(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118199896 A
(43)申请公布日 2024.06.14

(21)申请号 202410598348.9

(22)申请日 2024.05.15

(71)申请人 北京劳咨链科技有限公司
地址 100162 北京市大兴区欣雅街15号院3号楼6层609

(72)发明人 陈百顺

(74)专利代理机构 北京纽乐康知识产权代理事务所(普通合伙) 11210
专利代理师 苏泳生

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 9/30(2006.01)

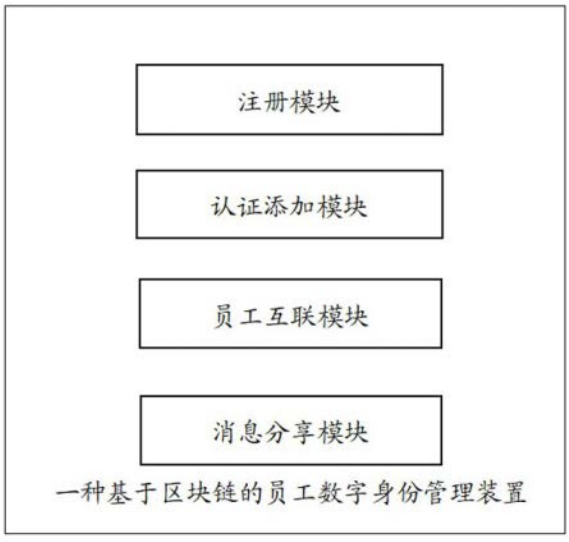
权利要求书3页 说明书10页 附图2页

(54)发明名称

一种基于区块链的员工数字身份管理装置及方法

(57)摘要

本发明涉及消息加密技术领域,并公开了一种基于区块链的员工数字身份管理装置及方法,其装置包括:注册模块,用于对每个人员的身份信息进行身份注册,获得每个员工的数字身份公钥和数字身份私钥;认证添加模块,用于基于员工的数字身份公钥对申请登陆的员工进行身份认证,基于身份认证结果对员工的好友列表进行添加,获得每个员工的互联列表;员工互联模块,用于基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;消息分享模块,用于基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。本发明实现了对企业的员工之间传输的消息加密,采用加密技术保证公司数据的安全。



CN 118199896 A

1.一种基于区块链的员工数字身份管理装置,其特征在于,包括:

注册模块,用于对每个人员的身份信息进行身份注册,获得每个员工的数字身份公钥和数字身份私钥;

认证添加模块,用于基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,基于身份认证结果对每个员工的好友列表进行添加,获得每个员工的互联列表;

员工互联模块,用于基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;

消息分享模块,用于基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。

2.根据权利要求1所述的一种基于区块链的员工数字身份管理装置,其特征在于,注册模块,包括:

身份信息获取子模块,用于获取每个人员上传的身份信息,并对每个人员上传的信息进行真实性审核,获得每个人员的真实性审核结果;

密钥生成子模块,用于基于每个人员的审核结果进行员工的身份注册,并生成每个完成身份注册的员工的密钥。

3.根据权利要求2所述的一种基于区块链的员工数字身份管理装置,其特征在于,身份信息获取子模块,包括:

获取单元,用于获取每个人员上传的身份信息,其中身份信息包括:姓名、身份证号、部门职位、工号;

审核单元,用于实时接收对人员上传的身份信息的人工审核结果时,当接收的人工审核结果为通过时,将对应人员标定为员工,并将审核通过当作对应人员的真实性审核结果,当接收的人工审核结果为不通过时,将对应人员标定为非员工,并将审核不通过作为对应人员的真实性审核结果。

4.根据权利要求2所述的一种基于区块链的员工数字身份管理装置,其特征在于,密钥生成子模块,包括:

注册单元,用于对所有真实性审核结果为审核通过的员工进行身份注册,并随机生成一个预设长度的数字串作为每个真实性审核结果为审核通过的员工的账号,且当随机生成的数字串与所有历史生成的数字串存在完全重合时,重新进行数字串的随机生成;

生成单元,用于对所有被标定为员工的人员进行密钥的生成分配,获得每个员工的数字身份公钥和数字身份私钥。

5.根据权利要求4所述的一种基于区块链的员工数字身份管理装置,其特征在于,生成单元对所有标定为员工的人员进行密钥的生成分配的方法,包括:

在预设质数集合中随机选取出两个质数m和n,其中两个质数m和n在预设质数集合中的间隔不大于预设个数间隔;

基于选取出的质数m和n确定出公钥设定数δ满足以下公式的所有取值:

$$\gcd\left[\frac{\left(\delta^{mcn(m-1,n-1)} * \mathrm{mod}(m,n)\right)}{m*n},(m*n)^2\right]=1;$$

其中，gcd（number1,number2）为两个正整数的最大公约数，δ为公钥设定数，$mcn(m-1,n-1)$为$m-1$和$n-1$的最小公倍数，$mod(m,n)$为质数m和n进行相除运算的余数；

将公钥设定数δ的所有取值中的最小值设定为员工的数字身份公钥，并基于质数m和n的最终取值，确定出$mcn(m-1,n-1)$的数值作为员工的数字身份私钥。

6.根据权利要求1所述的一种基于区块链的员工数字身份管理装置，其特征在于，认证添加模块，包括：

身份认证子模块，用于基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证，获得身份认证结果，其中身份认证结果为认证通过和认证不通过；

