可信组织机构身份平台

产品白皮书

目录

前 言

“身份”与每个人都息息相关，人们都在不同的地方拥有不同的身份属性，身份即一个人所有的属性和行为的集合。在现实生活中，我们拥有身份证、护照、驾照、企业工牌等，在以往，我们使用这些有着物理介质、或者部分电子化的凭据形式给出身份证明，但在产业互联网这个的大环境中，如何构造合理并可信的身份证明关系，使其具备数字化、网络化的特质，是值得探讨的课题。

另一方面，目前的产业应用尚未脱离互信互通的困境，数据孤岛和数据滥用的问题依旧存在。随着新基建等浪潮推动，产业互联网是进化的方向，人们日益重视隐私保护，数据成为生产要素，于是身份和相关凭据、数据的可信互通成为迫切的需求。

我们认为，在政策、技术和市场的共同驱动下，可信数字身份技术终将成为数字化进程的必然选择。我们的工作目标是希望最大化地挖掘可信数字身份技术的潜能，推动产业互联网技术的发展，促进可信数字身份技术与现有生态的融合。

荣泽科技在区块链+产业互联网的创新与实践过程中，逐渐认知到区块链+产业互联网并不单纯是一种技术，而是一种思维方式的变革，是一种社会化的“共识信任”理念，而推广这一理念不能依靠一家之力。因此荣泽科技聚集核心研发力量，倾力打造可信组织机构身份平台，期待携手合作伙伴共建区块链+产业互联网技术生态，落地更多的区块链+产业互联网“杀手锏”级应用。

荣泽科技愿意全面开放自身的区块链+产业互联网技术积累，与您互利共赢、共创未来！

1 概 述

1.1 现有数字身份痛点分析

从我们熟悉的互联网业务来看，用户的身份和数据已经一定程度上数字化和网络化，互联网公司通常也具备一整套处理认证和访问控制的业务系统。出于便利性考量，大多数互联网应用的数字身份以用户名密码为主，并结合真实身份认证完成实名验身。

互联网的账户体系通常从属于应用领域，如社交、电商等领域分别采用不同账号，这就使得用户要重复注册很多的账号密码。

其次，出于运营主体和运营壁垒考量，互联网业务在应用层面并不互联互通，跨应用的业务实现难度很大，尤其对于需要用户确权操作的跨应用业务，可能需要更改整个业务架构，以使得不同应用领域的用户身份。

互联网巨头依靠平台效应垄断市场，利用用户数据作为护城河，产生了大量价值，但用户对自己的数据并未拥有话语权和价值收入。用户的数字身份的关键控制点即账号密码，由服务商控制，对用户来说，仅为租借和使用服务商的服务，服务商可以决定账号禁用、服务终止，更进一步，由于利益驱使，围绕着用户数据发生的非法收集、数据泄露和买卖行为防不胜防，损害用户安全。

随着数字社会的发展，金融、政务、交通等实体经济领域也融合了大量的互联网因素，其原有的、基于物理介质和实体身份的认证体系在进化过程中，已经遭遇互联网服务类似的问题，由于实体经济的地域性特征更浓，安全等级要求更严，蕴含的价值更高，隐私挑战更大，事关国计民生，所以，身份认证带来的问题会更加突出。

综上所述，我们将其归结到三个痛点问题：

1、重复认证、多地认证的问题

例如，在金融场景下，同一公民去不同的银行开户需要分别进行 KYC，用户体验繁琐，身份数据相互重叠，数据可能存在差异甚至冲突。多头建设的身份体系存在诸多数据共享和使用上的障碍，不同企业主体间的数据信息分别存储，无法综合利用。

2、身份数据隐私与安全问题

用户身份信息散落在各个企业级的身份认证者手中,用户对自身信息的使用不够审慎,或者企业对用户身份进行信息验证都会引发身份信息的暴露,甚至对用户隐私信息造成严重侵犯。其次,用户身份信息在各家企业的服务器上存储,不同的企业对数据安全的重视程度和措施强度不同,使得用户的数据泄漏是一个木桶效应的问题,任何一处被攻破,用户的隐私即被泄露。用户个人信息维护成本昂贵。

