(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113468588 B
(45)授权公告日 2021.11.26

(21)申请号 202111035456.8

(22)申请日 2021.09.06

(65)同一申请的已公布的文献号
申请公布号 CN 113468588 A

(43)申请公布日 2021.10.01

(73)专利权人 环球数科集团有限公司
地址 518063 广东省深圳市南山区粤海街道高新南九道10号深圳湾科技生态园10栋B座17层01-03号

(72)发明人 张卫平 丁烨 张浩宇

(74)专利代理机构 北京清控智云知识产权代理事务所(特殊普通合伙) 11919
代理人 马肃

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/31(2013.01)

审查员 赵玉华

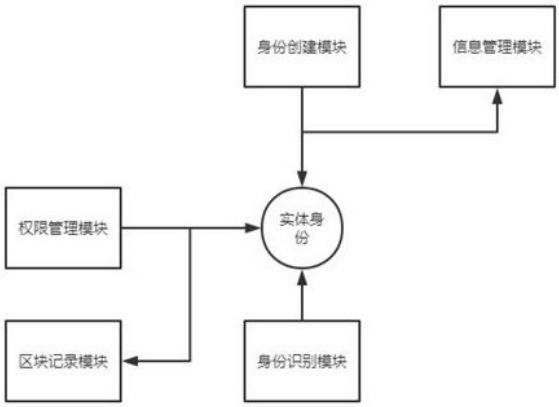
权利要求书1页 说明书6页 附图3页

(54)发明名称

一种基于区块链的身份管理系统

(57)摘要

本发明提供了一种基于区块链的身份管理系统,包括身份创建模块、权限管理模块、身份识别模块、信息管理模块和区块记录模块,所述身份创建模块用于创建实体身份和虚拟身份,所述权限管理模块用于对权限进行管理,所述身份识别模块用于识别实体身份,所述信息管理模块用于记录实体身份与个人信息,所述区块记录模块利用区块链技术对所述实体身份权限变更情况进行记录。本系统将权限、虚拟身份与实体身份单独管理,使得实体身份自主变更权限的难度增加,同时在实体身份变更绑定的虚拟身份设置规则防止所述实体身份自主变更绑定,最后用区块链技术记录实体身份的变更情况,方便追溯问题。



CN 113468588 B

1.一种基于区块链的身份管理系统,其特征在于,包括身份创建模块、权限管理模块、身份识别模块、信息管理模块和区块记录模块,所述身份创建模块用于创建实体身份和虚拟身份,所述权限管理模块用于对权限进行管理,所述身份识别模块用于识别实体身份,所述信息管理模块用于记录实体身份与个人信息,所述区块记录模块利用区块链技术对所述实体身份权限变更情况进行记录;

所述权限管理模块赋予所述虚拟身份不同的权限,所述实体身份通过与对应的虚拟身份绑定获得权限,所述身份识别模块通过识别实体身份获取其拥有的权限进而决定是否开放区域或资料的访问权;

所述实体身份包括三个字段:芯片ID、虚拟ID和变更标记,所述芯片ID为代表所述实体身份的唯一ID,所述虚拟ID为绑定的虚拟身份的ID,所述变更标记用于表示是否绑定临时虚拟身份,所述虚拟ID字段只能存储一个ID,所述变更标记默认情况下为固定值,当所述实体身份绑定的虚拟身份需变动时,所述临时虚拟身份的变更标记为由所述权限管理模块赋予的一段字符串,所述字符串会随赋予时间点的不同而不同;

所述字符串的计算公式为:

$$\begin{cases} Z_i(j)=\left(Z_{i-1}(j+1)+\left|\frac{(t-t')}{j}\right| \bmod 16\right) \bmod 16, 1\le j<n \\ Z_i(j)=\left(Z_{i-1}(1)+\left|\frac{(t-t')}{j}\right| \bmod 16\right) \bmod 16, \ j=n \end{cases};$$

其中,$Z_i(j)$表示第i个字符串的第j个字符对应的值,t为当前时间点,t'为上次赋予字符串的时间点,n为字符串的长度。

2.如权利要求1所述的一种基于区块链的身份管理系统,其特征在于,所述实体身份还包括第四个字段:权限ID,所述权限ID为所述权限管理模块赋予的临时权限,所述临时权限具有时效,当时效耗尽时所述权限ID字段会自动恢复成默认值。