好友添加子模块，用于获取所有条添加好友申请的申请方的身份认证结果和被申请方的身份认证结果，当申请方的身份认证结果和被申请方的身份认证结果都为认证通过时，基于对应条添加好友申请更新对应的申请方和被申请方的好友列表，获得每个员工的互联列表。

7.根据权利要求6所述的一种基于区块链的员工数字身份管理装置，其特征在于，身份认证子模块基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证获得身份认证结果的方法，包括：

将系统中的所有员工账号及员工的数字身份公钥保存至系统数据终端，并实时接收登陆员工的输入信息，其中输入信息包括员工账号；

基于输入信息从系统数据终端获得登陆员工的数字身份公钥，基于登陆员工的数字身份公钥对从预设登陆题库中任选的题目进行加密，并将加密题目由系统后台发送至登陆员工端；

当系统后台在预设时间内接收到来自登陆员工端的加密题目的正确答案时，将认证通过作为对应登陆员工的身份认证结果，当系统后台在预设时间内未接收到来自登陆员工端的加密题目的正确答案时，将认证不通过作为对应登陆员工的身份认证结果。

8.根据权利要求5所述的一种基于区块链的员工数字身份管理装置，其特征在于，员工互联模块基于每个员工的互联列表对互联双方的消息传输过程进行加密的方法，包括：

获取互联双方中进行消息传输一方的传输消息，并将传输消息进行二进制转换，获得传输消息的二进制表示；

若检测到申请互联的双方各自的互联列表中存在对方的账号时，基于区块链将各自的数字身份公钥发送给对方，并基于互联双方的公钥对互联双方的消息传输过程进行加密，即为：

$$M=\frac{m^{E}*mod(m_1,n_1)}{\ln(1+m_1*n_1)}$$；

其中，M为对传输消息的二进制表示进行加密后的加密消息的二进制表示，m为传输消息的二进制表示，E为互联双方中接收消息的一方的数字身份公钥，$mod(m_1,n_1)$为质数m_1和n_1进行相除运算的余数，m_1和n_1互联双方中接收消息的一方获取数字身份公钥时对应的两个质数，ln为自然对数，且自然常数e的取值为2.718。

9.根据权利要求1所述的一种基于区块链的员工数字身份管理装置,其特征在于,消息分享模块基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密的方法,包括:

获取申请消息分享的员工进行消息分享的分享消息,并将分享消息进行二进制转换,获得分享消息的二进制表示;

获取申请消息分享的员工的互联列表,并基于区块链将进行消息分享的员工的数字身份公钥发送给互联列表中的所有好友;

基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,即为:

$$W=\frac{w^{Q}*\mathrm{mod}(m_2,n_2)}{\ln(1+m_2*n_2)};$$

其中,W为对分享消息的二进制表示进行加密的加密消息的二进制表示,w为分享传输的二进制表示,Q为进行消息分享的员工的数字身份私钥,$\mathrm{mod}(m_2,n_2)$为质数m_2和n_2进行相除运算的余数,m_2和n_2为进行消息分享的一方获取数字身份私钥时对应的两个质数,$\ln$为自然对数,且自然常数e的取值为2.718。

10.一种基于区块链的员工数字身份管理方法,其特征在于,应用于执行权利要求1至9中任一所述的一种基于区块链的员工数字身份管理装置,包括:

S1:对每个人员的身份信息进行身份注册,获得每个员工的数字身份公钥和数字身份私钥;

S2:基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,基于身份认证结果对每个员工的好友列表进行添加,获得每个员工的互联列表;

S3:基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;

S4:基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。

一种基于区块链的员工数字身份管理装置及方法

技术领域

[0001] 本发明涉及消息加密技术领域,特别涉及一种基于区块链的员工数字身份管理装置及方法。

背景技术

[0002] 目前,传统的互联网身份管理模型依赖一个可信的第三方机构,个人的身份信息不在用户自己手中,而在一个中心化的第三方机构中。但随着社会的发展,中心化机构维护用户身份的代价越来越大,中心化服务结构暴露出的用户个人信息和消息传输泄露问题,使得人们越来越重视自己的隐私信息,传统的身份管理面临的难题急需解决。区块链作为一种新兴的综合性技术,将区块链技术和身份管理进行结合,是身份管理方面的一次质的飞跃,尤其是对一些数据须进行保密的公司,例如大数据公司,它们的数据需要保证安全性和可追溯性,公司员工之间的消息传输使用U盘等设备拷贝太繁琐,但使用社交平台传输难以保证安全和保密性,所以急需依靠区块链技术达到员工间消息加密传输的目的。