3、中心化认证效率和容错性问题

在传统的 PKI 系统中,数字证书是认证的核心,它由相对权威的 CA 机构签发的。

一方面,这种中心结构可能存在性能问题,其涉及证书的所有操作,任务繁重,可能成为性能短板拖累效率,如庞大的已撤销证书列表的有效分发。另一方面,单中心的结构容易使其成为攻击的目标,一旦上级 CA 机构被攻破,则与之相关联的下级 CA 也会受到牵连。

1.2 可信数字身份

在政策、技术、市场因素的共同驱动下,产生了一种新的数字身份形态——分布式数字身份,它用分布式基础设施改变应用厂商控制数字身份的模式,让用户控制和管理数字身份,通过将数据所有权归还用户从根本上解决隐私问题。

要使身份具有真正的自我主权,这种基础设施必然需要驻留在分散信任的环境中。区块链技术的出现让自我主权身份的实现终于找到了突破口,作为分布式体系里的代表性技术,区块链有望成为分布式数字身份的技术基础。区块链技术用哈希链的数据结构改变了电子数据易被篡改的属性,用“区块+共识算法”解决分布式系统的数据一致性问题,拜占庭容错能力保证跨实体运行的系统不受少数节点恶意行为的影响,从而解决业务层面的信任难题,有望在服务商之间搭建互联互通的协议。

荣泽科技聚焦于分布式数字身份领域的可信组织机构身份,解决产业互联网中多组织协同时的统一身份问题,帮助多组织协同场景下的应用实现统一的身份鉴权、个人与组织的关系验证以及组织成员所代表的组织身份验证,促进了多应用互联及产业协同。

1.3 产品定位

多组织共同协作的业务场景中需要各参与方身份可信,从而使得业务过程的真实有效、结果不可抵赖。其可信身份体现在参与业务的主体（个人）公民身份可信、个人和组织的关系可信、组织成员所代表的组织身份可信。

可信组织机构身份平台是一种帮助管理、验证身份及身份关系的平台。即管理个人与组织的关系以及组织成员在产业协同中的所代表的组织身份,并为产业协同 DApp 提供个人身份鉴权服务、个人与组织关系验证服务、组织成员所代表的组织身份验证服务。