3.如权利要求2所述的一种基于区块链的身份管理系统,其特征在于,所述实体身份获得新权限的方式仅限于变更绑定的虚拟身份和获得临时权限,当所述实体身份获得新权限时,所述区块记录模块会将此操作的具体情况记录在区块链中。

4.如权利要求3所述的一种基于区块链的身份管理系统,其特征在于,所述区块链中的区块内容包括块ID、链接块ID、芯片ID、芯片链块ID和操作内容,所述块ID用于表示本区块的ID,所述链接块ID用于表示上一个区块的ID,所述芯片ID为本区块对应的实体身份的芯片ID,所述芯片链块ID为上一个具有相同芯片ID的区块的块ID。

5.如权利要求4所述的一种基于区块链的身份管理系统,其特征在于,所述系统还包括告警模块,当所述实体身份的权限变化违规时,所述告警模块会发出告警并冻结对应的实体身份。

一种基于区块链的身份管理系统

技术领域

[0001] 本发明涉及管理系统技术领域,尤其涉及一种基于区块链的身份管理系统。

背景技术

[0002] 目前很多组织、团体或公司会采用身份管理系统来管理自己的成员,尤其是涉及机密资料需要对不同的成员设置不同的权限时,具有权限管理的身份管理系统会显得更加重要,但目前的系统大多对成员身份直接赋予对应的权限,使得直接对成员身份的权限进行篡改的可能性大增,不够安全。

[0003] 现在已经开发出了很多身份管理系统,经过我们大量的检索与参考,发现现有的身份管理系统有如公开号为KR101730459B1,KR101195292B1、CN102238148B和KR101620934B1所公开的系统,所述身份管理方法基于标识网实现,终端及身份管理IDP服务器具有表示标识网内身份的身份标识AID,所述终端发起身份服务流程时,所述标识网的接入服务节点ASN利用终端和IDP服务器的AID将终端的身份服务请求发送给所述IDP服务器,所述IDP服务器根据所述身份服务请求实现对所述终端的身份管理。但该系统对不同身份的权限管理不够严密,能够直接对身份所拥有的权限进行修改,使得系统的安全性不够高。

发明内容

[0004] 本发明的目的在于,针对所存在的不足,提出了一种基于区块链的身份管理系统,

[0005] 本发明采用如下技术方案:

[0006] 一种基于区块链的身份管理系统,包括身份创建模块、权限管理模块、身份识别模块、信息管理模块和区块记录模块,所述身份创建模块用于创建实体身份和虚拟身份,所述权限管理模块用于对权限进行管理,所述身份识别模块用于识别实体身份,所述信息管理模块用于记录实体身份与个人信息,所述区块记录模块利用区块链技术对所述实体身份权限变更情况进行记录;

[0007] 所述权限管理模块赋予所述虚拟身份不同的权限,所述实体身份通过与对应的虚拟身份绑定获得权限,所述身份识别模块通过识别实体身份获取其拥有的权限进而决定是否开放区域或资料的访问权;

[0008] 所述实体身份包括三个字段:芯片ID、虚拟ID和变更标记,所述芯片ID为代表所述实体身份的唯一ID,所述虚拟ID为绑定的虚拟身份的ID,所述变更标记用于表示是否绑定临时虚拟身份,所述虚拟ID字段只能存储一个ID,所述变更标记默认情况下为固定值,当所述实体身份绑定的虚拟身份需变动时,所述临时虚拟身份时的变更标记为由所述权限管理模块赋予的一段字符串,所述字符串会随赋予时间点的不同而不同;

[0009] 所述字符串的变化公式为:

[0010] $$\begin{cases} Z_i(j)=\left(Z_{i-1}(j+1)+\left|\frac{(t-t')}{j}\right| \bmod 16\right) \bmod 16, 1\le j<n \\ Z_i(j)=\left(Z_{i-1}(1)+\left|\frac{(t-t')}{j}\right| \bmod 16\right) \bmod 16, \ j=n \end{cases};$$