[0003] 但是,现有的基于区块链的员工数字身份管理装置及方法只是将区块链与传统企业中人力资源管理工作相融合,建立职工信用管理系统,通过信用积分对职工的个人工作行为表现进行量化追踪,未考虑如何对企业的员工之间传输的消息进行加密,也未考虑采用加密技术保证有关公司数据的安全。例如公开号为“CN114579943A”、专利名称为“一种基于区块链的职工数字身份管理系统及方法”,其方法包括以下步骤:系统包括普通员工个人终端、上级组织管理终端、后台云服务器、区块链上智能合约与区块链下分布式数据库。本发明将区块链与传统企业中人力资源管理工作相融合,建立职工信用管理系统,通过信用积分对职工的个人工作行为表现进行量化追踪。解决了传统企业管理工作中职工个人评价标准量化不足,员工档案信息流转过程复杂,缺乏可信任环境,数据易被篡改和泄露等问题,通过区块链技术不可篡改,可溯源,低成本搭建分布式可信任环境等优势,来保障职工信息在记录和流转过程中的安全可信。但是只是将区块链与传统企业中人力资源管理工作相融合,建立职工信用管理系统,通过信用积分对职工的个人工作行为表现进行量化追踪,未考虑如何对企业的员工之间传输的消息进行加密,也未考虑采用加密技术保证有关公司数据的安全。

[0004] 因此,本发明提出了一种基于区块链的员工数字身份管理装置及方法,用以对企业的员工之间传输的消息进行加密,采用加密技术保证有关公司数据的安全。

发明内容

[0005] 本发明提供一种基于区块链的员工数字身份管理装置及方法,用以基于对每个员工生成分配的数字身份公钥和数字身份私钥,实现了更安全、更准确地对互联双方的消息传输过程和对消息分享传输过程的加密,实现了员工间信息或数据交流的保密性和安全性。

[0006] 本发明提供一种基于区块链的员工数字身份管理装置,包括:

注册模块,用于对每个人员的身份信息进行身份注册,获得每个员工的数字身份公钥和数字身份私钥;

认证添加模块,用于基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,基于身份认证结果对每个员工的好友列表进行添加,获得每个员工的互联列表;

员工互联模块,用于基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;

消息分享模块,用于基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。

[0007] 优选的,基于区块链的员工数字身份管理装置,注册模块,包括:

身份信息获取子模块,用于获取每个人员上传的身份信息,并对每个人员上传的信息进行真实性审核,获得每个人员的真实性审核结果;

密钥生成子模块,用于基于每个人员的审核结果进行员工的身份注册,并生成每个完成身份注册的员工的密钥。

[0008] 优选的,基于区块链的员工数字身份管理装置,身份信息获取子模块,包括:

获取单元,用于获取每个人员上传的身份信息,其中身份信息包括:姓名、身份证号、部门职位、工号;

审核单元,用于实时接收对人员上传的身份信息的人工审核结果时,当接收的人工审核结果为通过时,将对应人员标定为员工,并将审核通过当作对应人员的真实性审核结果,当接收的人工审核结果为不通过时,将对应人员标定为非员工,并将审核不通过作为对应人员的真实性审核结果。

[0009] 优选的,基于区块链的员工数字身份管理装置,密钥生成子模块,包括:

注册单元,用于对所有真实性审核结果为审核通过的员工进行身份注册,并随机生成一个预设长度的数字串作为每个真实性审核结果为审核通过的员工的账号,且当随机生成的数字串与所有历史生成的数字串存在完全重合时,重新进行数字串的随机生成;

生成单元,用于对所有被标定为员工的人员进行密钥的生成分配,获得每个员工的数字身份公钥和数字身份私钥。

[0010] 优选的,基于区块链的员工数字身份管理装置,生成单元对所有标定为员工的人员进行密钥的生成分配的方法,包括:

在预设质数集合中随机选取出两个质数m和n,其中两个质数m和n在预设质数集合中的间隔不大于预设个数间隔;

基于选取出的质数m和n确定出公钥设定数δ满足以下公式的所有取值:

$$\gcd\left[\frac{\left(\delta^{mcn(m-1,n-1)} * \mathrm{mod}(m,n)\right)}{m*n},(m*n)^2\right]=1;$$

其中,gcd(number1,number2)为两个正整数的最大公约数,δ为公钥设定数,$mcn(m-1,n-1)$为$m-1$和$n-1$的最小公倍数,$\mathrm{mod}(m,n)$为质数m和n进行相除运算的余数;

将公钥设定数δ的所有取值中的最小值设定为员工的数字身份公钥,并基于质数m和n的最终取值,确定出$mcn(m-1,n-1)$的数值作为员工的数字身份私钥。

[0011] 优选的,基于区块链的员工数字身份管理装置,认证添加模块,包括:

身份认证子模块,用于基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,其中身份认证结果为认证通过和认证不通过;

好友添加子模块,用于获取所有条添加好友申请的申请方的身份认证结果和被申请方的身份认证结果,当申请方的身份认证结果和被申请方的身份认证结果都为认证通过时,基于对应条添加好友申请更新对应的申请方和被申请方的好友列表,获得每个员工的互联列表。

[0012] 优选的,基于区块链的员工数字身份管理装置,身份认证子模块基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证获得身份认证结果的方法,包括:

将系统中的所有员工账号及员工的数字身份公钥保存至系统数据终端,并实时接收登陆员工的输入信息,其中输入信息包括员工账号;

基于输入信息从系统数据终端获得登陆员工的数字身份公钥,基于登陆员工的数字身份公钥对从预设登陆题库中任选的题目进行加密,并将加密题目由系统后台发送至登陆员工端;

当系统后台在预设时间内接收到来自登陆员工端的加密题目的正确答案时,将认证通过作为对应登陆员工的身份认证结果,当系统后台在预设时间内未接收到来自登陆员工端的加密题目的正确答案时,将认证不通过作为对应登陆员工的身份认证结果。