1.4 产品优势

提供多重的可信能力：

可信组织机构身份平台应用区块链网络作为基础设施,保障了身份数据在存储、传输以及使用中全程可信。

连接权威且中立的机构,对个人、组织以及个人与组织的真实关系进行验证,保障的身份数据的真实、可信。

（1）数据存储可信

可追溯能力：

采用分布式账本以及“区块+哈希链”的存储结构，使得历史数据永远留存且无法篡改，实现数据的全程可追溯。例如：

⑴ 组织成员外部身份的全生命周期的过程数据的追溯

⑵ 组织管理员的全生命周期的过程数据的追溯

⑶ 应用访问过程数据的追溯

应用访问个人身份的日志、应用访问组织身份的日志。

分布式存储的一致性：

采用分布式账本以及“区块+共识算法”，使得系统不受少数节点恶意行为的影响，保障了分布式存储的一致性。

（2）数据传输可信

数据传输信道可信：

采用传输信道加密技术，使得数据传输过程中不会泄漏与篡改，保障了数据传输信道的可信。

数据传输身份可信：

通过在数据传输时使用权威机构颁发的 CA 证书进行双向数字签名并互相验证对方的身份，保障了数据传输双方身份的可信。

（3）数据使用过程可信

采用智能合约以及安全沙箱技术，身份数据通过智能合约在安全沙箱中完成计算与验证，数据不会泄漏到沙箱之外，保障了数据使用过程的可信。

（4）证书/密钥可信

通过权威机构进行证书的签发和背书，通过 PKI 体系来实现公钥的安全分发，保障了证书/公钥的可信。

通过安全硬件（TEE）保存私钥，并通过生物特征加以保护，保障了私钥的安全。

（5）数据来源可信

连接权威且中立的机构，对个人身份、组织信息以及个人与组织的关系进行验证，从源头保障数据真实可信。

1. 连接工商数据，使得企业法定代表人身份更可信

2. 连接社保数据，使得组织和个人的关系更可信

3. 活体检测，并连接权威机构进行实名验证

（6）基于数据变化动态感知的安全预警

基于数据关系变化的动态感知，识别异常场景并自动预警，实现了事故预防能力。例如：

异常场景 1：组织管理员频繁变更

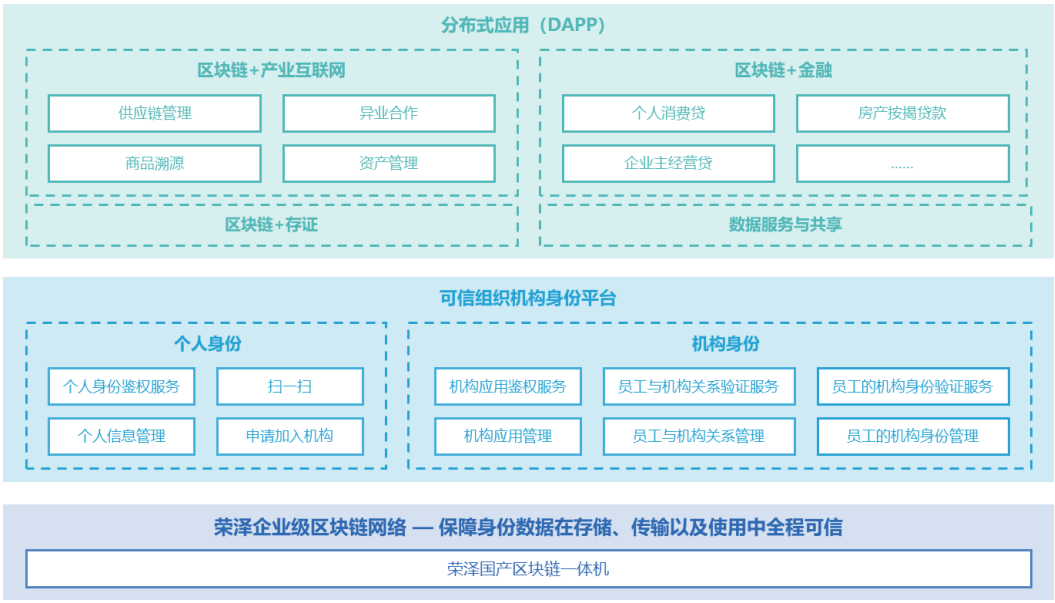
异常场景 2：成员的组织身份频繁变更

2 产品概述

可信组织机构身份平台旨在建立与维护跨平台、跨组织的可信组织机构身份网络，为多组织共同协作的应用提供统一、可信的身份验证及身份数据共享服务。

2.1 功能架构

可信组织机构身份平台的功能如下图所示，主要包括个人身份和组织身份两大部分。



（图 1）功能架构

可信组织机构身份平台以荣泽区块链技术为基础，用哈希链的数据结构改变了电子数据易被篡改的属性，用“区块+共识算法”解决分布式系统的数据一致性问题，拜占庭容错能力保证跨实体运行的系统不受少数节点恶意行为的影响，从而解决业务层面的信任难题，保障了数字身份的全流程可信。

2.2 功能介绍

2.2.1 个人场景

2.2.1.1 登录

支持用户使用手机号码+短信验证码登录，同时支持移动客户端扫码登录。

2.2.1.2 实名验证

个人登录系统,实名认证通过后执行其它操作。系统支持以下实名认证方式:

1、通过移动客户端活体检测+人脸识别，并连接权威且中立的机构在线完成个人身份的实名验证

2、上传身份证正反面及手持身份证正面照进行实名认证，此种认证方式需要平台管理员审核。

2.2.1.3 加入组织

个人通过实名认证后，可选择并申请加入组织（可同时加入多个组织），组织管理员审核通过后即可绑定个人与组织的关系,绑定后此人可称为组织的成员。

2.2.2 法定代表人或委托授权人的场景

2.2.2.1 新增组织

组织法定代表人或委托授权人可在平台注册组织机构。

法定代表人登录，上传营业执照及手持身份证正面照进行实名认证，此种认证方式需要平台管理员审核。也可在移动客户端通过法定代表人活体检测+人脸识别并连接权威机构在线完成组织的实名验证。