[0011] 其中，$Z_i(j)$表示第i个字符串的第j个字符对应的值，t为当前时间点，t'为上次赋予字符段的时间点，n为字符串的长度；

[0012] 进一步的，所述实体身份还包括第四个字段：权限ID，所述权限ID为所述权限管理模块赋予的临时权限，所述临时权限具有时效，当时效耗尽时所述权限ID字段会自动恢复成默认值；

[0013] 进一步的，所述实体身份获得新权限的方式仅限于变更绑定的虚拟身份和获得临时权限，当所述实体身份获得新权限时，所述区块记录模块会将此操作的具体情况记录在区块链中；

[0014] 进一步的，所述区块链中的区块内容包括块ID、链接块ID、芯片ID、芯片链块ID和操作内容，所述块ID用于表示本区块的ID，所述链接块ID用于表示上一个区块的ID，所述芯片ID为本区块对应的实体身份的芯片ID，所述芯片链块ID为上一个具有相同芯片ID的区块的块ID；

[0015] 进一步的，所述系统还包括告警模块，当所述实体身份的权限变化违规时，所述告警模块会发出告警并冻结对应的实体身份。

[0016] 本发明所取得的有益效果是：

[0017] 本系统从多个方面对实体身份的权限加强管理，第一，通过增加虚拟身份这个过渡体，使实体身份不直接与权限进行绑定，增加了实体身份改变权限的难度，同时也增大了实体身份自行更改绑定的暴露可能性，第二，在更改虚拟身份的绑定时添加了虚拟临时身份机制，即使知道了需要更改的虚拟身份ID也会因违反机制而触发告警，第三，通过区块链会权限的更改进行记录，更容易对违规授权进行回溯及追责。

附图说明

[0018] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制，而是将重点放在示出实施例的原理上。在不同的视图中，相同的附图标记指定对应的部分。

[0019] 图1为整体结构框架示意图；

[0020] 图2为实体身份、虚拟身份和权限关系示意图；

[0021] 图3为临时虚拟身份作用示意图；

[0022] 图4为实体身份字段示意图；

[0023] 图5为区块链链式结构示意图。

具体实施方式

[0024] 为了使得本发明的目的、技术方案及优点更加清楚明白，以下结合其实施例，对本发明进行进一步详细说明；应当理解，此处所描述的具体实施例仅用于解释本发明，并不用于限定本发明。对于本领域技术人员而言，在查阅以下详细描述之后，本实施例的其它系

统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内，包括在本发明的范围内，并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征，并且这些特征根据以下将详细描述将是显而易见的。

[0025] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或组件必须具有特定的方位，以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制，对于本领域的普通技术人员而言，可以根据具体情况理解上述术语的具体含义。

[0026] 实施例一。

[0027] 结合图1，本实施例提供了一种基于区块链的身份管理系统，包括身份创建模块、权限管理模块、身份识别模块、信息管理模块和区块记录模块，所述身份创建模块用于创建实体身份和虚拟身份，所述权限管理模块用于对权限进行管理，所述身份识别模块用于识别实体身份，所述信息管理模块用于记录实体身份与个人信息，所述区块记录模块利用区块链技术对所述实体身份权限变更情况进行记录；

[0028] 所述权限管理模块赋予所述虚拟身份不同的权限，所述实体身份通过与对应的虚拟身份绑定获得权限，所述身份识别模块通过识别实体身份获取其拥有的权限进而决定是否开放区域或资料的访问权；

[0029] 所述实体身份包括三个字段：芯片ID、虚拟ID和变更标记，所述芯片ID为代表所述实体身份的唯一ID，所述虚拟ID为绑定的虚拟身份的ID，所述变更标记用于表示是否绑定临时虚拟身份，所述虚拟ID字段只能存储一个ID，所述变更标记默认情况下为固定值，当所述实体身份绑定的虚拟身份需变动时，所述临时虚拟身份时的变更标记为由所述权限管理模块赋予的一段字符串，所述字符串会随赋予时间点的不同而不同；

