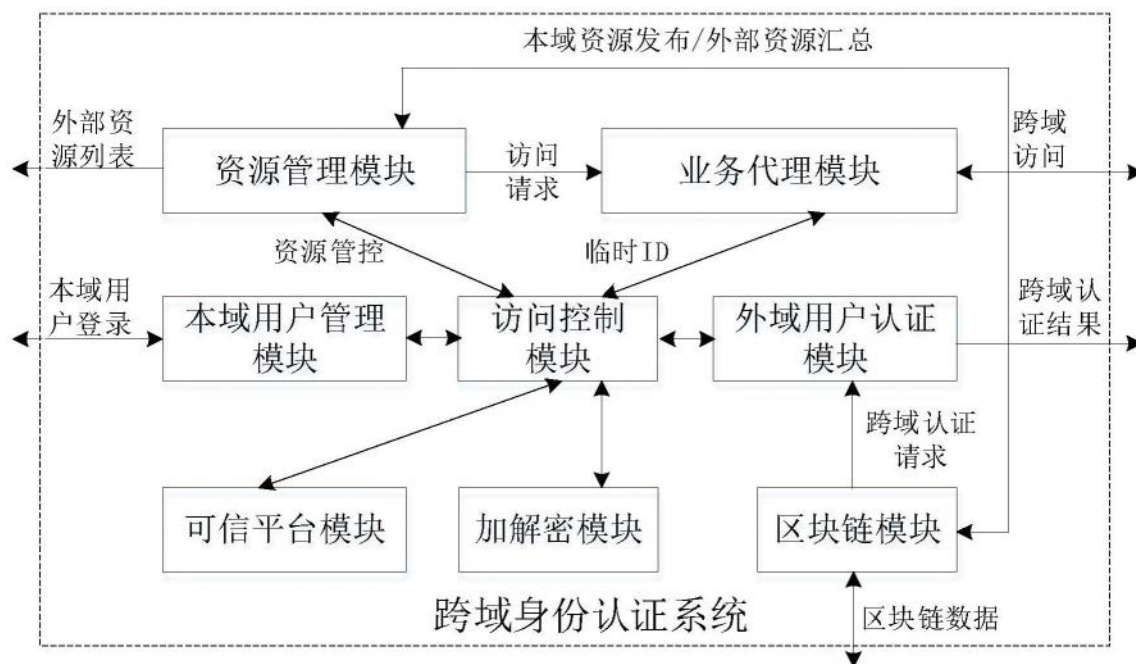


图2

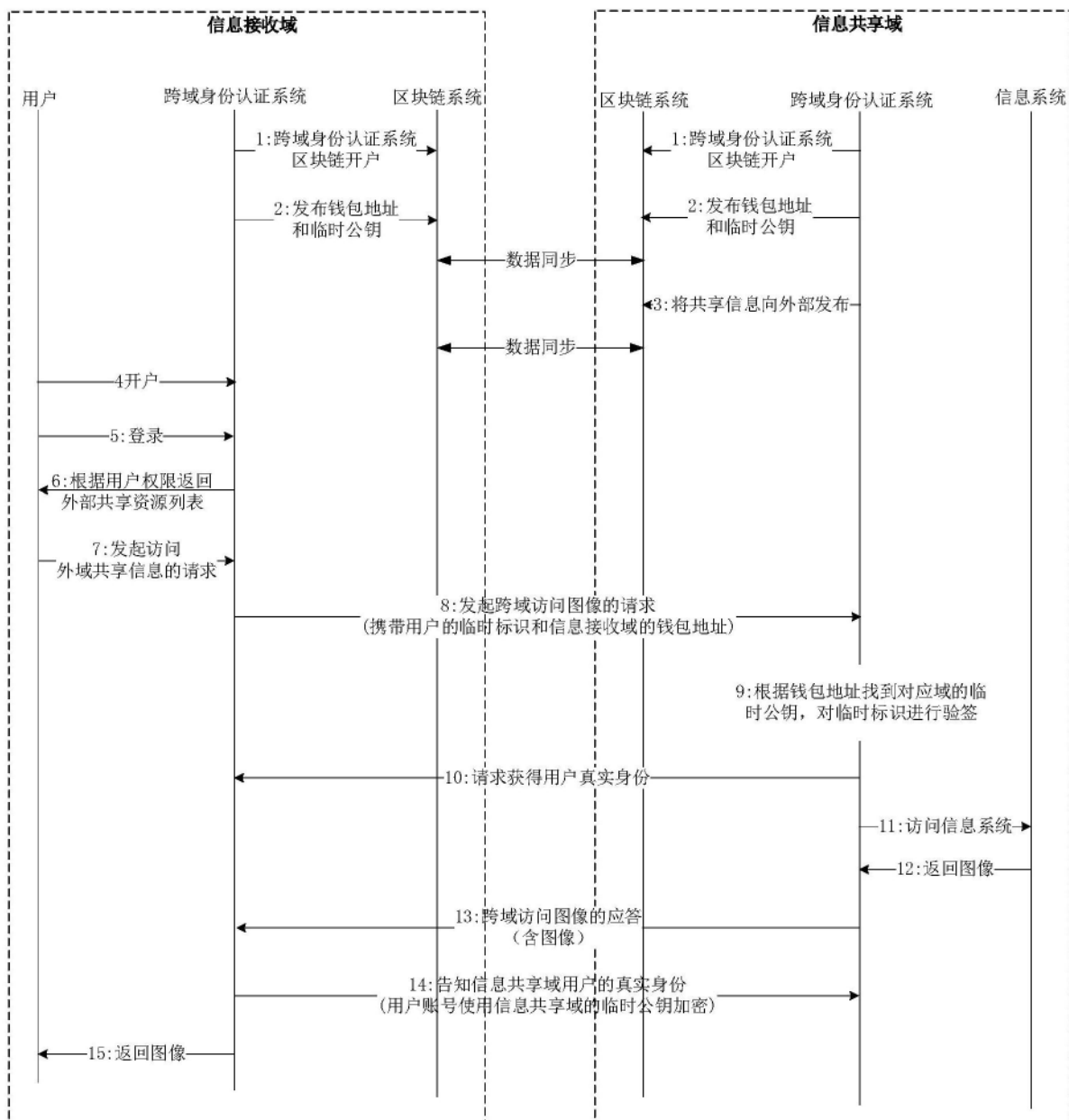