[0013] 优选的,基于区块链的员工数字身份管理装置,员工互联模块基于每个员工的互联列表对互联双方的消息传输过程进行加密的方法,包括:

获取互联双方中进行消息传输一方的传输消息,并将传输消息进行二进制转换,获得传输消息的二进制表示;

若检测到申请互联的双方各自的互联列表中存在对方的账号时,基于区块链将各自的数字身份公钥发送给对方,并基于互联双方的公钥对互联双方的消息传输过程进行加密,即为:

$$M=\frac{m^{E}*\mathrm{mod}(m_1,n_1)}{\ln(1+m_1*n_1)};$$

其中,M为对传输消息的二进制表示进行加密后的加密消息的二进制表示,m为传输消息的二进制表示,E为互联双方中接收消息的一方的数字身份公钥,$\mathrm{mod}(m_1,n_1)$为质数m_1和n_1进行相除运算的余数,m_1和n_1为互联双方中接收消息的一方获取数字身份公钥时对应的两个质数,ln为自然对数,且自然常数e的取值为2.718。

[0014] 优选的,基于区块链的员工数字身份管理装置,消息分享模块基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密的方法,包括:

获取申请消息分享的员工进行消息分享的分享消息,并将分享消息进行二进制转换,获得分享消息的二进制表示;

获取申请消息分享的员工的互联列表,并基于区块链将进行消息分享的员工的数字身份公钥发送给互联列表中的所有好友;

基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,即为:

$$W=\frac{w^{Q}*\mathrm{mod}(m_2,n_2)}{\ln(1+m_2*n_2)};$$

其中,W为对分享消息的二进制表示进行加密的加密消息的二进制表示,w为分享传输的二进制表示,Q为进行消息分享的员工的数字身份私钥,$\mathrm{mod}(m_2,n_2)$为质数m_2和n_2进行相除运算的余数,m_2和n_2为进行消息分享的一方获取数字身份私钥时对应的两个质数,ln为自然对数,且自然常数e的取值为2.718。

[0015] 本发明提供一种基于区块链的员工数字身份管理方法,应用于实施例1至9中任一一种基于区块链的员工数字身份管理装置,包括:

S1:对每个人员的身份信息进行身份注册,获得每个员工的数字身份公钥和数字身份私钥;

S2:基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,基于身份认证结果对每个员工的好友列表进行添加,获得每个员工的互联列表;

S3:基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;

S4:基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。

[0016] 本发明相对于现有技术产生的有益效果为:基于对每个员工生成分配的数字身份公钥和数字身份私钥,更安全、更准确地对互联双方的消息传输过程和对消息分享传输过程的加密,实现了员工间信息或数据交流的保密性和安全性。

[0017] 本发明的其它特征和优点将在随后的说明书中阐述,并且,部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的本申请文件中所特别指出的结构来实现和获得。

[0018] 下面通过附图和实施例,对本发明的技术方案做进一步的详细描述。

附图说明

[0019] 附图用来提供对本发明的进一步理解,并且构成说明书的一部分,与本发明的实施例一起用于解释本发明,并不构成对本发明的限制。在附图中:

图1为本发明实施例中一种基于区块链的员工数字身份管理装置示意图;

图2为本发明实施例中一种基于区块链的员工数字身份管理方法流程图。

具体实施方式

[0020] 以下结合附图对本发明的优选实施例进行说明,应当理解,此处所描述的优选实施例仅用于说明和解释本发明,并不用于限定本发明。

实施例1:

[0021] 本发明提供了一种基于区块链的员工数字身份管理装置,参考图1,包括:

注册模块,用于对每个人员的身份信息进行身份注册,获得每个员工的数字身份

公钥和数字身份私钥;

认证添加模块,用于基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,基于身份认证结果对每个员工的好友列表进行添加,获得每个员工的互联列表;

员工互联模块,用于基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;