[0030] 所述字符串的变化公式为：

[0031] $$\begin{cases} Z_i(j)=\left(Z_{i-1}(j+1)+\left|\frac{(t-t')}{j}\right| \bmod 16 \right) \bmod 16, 1\le j<n \\ Z_i(j)=\left(Z_{i-1}(1)+\left|\frac{(t-t')}{j}\right| \bmod 16 \right) \bmod 16, \ j=n \end{cases} ;$$

[0032] 其中，$Z_i(j)$表示第i个字符串的第j个字符对应的值，t为当前时间点，t’为上次赋予字符段的时间点，n为字符串的长度；

[0033] 所述实体身份还包括第四个字段：权限ID，所述权限ID为所述权限管理模块赋予的临时权限，所述临时权限具有时效，当时效耗尽时所述权限ID字段会自动恢复成默认值；

[0034] 所述实体身份获得新权限的方式仅限于变更绑定的虚拟身份和获得临时权限，当所述实体身份获得新权限时，所述区块记录模块会将此操作的具体情况记录在区块链中；

[0035] 所述区块链中的区块内容包括块ID、链接块ID、芯片ID、芯片链块ID和操作内容，所述块ID用于表示本区块的ID，所述链接块ID用于表示上一个区块的ID，所述芯片ID为本区块对应的实体身份的芯片ID，所述芯片链块ID为上一个具有相同芯片ID的区块的块ID；

[0036] 所述系统还包括告警模块，当所述实体身份的权限变化违规时，所述告警模块会

发出告警并冻结对应的实体身份。

[0037] 实施例二。

[0038] 本实施例包含了实施例一的全部内容，结合图2，本实施例的所述身份创建模块用于创建实体身份和虚拟身份，所述实体身份包括一个身份终端，所述身份终端内包含具有唯一ID的芯片，所述身份终端与个人绑定，个人信息与对应的芯片ID被记录在信息管理模块中，所述虚拟身份为拥有不同权限的虚拟个人，所述实体身份需绑定所述虚拟身份后获得相应的权限，多个实体身份能够绑定到同一个虚拟身份，一个实体身份在一个时间点至多且至少绑定一个虚拟身份；

[0039] 所述权限管理模块用于给所述虚拟身份赋予权限，所有虚拟身份拥有不同的权限，所述权限管理模块还能够给所述实体身份赋予临时权限；

[0040] 所述身份识别模块用于识别所述身份终端的芯片ID，从而获得所述实体身份拥有的权限，并根据拥有的权限决定是否开放访问；

[0041] 所述区块记录模块用于记录所述实体身份的权限变化，所述变化包括实体身份绑定的虚拟身份的变化以及实体身份的临时权限的变化；

[0042] 所述虚拟身份包括一个最高虚拟身份，所述最高虚拟身份拥有所有权限，所述最高虚拟身份在系统刚开始工作时由所述身份创建模块自动创建；

[0043] 结合图3，所述虚拟身份包括一个临时虚拟身份，所述临时虚拟身份的特别之处在于一个实体身份可以同时绑定一个临时虚拟身份和一个其它虚拟身份，所述临时虚拟身份不拥有任何权限，其作用在于当要更改一个实体身份绑定的虚拟身份时，需将所述实体身份先绑定临时虚拟身份，解绑所述实体身份绑定的原有虚拟身份，再将新的虚拟身份与所述实体身份绑定，最后解绑临时虚拟身份；

[0044] 当所述实体身份在一个时间点内未绑定任何虚拟身份或绑定超过一个非临时虚拟身份的虚拟身份时，所述系统会产生身份告警；

[0045] 所述虚拟身份中拥有最少权限的为基础虚拟身份，新创建的实体身份直接绑定所述基础虚拟权限，除了所述基础虚拟身份和临时虚拟身份外的其余虚拟身份拥有权限管理模块的操作权限；

[0046] 所述实体身份与所述虚拟身份的绑定或解绑由另一个拥有权限管理模块操作权限的实体身份对所述权限管理模块进行操作而实现，但操作所述权限管理模块能够解绑和绑定的虚拟身份会根据操作者自身拥有的权限而有所不同；