委托授权人认证登录，上传授权委托书/营业执照等，平台管理员审核通过后即可完成组织的注册。

组织注册成功后，法定代表人或委托授权人默认成为组织管理员。

2.2.2.2 组织管理员

实际场景中，法定代表人不可能常态化的去管理组织成员的外部身份，所以可增加其他人作为组织管理员。

如遇特殊情况,可以删除组织管理员(一个组织至少要有一个组织管理员)。

2.2.3 组织管理员的场景

2.2.3.1 应用管理

组织授权外部应用使用相关身份验证服务。组织管理员可以添加、删除、禁用、启用应用。

2.2.3.2 组织身份管理

组织身份指组织和外部应用管理方约定好参与其应用场景的组织身份，其中一个应用可以约定多个身份。组织身份管理功能包括定义组织身份、删除组织身份、组织成员关联组织身份、组织成员停用组织身份功能。

2.2.3.3 成员与组织关系管理

自然人申请加入组织后，需要组织管理员审核通过才能生效。

如遇特殊情况，可以将成员从组织移除，也可以临时锁定、解锁组织成员。

2.2.4 平台管理员的场景

2.2.4.1 管理应用

管理接入平台的应用，这些应用会形成信息列表提供给组织。组织在此列表基础上提供服务开放的功能。

平台管理员可以添加、删除、禁用、启用应用。

2.2.4.2 审核个人实名认证

审核自然人的实名认证。当采用活体检测+人脸识别并连接权威机构实名验证时，则由系统自动审核。

2.2.4.3 审核组织实名认证

审核组织的实名认证。当采用法定代表人活体检测+人脸识别并连接权威机构实名验证时，则由系统自动审核。

2.2.5 API 接口

2.2.5.1 个人身份鉴权

提供 API 接口或 SDK，验证个人是否为本系统实名用户。

2.2.5.2 个人与组织关系验证

提供 API 接口或 SDK，验证个人是否是组织成员。

2.2.5.3 员工的组织身份验证

提供 API 接口或 SDK，验证成员的组织身份是否真实可信。

3 应用领域

3.1 政务领域

政务信息化发展的难点在资源整合与应用，打破“各自为政、条块分割、烟囱林立、信息孤岛”的问题。由于业务烟囱的存在，其业务系统间不同数据格式、不同数据标准、不同数据管辖权造成了数据鸿沟，以及行政资源的浪费与行政效率的低下，无法实现政府内部纵向或横向协同，跨部门业务由业务申请人在数个政府部门之间奔跑传递。利用可信企业身份平台管理数据的所有权、管理权、使用权等，更好的服务于政务，有助于打破信息孤岛、促进协同、降低成本提高效率、提升政府透明化治理等作用。

3.2 供应链领域

供应链是一个商流、物流、信息流、资金流所共同组成的，并将行业内的供应商、制造商、分销商（零售商、批发商）、终端用户串联在一起的复杂网链结构。这种复杂的网链结构需要统一的识别码将不同系统中的组织、人、机、物等关联起来，而可信企业身份作为一种统一的数字身份平台，结合可信存证，与生俱来地适用于供应链领域。例如：物流、溯源防伪等。

3.3 物联网领域

物联网（IoT）蓬勃发展的今天，它不仅给个人消费带来变化，还给整个社会发展带来了深刻变化。目前，大型的物联网平台依靠中心化模型控制各个电子设备之间链接与交互，但是在很多场景下，这种方法变得不是那么实际。而可信身份平台正好可以解决这一问题。可信身份平台可以帮助管理物联网平台的各电子设备的关系、管理电子设备的所有权、管理权、使用权以及其产生的数据的所有权等，保证数据的安全性和可信性。可以企业身份在工业设备、智慧交通与智慧城市等领域都可以有很好的应用。

3.4 数据服务与共享

数据作为数字经济的生产资料，只有流通起来才能产生社会价值与经济价值。目前数据的流通面临数据的权属问题，即数据的所有权、管理权、使用权、受益权等。利用可信企业身份可追溯、不可篡改的特性，可以确保数据权属的真实性，

同时保证身份的不可伪造性。同时利用智能合约，数据可用不可见，进一步保护用户隐私以及数据生态的利益。

4 联系我们

官网：http://www.rongzer.com/

地址：南京市浦口区江北新区研创园腾飞大厦 B 座 17 楼

电话：18551702841

邮箱：ding.dan@rongzer.com