消息分享模块,用于基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。

[0022] 该实施例中,身份信息包括每个人员的姓名、身份证号、部门职位、工号。

[0023] 该实施例中,身份注册为接收人员上传的对身份信息的人工审核结果,并对所有真实性审核结果为审核通过的员工进行身份注册进而获得员工账号的过程。

[0024] 该实施例中,数字身份公钥和数字身份私钥为对所有被标定为员工的人员分配的、用以对发送信息进行加密或解密的算法。

[0025] 该实施例中,申请系统登陆为向基于区块链的员工数字身份管理装置进行登陆或访问申请的过程。

[0026] 该实施例中,身份认证为基于员工的数字身份公钥和系统数据终端对申请系统登陆的员工进行身份真实性验证的过程。

[0027] 该实施例中,身份认证结果包括认证通过和认证不通过两种情况。

[0028] 该实施例中,好友列表为每个员工在基于区块链的员工数字身份管理装置中可进行消息传输和消息分享的人员列表。

[0029] 该实施例中,添加为基于添加好友申请对每个员工在基于区块链的员工数字身份管理装置中可进行消息传输和消息分享的人员列表进行更新的过程。

[0030] 该实施例中,互联列表为对每个员工的好友列表进行更新后获得的最新的可进行消息传输和消息分享的人员列表。

[0031] 该实施例中,互联双方为进行互相的消息传输的两方。

[0032] 该实施例中,消息传输为互联双方之间进行消息发送的过程。

[0033] 该实施例中,对互联双方的消息传输过程进行加密为基于互联双方的数字身份公钥对互联双方之间进行发送的消息的二进制表示进行加密的过程。

[0034] 该实施例中,互联传输加密结果为基于互联双方的数字身份公钥对互联双方之间进行发送的消息的二进制表示进行加密的结果。

[0035] 该实施例中,消息分享为对每个员工的互联列表中的所有好友进行分享消息的过程。

[0036] 该实施例中,对消息分享传输过程进行加密为基于每个员工的数字身份私钥对分享传输的消息的二进制表示进行加密的过程。

[0037] 该实施例中,分享传输加密结果为基于每个员工的数字身份私钥对分享传输的消息的二进制表示进行加密的结果。

[0038] 以上技术的有益效果为:基于对每个员工生成分配的数字身份公钥和数字身份私钥更安全、更准确地地对互联双方的消息传输过程和对消息分享传输过程进行加密,实现了员工间信息或数据交流的保密性和安全性。

[0039] 实施例2:在实施例1的基础上,基于区块链的员工数字身份管理装置,注册模块,包括:

身份信息获取子模块,用于获取每个人员上传的身份信息,并对每个人员上传的信息进行真实性审核,获得每个人员的真实性审核结果;

密钥生成子模块,用于基于每个人员的审核结果进行员工的身份注册,并生成每个完成身份注册的员工的密钥。

[0040] 该实施例中,真实性审核为对每个人员上传的身份信息进行判断上传的身份信息是否为公司员工的人工审核。

[0041] 该实施例中,真实性审核结果包括审核通过和审核不通过。

[0042] 该实施例中,员工的密钥为每个员工的数字身份公钥和数字身份私钥。

[0043] 以上技术的有益效果为:基于每个人员上传的身份信息更精确地判断上传的身份信息是否为公司员工,更精确地对被判定为员工的人员进行账号的分配和密钥的生成。

[0044] 实施例3:

在实施例2的基础上,基于区块链的员工数字身份管理装置,身份信息获取子模块,包括:

获取单元,用于获取每个人员上传的身份信息,其中身份信息包括:姓名、身份证号、部门职位、工号;

审核单元,用于实时接收对人员上传的身份信息的人工审核结果时,当接收的人工审核结果为通过时,将对应人员标定为员工,并将审核通过当作对应人员的真实性审核结果,当接收的人工审核结果为不通过时,将对应人员标定为非员工,并将审核不通过作为对应人员的真实性审核结果。

[0045] 该实施例中,人工审核结果为审核人员进行的基于实时接收对人员上传的身份信息判断上传的身份信息是否为公司员工的审核,其中人工审核结果包括通过和不通过。

[0046] 该实施例中,标定为对上传的身份信息对应的人员进行的身份的标示确定,其中身份包括员工和非员工。

[0047] 以上技术的有益效果为:基于实时接收的所有人员上传的身份信息更准确地标定出身份为员工的人员和身份为非员工的人员,便于后续身份注册。

[0048] 实施例4:

在实施例2的基础上,基于区块链的员工数字身份管理装置,密钥生成子模块,包括:

注册单元,用于对所有真实性审核结果为审核通过的员工进行身份注册,并随机生成一个预设长度的数字串作为每个真实性审核结果为审核通过的员工的账号,且当随机生成的数字串与所有历史生成的数字串存在完全重合时,重新进行数字串的随机生成;

生成单元,用于对所有被标定为员工的人员进行密钥的生成分配,获得每个员工的数字身份公钥和数字身份私钥。

[0049] 该实施例中,预设长度为预先设置的员工账号中包含的字符总数,例如12个字符。

[0050] 该实施例中,员工的账号为每个员工用于登陆基于区块链的员工数字身份管理装置所需的、表征每个员工身份的数字串,且每个员工对应一个账号,账号不会出现重合。

[0051] 该实施例中,数字串为由多个纯数字组成的一串数字。

[0052] 该实施例中,历史生成的数字串为注册单元在之前生成的所有的被当作员工账号的数字串。

[0053] 该实施例中,完全重合为随机生成的数字串与所有历史生成的数字串中的至少一个数字串完全相同。

[0054] 该实施例中,生成分配为基于预设质数集合中随机选取出两个质数对所有被标定为员工的人员进行密钥的生成的过程。

[0055] 以上技术的有益效果为:实现对所有员工进行账号的分配,并对每个员工的密钥进行了更精确地的生成,便于后续对传输消息的二进制表示和对分享消息的二进制表示的加密。

[0056] 实施例5:

在实施例4的基础上,基于区块链的员工数字身份管理装置,生成单元对所有标定为员工的人员进行密钥的生成分配的方法,包括:

在预设质数集合中随机选取出两个质数m和n,其中两个质数m和n在预设质数集合中的间隔不大于预设个数间隔;

基于选取出的质数m和n确定出公钥设定数δ满足以下公式的所有取值:

$$\gcd\left[\frac{\left(\delta^{mcn(m-1,n-1)} * \mathrm{mod}(m,n)\right)}{m*n},(m*n)^2\right]=1;$$

其中,gcd(number1,number2)为两个正整数的最大公约数,δ为公钥设定数,$mcn(m-1,n-1)$为$m-1$和$n-1$的最小公倍数,$\mathrm{mod}(m,n)$为质数m和n进行相除运算的余数;