[0047] 拥有身份创建模块操作权限的实体身份能够通过身份创建模块创建或注销一个实体身份，当创建一个实体身份时，会在所述信息管理模块内申请一块存储区域用于保存个人信息以及芯片ID，当销毁一个实体身份时，所述信息管理模块内对应的存储区域会删除保存的内容；

[0048] 当需要访问资料或进入特定区域时，需要所述身份识别模块对身份终端进行识别并确认是否有资格访问或进入，所述身份识别模块会读取所述身份终端的芯片ID，根据所述芯片ID搜索到其绑定的虚拟身份，再搜索所述虚拟身份被赋予的权限中是否有需要的权限，若有，则允许其继续访问资料或进入区域，若无，则禁止其访问或进入，若所述实体身份被赋予临时权限，则所述身份识别模块会先确认临时权限是否为对应的权限，再搜索虚拟身份被赋予的权限；

[0049] 所述权限管理模块能够给所述实体身份赋予临时权限，所述临时权限存在时限和/或次限，当所述临时权限存在时限时，从被赋予临时权限的时间算起，到达时限后所述临时权限自动取消，当所述临时权限存在次限时，当被所述身份识别模块检测并使用所述临时权限访问资料或进入区域后，次数减一，当次数减为零后所述临时权限自动取消，当所述临时权限同时存在时限和次限时，其中一个限制耗尽时所述临时权限自动取消；

[0050] 所述实体身份、虚拟身份和权限通过下述方式进行绑定或关联：

[0051] 结合图4，所述实体身份包括四个字段：芯片ID、虚拟ID、变更标记和权限ID，所述芯片ID为对应的身份终端内的芯片ID，所述虚拟ID为绑定的虚拟身份的ID，所述变更标记用于表示是否绑定临时虚拟身份，所述权限ID为被授予的临时权限的ID，需要注意的是，所述虚拟ID字段只能存储一个ID，所述权限ID字段只能存储一个ID和限制内容，所述变更标记为1时表示绑定了临时虚拟身份，所述变更标记为0时表示未绑定临时虚拟身份，为了提高身份的安全性和可靠性，当绑定临时虚拟身份时的变更标记为由所述权限管理模块赋予的一段字符串，所述字符串会随赋予时间点的不同而不同；

[0052] 所述虚拟身份包括两个字段：虚拟ID和权限ID，所述虚拟ID为本虚拟身份的ID，具有唯一性，所述权限ID字段用于保存所述虚拟身份被赋予的权限的ID，所述虚拟身份的虚拟ID和权限ID自所述虚拟身份被创建时起便不可变更；

[0053] 所述权限包括两个字段：权限ID和注释，所述权限ID为本权限的ID，具有唯一性，所述注释字段中记载了需要用到本权限的场所；

[0054] 所述实体身份被保存在实体身份库中，所述虚拟身份被保存在虚拟身份库中，所述权限被保存在权限库中；

[0055] 所述字符串的变化公式为：

[0056]
$$\begin{cases} Z_i(j)=\left(Z_{i-1}(j+1)+\left|\dfrac{(t-t')}{j}\right| \bmod 16\right) \bmod 16, 1\le j<n \\ Z_i(j)=\left(Z_{i-1}(1)+\left|\dfrac{(t-t')}{j}\right| \bmod 16\right) \bmod 16, \ j=n \end{cases}$$ ；

[0057] 其中，$Z_i(j)$表示第i个字符串的第j个字符对应的值，t为当前时间点，t’为上次赋予字符段的时间点，n为字符串的长度；

[0058] 所述字符串由数字0-9、字母A至F构成，字母A至F对应的值为10至15；

[0059] 所述字符串的下标i达到上限后从0开始重新计数；

[0060] 所述实体身份在创建、变更绑定的虚拟身份、赋予临时权限以及注销时会在区块记录模块中生成一个区块并加入到区块链中，由于所述实体身份的上述操作并不频繁，所以一个区块中只记录一个实体身份的上述一个操作，使得区块链具有高时效性；