图3

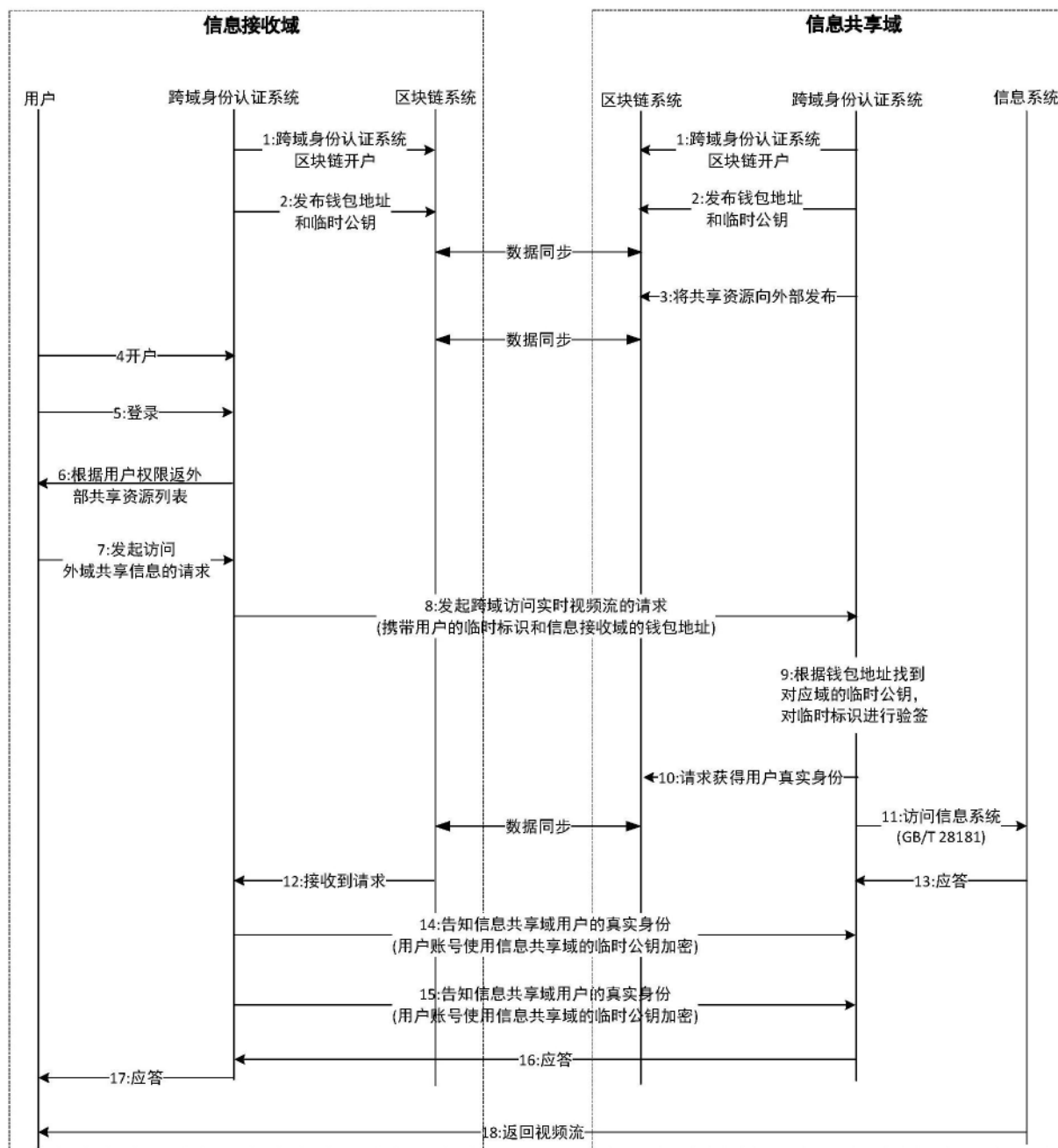


图4