将公钥设定数δ的所有取值中的最小值设定为员工的数字身份公钥,并基于质数m和n的最终取值,确定出$mcn(m-1,n-1)$的数值作为员工的数字身份私钥。

[0057] 该实施例中,预设质数集合为预先设置的用以生成每个员工的密钥的质数集合。

[0058] 该实施例中,预设个数间隔为预先设置的用以确保随机选取出两个质数不影响密钥生成的质数间隔,例如两个质数m和n在预设质数集合中间隔内存在的质数总个数不超过8。

[0059] 该实施例中,公钥设定数为用以确定出每个员工的数字身份公钥和数字身份私钥的中间数。

[0060] 以上技术的有益效果为:基于选取出的质数m和n更精确地获得所有公钥设定数,并基于公钥设定数的所有取值中的最小值更精确地获得每个员工的数字身份公钥和数字身份私钥,此实施例给出了一种基于公钥设定数确定员工的数字身份公钥和数字身份私钥的方法。

[0061] 实施例6:

在实施例1的基础上,基于区块链的员工数字身份管理装置,认证添加模块,包括:

身份认证子模块,用于基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证,获得身份认证结果,其中身份认证结果为认证通过和认证不通过;

好友添加子模块,用于获取所有条添加好友申请的申请方的身份认证结果和被申

请方的身份认证结果,当申请方的身份认证结果和被申请方的身份认证结果都为认证通过时,基于对应条添加好友申请更新对应的申请方和被申请方的好友列表,获得每个员工的互联列表。

[0062] 该实施例中,添加好友申请为每个员工基于员工数字身份管理装置申请将其他员工添加入互联列表的请求。

[0063] 以上技术的有益效果为:基于身份认证结果更及时地将申请方和被申请方的好友列表进行更新,此实施例给出了一种对员工的互联列表进行实时更新的方法。

[0064] 实施例7:

在实施例6的基础上,基于区块链的员工数字身份管理装置,身份认证子模块基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证获得身份认证结果的方法,包括:

将系统中的所有员工账号及员工的数字身份公钥保存至系统数据终端,并实时接收登陆员工的输入信息,其中输入信息包括员工账号;

基于输入信息从系统数据终端获得登陆员工的数字身份公钥,基于登陆员工的数字身份公钥对从预设登陆题库中任选的题目进行加密,并将加密题目由系统后台发送至登陆员工端;

当系统后台在预设时间内接收到来自登陆员工端的加密题目的正确答案时,将认证通过作为对应登陆员工的身份认证结果,当系统后台在预设时间内未接收到来自登陆员工端的加密题目的正确答案时,将认证不通过作为对应登陆员工的身份认证结果。

[0065] 该实施例中,系统数据终端为基于区块链的员工数字身份管理装置中存储所有员工账号及员工的数字身份公钥的子装置。

[0066] 该实施例中,预设登陆题库为预先设置的用以对登陆员工进行身份认证的题目库,例如1+1=?。

[0067] 该实施例中,加密题目为对从预设登陆题库中选出的题目进行加密后获得的题目。

[0068] 该实施例中,正确答案为预设登陆题库中加密题目的答案。

[0069] 以上技术的有益效果为:基于预设登陆题库和员工的数字身份公钥实现对登陆员工进行更精确、更安全地的身份认证,此实施例给出了一种基于预设登陆题库和员工的数字身份公钥对登陆员工进行身份认证的方法,便于后续对好友列表进行更新。

[0070] 实施例8:

在实施例5的基础上,基于区块链的员工数字身份管理装置,员工互联模块基于每个员工的互联列表对互联双方的消息传输过程进行加密的方法,包括:

获取互联双方中进行消息传输一方的传输消息,并将传输消息进行二进制转换,获得传输消息的二进制表示;

若检测到申请互联的双方各自的互联列表中存在对方的账号时,基于区块链将各自的数字身份公钥发送给对方,并基于互联双方的公钥对互联双方的消息传输过程进行加密,即为:

$$M=\frac{m^{E}*\mathrm{mod}(m_1,n_1)}{\ln(1+m_1*n_1)};$$

其中，M为对传输消息的二进制表示进行加密后的加密消息的二进制表示，m为传输消息的二进制表示，E为互联双方中接收消息的一方的数字身份公钥，$mod(m_1,n_1)$为质数m_1和n_1进行相除运算的余数，m_1和n_1为互联双方中接收消息的一方获取数字身份公钥时对应的两个质数，ln为自然对数，且自然常数e的取值为2.718。

[0071] 该实施例中，传输消息的二进制表示为对互联双方传输给对方的消息进行二进制转换获得的二进制表示。

[0072] 该实施例中，公式中二进制数和十进制数可以直接进行位级相乘运算，在计算机科学领域被称为按位与，当二进制数值和十进制数值进行位级相乘运算时，首先将二进制数值和十进制数值都转换为二进制表示，然后，按照二进制位级的规则进行逐位相乘、求和，最后将结果转换回十进制或二进制表示。

[0073] 以上技术的有益效果为：基于互联双方的公钥对互联双方的传输消息的二进制表示进行加密，实现了消息传输的保密性和安全性，此实施例给出了一种对传输消息的二进制表示进行加密的方法。