[0061] 结合图5，所述区块中包括块ID、链接块ID、芯片ID、芯片链块ID和操作内容，所述块ID用于表示本区块的ID，所述链接块ID用于表示上一个区块的ID，通过所述块ID和所述链接块ID将所有的区块连接成一个区块链，所述芯片ID为本区块对应的实体身份的芯片ID，所述芯片链块ID为上一个具有相同芯片ID的区块的块ID，通过所述芯片ID和所述芯片链块ID能够在所述区块链中快速地找出某一实体身份相关的所有区块，所述操作内容包括本区块对应的实体身份的具体变化情况以及操作人的实体身份；

[0062] 当所述区块中的操作内容为赋予临时权限时，所述区块记录模块会生成一份简易报告，所述简易报告会发送给操作人的实体身份关联的邮箱中；

[0063] 当所述身份识别模块检到并需要使用临时权限时，所述身份识别模块会向所述区块记录模块中查找是否存在相应的区块记录，若不存在，所述系统会产生告警。

[0064] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所描述的顺序不同的顺序执行方法，和/或可以添加，省略和/或组合各种部件。而且，关于某些配置描述的特征可以以各种其他配置组合，如可以以类似的方式组合配置的不同方面和元素。此外，随着技术发展其中的元素可以更新，即许多元素是示例，并不限制本公开或权利要求的范围。

[0065] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而，可以在没有这些具体细节的情况下实践配置例如，已经示出了众所周知的电路，过程，算法，结构和技术而没有不必要的细节，以避免模糊配置。该描述仅提供示例配置，并且不限制权利要求的范围，适用性或配置。相反，前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下，可以对元件的功能和布置进行各种改变。

[0066] 综上，其旨在上述详细描述被认为是例示性的而非限制性的，并且应当理解，以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

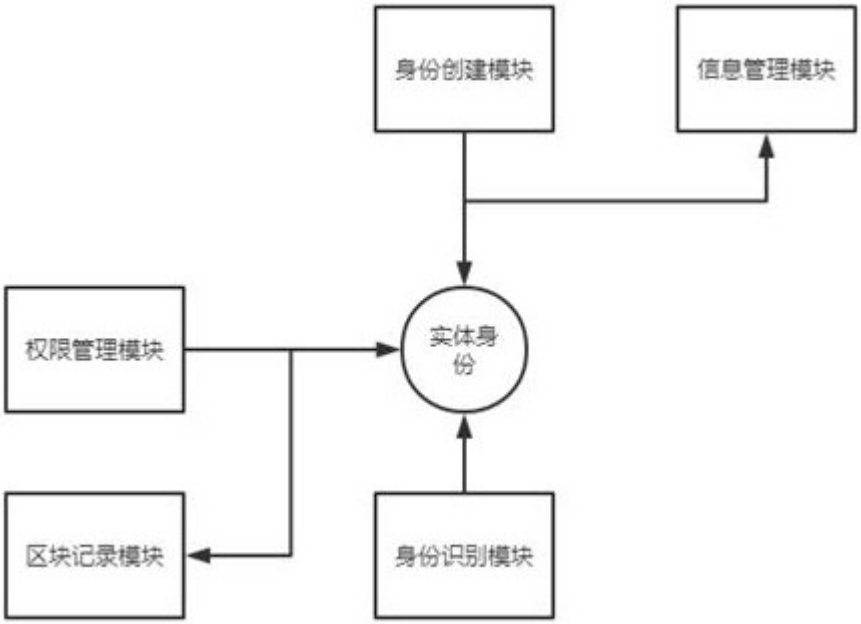


图1

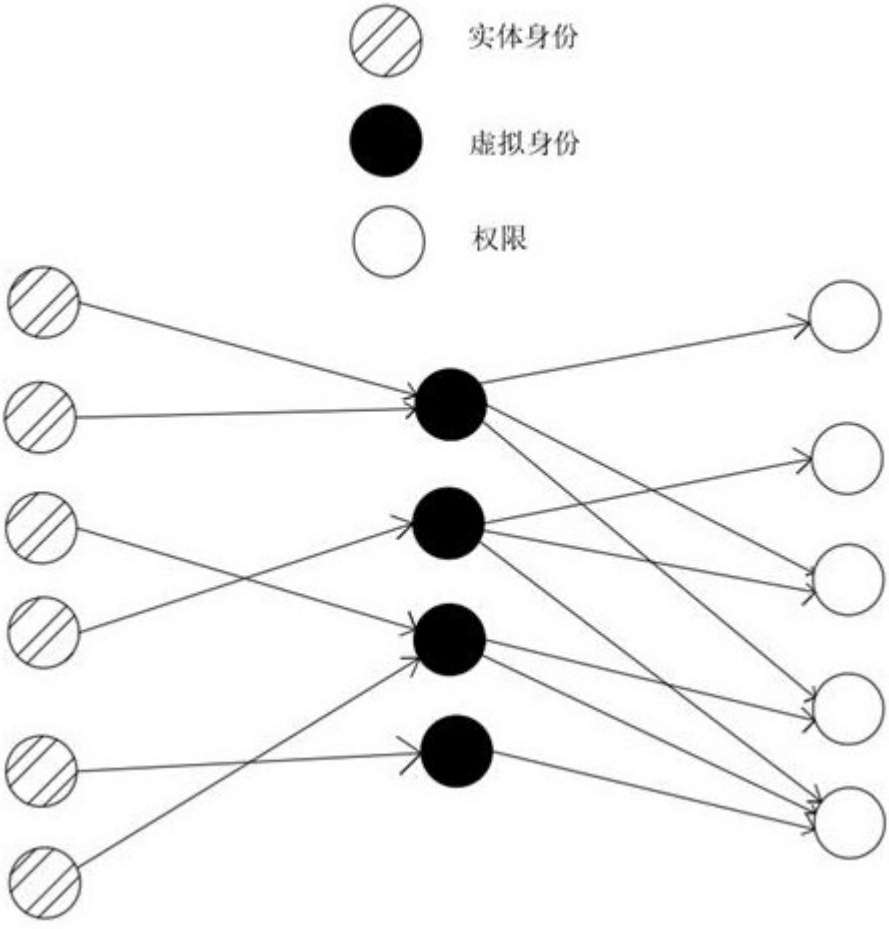


图2

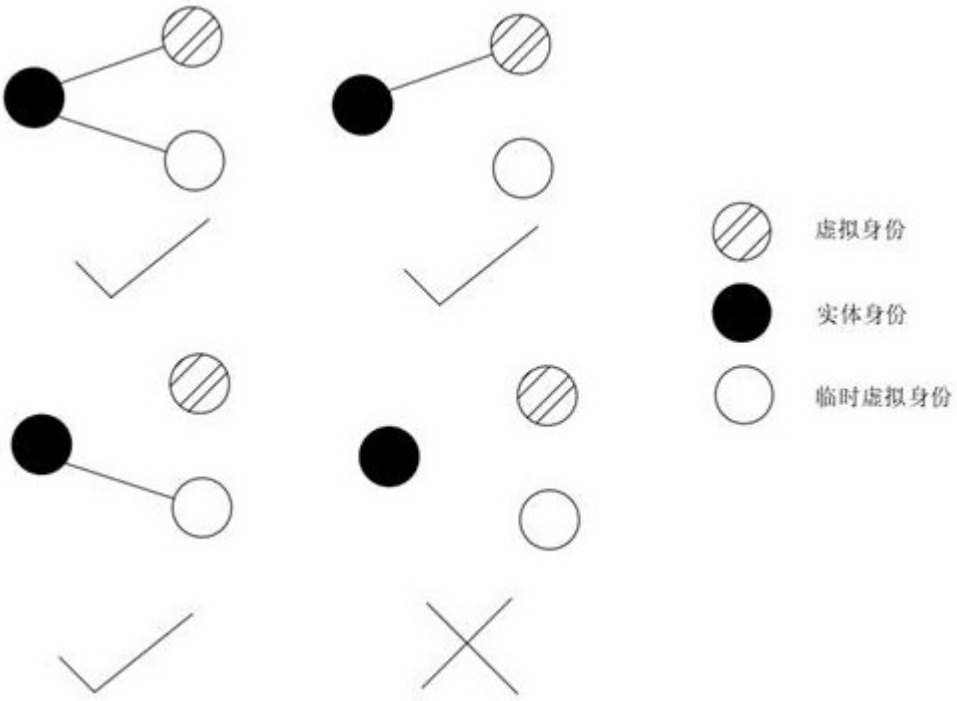


图3