[0074] 实施例9：

在实施例1的基础上，基于区块链的员工数字身份管理装置，消息分享模块基于每个员工的互联列表进行消息分享，并对消息分享传输过程进行加密的方法，包括：

获取申请消息分享的员工进行消息分享的分享消息，并将分享消息进行二进制转换，获得分享消息的二进制表示；

获取申请消息分享的员工的互联列表，并基于区块链将进行消息分享的员工的数字身份公钥发送给互联列表中的所有好友；

基于每个员工的互联列表进行消息分享，并对消息分享传输过程进行加密，即为：

$$W=\frac{w^{Q}*mod(m_2,n_2)}{\ln(1+m_2*n_2)};$$

其中，W为对分享消息的二进制表示进行加密的加密消息的二进制表示，w为分享传输的二进制表示，Q为进行消息分享的员工的数字身份私钥，$mod(m_2,n_2)$为质数m_2和n_2进行相除运算的余数，m_2和n_2为进行消息分享的一方获取数字身份私钥时对应的两个质数，ln为自然对数，且自然常数e的取值为2.718。

[0075] 该实施例中，分享消息的二进制表示为对员工基于互联列表进行消息分享的分享消息进行二进制转换获得的二进制表示。

[0076] 以上技术的有益效果为：基于进行消息分享的员工的数字身份私钥对分享消息的二进制表示进行加密，实现了消息分享的保密性和安全性，此实施例给出了一种对分享消息的二进制表示进行加密的方法。

[0077] 实施例10：

本发明提供一种基于区块链的员工数字身份管理方法，应用于实施例1至9中任一一种基于区块链的员工数字身份管理装置，参考图2，包括：

S1：对每个人员的身份信息进行身份注册，获得每个员工的数字身份公钥和数字身份私钥；

S2：基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证，获得身

份认证结果,基于身份认证结果对每个员工的好友列表进行添加,获得每个员工的互联列表;

S3:基于每个员工的互联列表对互联双方的消息传输过程进行加密,获得互联传输加密结果;

S4:基于每个员工的互联列表进行消息分享,并对消息分享传输过程进行加密,获得分享传输加密结果。

[0078] 以上技术的有益效果为:基于对每个员工生成分配的数字身份公钥和数字身份私钥更安全、更准确地地对互联双方的消息传输过程和对消息分享传输过程进行加密,实现了员工间信息或数据交流的保密性和安全性。

[0079] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

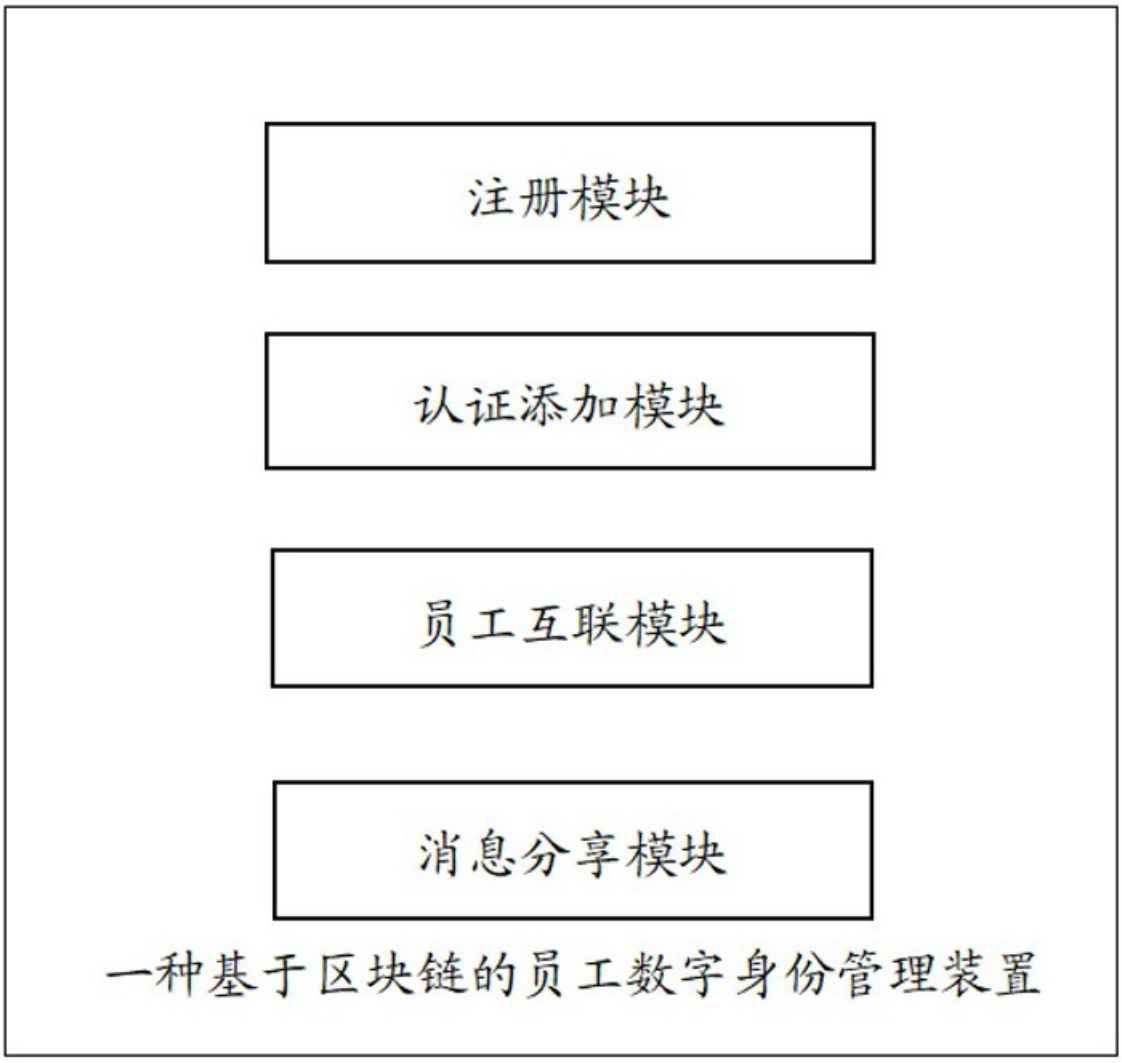


图 1

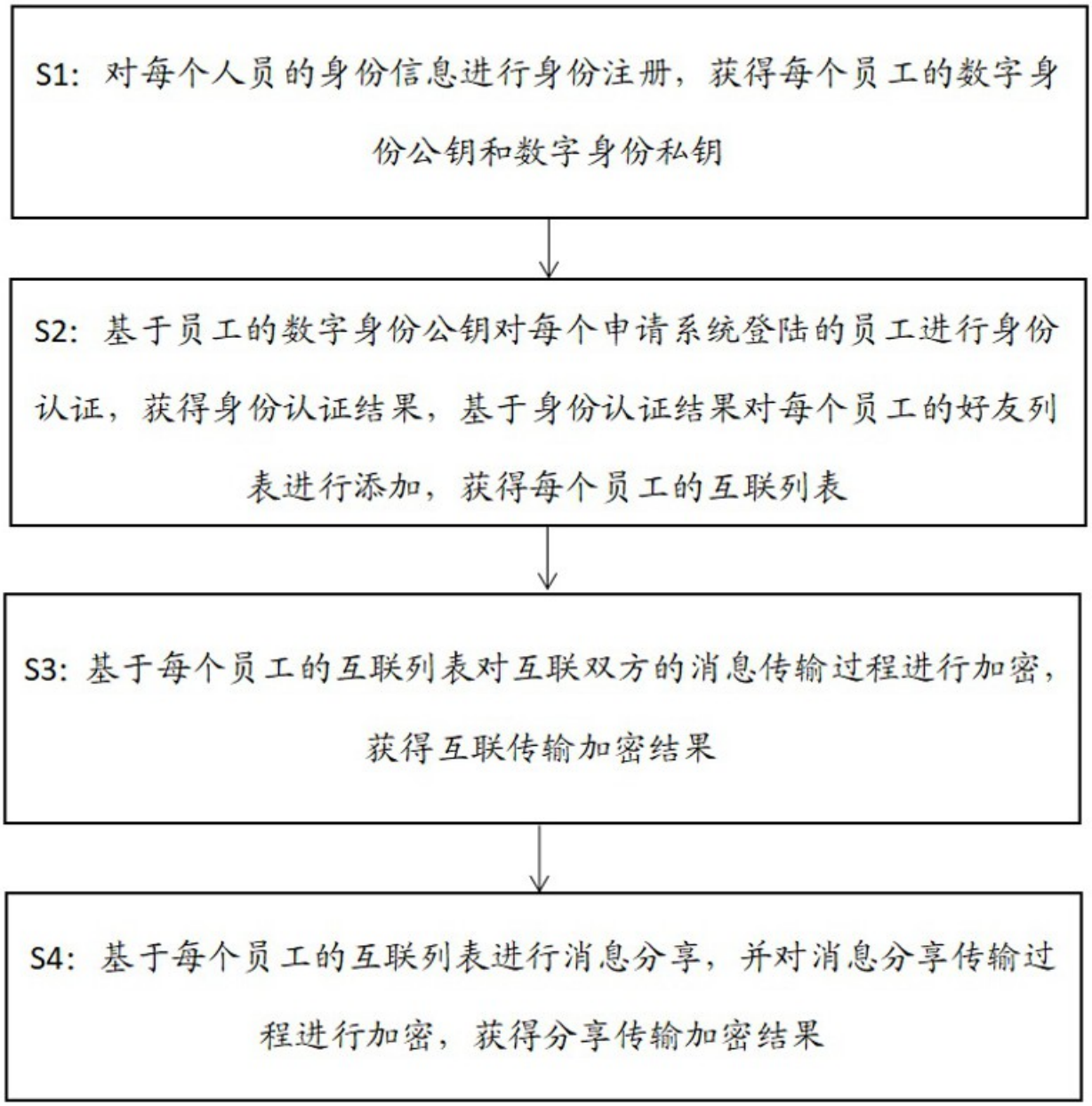

S1：对每个人员的身份信息进行身份注册，获得每个员工的数字身份公钥和数字身份私钥
S2：基于员工的数字身份公钥对每个申请系统登陆的员工进行身份认证，获得身份认证结果，基于身份认证结果对每个员工的好友列表进行添加，获得每个员工的互联列表
S3：基于每个员工的互联列表对互联双方的消息传输过程进行加密，获得互联传输加密结果
S4：基于每个员工的互联列表进行消息分享，并对消息分享传输过程进行加密，获得分享传输加密结果

图 2