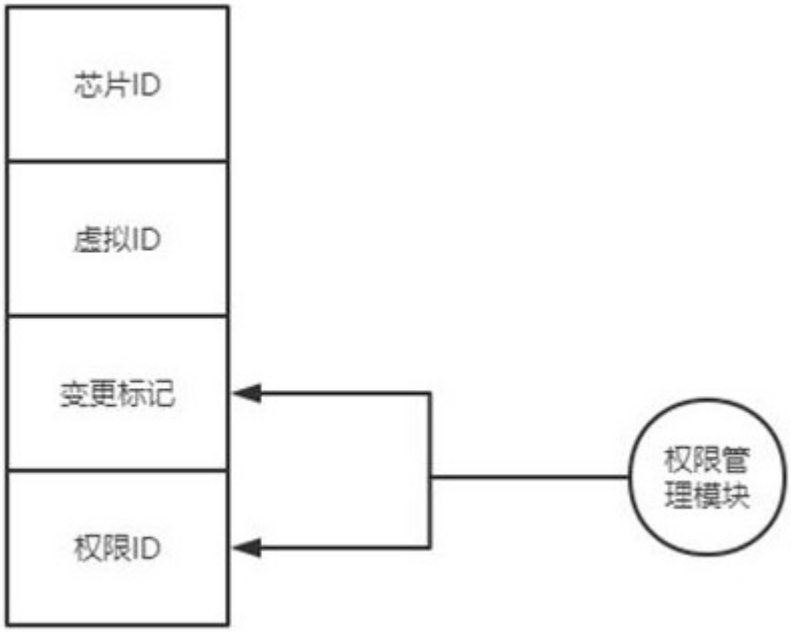


图4

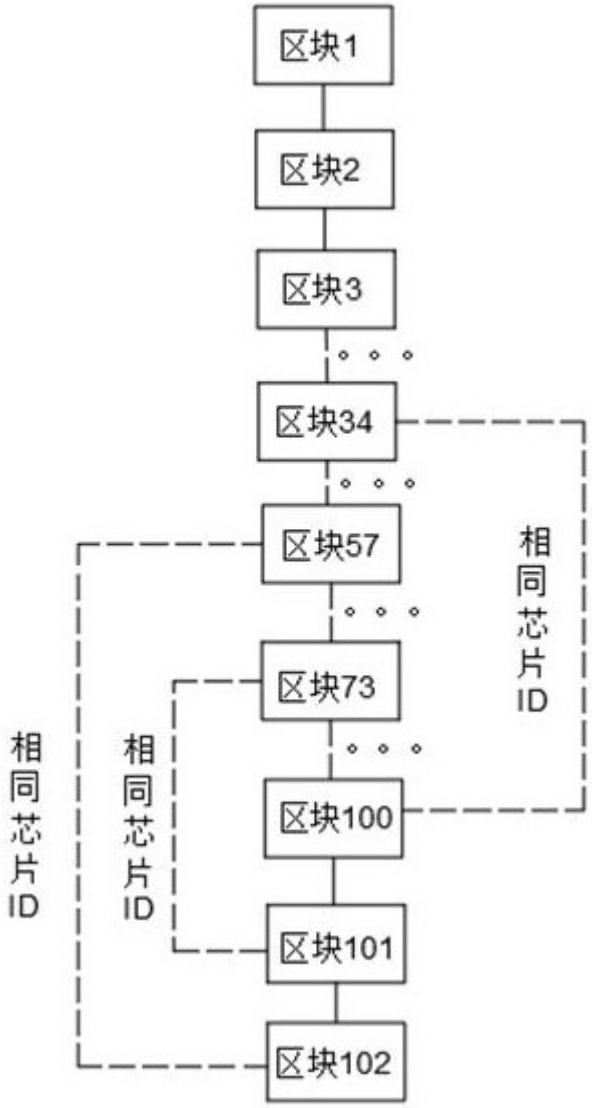

区块1
区块2
区块3
区块34
区块57
区块73
区块100
区块101
区块102
相同芯片ID
相同芯片ID
相同芯片ID

图5