(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113139209 B
(45)授权公告日 2023.09.26

(21)申请号 202110404903.6
(22)申请日 2021.04.15
(65)同一申请的已公布的文献号
申请公布号 CN 113139209 A
(43)申请公布日 2021.07.20
(73)专利权人 中国科学院软件研究所
地址 100190 北京市海淀区中关村南四街4号
(72)发明人 曾靖 蒋步云 李春晓 张亚丰 郑龙帅 李玉成 梁赓
(74)专利代理机构 北京君尚知识产权代理有限公司 11200
专利代理师 邱晓锋
(51)Int.Cl.
G06F 21/64(2013.01)
G06F 21/62(2013.01)
(56)对比文件
CN 111901106 A,2020.11.06
CN 112636930 A,2021.04.09
CN 112035883 A,2020.12.04
CN 110049066 A,2019.07.23
CN 111680324 A,2020.09.18
CN 110555772 A,2019.12.10
CN 109902508 A,2019.06.18
CN 106533681 A,2017.03.22
CN 112311538 A,2021.02.02
US 2017033934 A1,2017.02.02
闫建华.格基签密关键技术研究.《中国博士学位论文全文数据库 信息科技辑》.2016,(第03期),I136-105.
Nan Guo 等.Aggregate Signature-Based Efficient Attributes Proof with Pairing-Based Anonymous Credential.《2013 16th International Conference on Network-Based Information Systems》.2013,第276-281页.
审查员 周杨

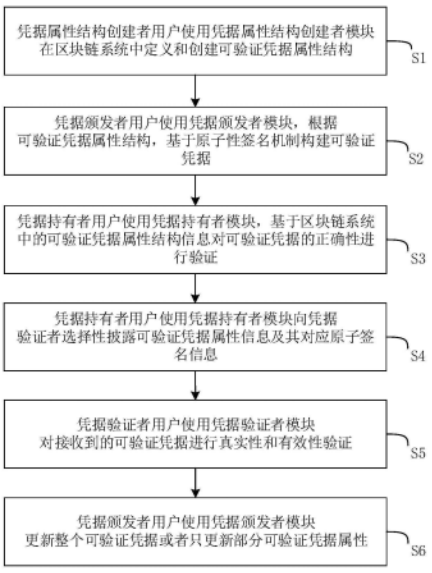
权利要求书3页 说明书7页 附图5页

(54)发明名称

一种基于原子性签名的可验证凭据实现方法和系统

(57)摘要

本发明提供了一种基于原子性签名的可验证凭据实现方法和系统。所述方法包括:凭据属性结构创建者定义和创建可验证凭据属性结构;凭据颁发者根据可验证凭据属性结构,基于原子性签名机制构建可验证凭据;凭据持有者对可验证凭据的正确性进行验证;凭据持有者向凭据验证者选择性披露可验证凭据属性信息及其对应原子签名信息;凭据验证者对接收到的可验证凭据进行真实性和有效性验证;凭据颁发者更新整个可验证凭据或者只更新部分可验证凭据属性。基于本发明实现的可验证凭据方案,在支持更方便和更安全地选择性披露信息之外,还能更灵活高效地更新可验证凭据属性。



CN 113139209 B

1.一种基于原子性签名的可验证凭据实现方法,其特征在于,包括以下步骤:

凭据属性结构创建者定义和创建可验证凭据属性结构,并且将可验证凭据属性结构信息记录于数据系统中;

凭据颁发者根据可验证凭据属性结构信息,基于原子性签名机制构建含若干原子签名信息的完整可验证凭据;

凭据持有者从完整可验证凭据中选择待披露的若干属性信息及其对应的原子签名信息,形成可验证凭据出示信息,提交给凭据验证者;

凭据验证者对接收到的可验证凭据出示信息进行真实性和有效性验证;

所述凭据颁发者根据可验证凭据属性结构信息,基于原子性签名机制构建含若干原子签名信息的完整可验证凭据,包括:

获取数据系统中记录的可验证凭据属性结构信息,填写可验证凭据元数据以及相应属性的属性值;

对每个可验证凭据属性进行唯一编号;

基于原子性签名机制,针对每个可验证凭据属性生成各自对应的原子签名信息;

构建完整可验证凭据;

在数据系统中初始化完整可验证凭据的状态信息以及各可验证凭据属性的状态信息;

所述原子性签名机制是指对于每一个可验证凭据属性及其编号,凭据颁发者使用基于非对称密钥的数字签名算法,单独对其与可验证凭据元数据所组成的信息进行签名以生成原子签名信息,原子签名信息的生成与当前可验证凭据属性之外的其他任何可验证凭据属性均无关;

所述凭据验证者对接收到的可验证凭据出示信息进行真实性和有效性验证,包括:

(1):根据可验证凭据元数据中的凭据有效期起始时间以及凭据有效期终止时间,验证可验证凭据当前是否处于有效期内,若未处于,则不进行后续操作;否则,执行步骤(2);

(2):向数据系统获取可验证凭据的状态信息,验证是否符合要求,若不符合,则不进行后续步骤;若符合,则执行步骤(3);

(3):向数据系统获取可验证凭据中每个可验证凭据属性的状态信息,验证是否都有效,若存在无效的可验证凭据属性,则不进行后续步骤;若都有效,则执行步骤(4);

(4):根据可验证凭据中的签名算法以及验签公钥信息,对每一个被披露出来的可验证凭据属性及其对应原子签名进行基于非对称密钥的数字验签操作,若每个验签操作均正确,则通过对可验证凭据的验证,否则不通过。

2.根据权利要求1所述的基于原子性签名的可验证凭据实现方法,其特征在于:所述数据系统是中心化的数据服务系统,或者是去中心化的区块链系统。

3.根据权利要求1所述的基于原子性签名的可验证凭据实现方法,其特征在于:所述可验证凭据属性结构信息包含:凭据属性结构唯一标识、凭据类型名称、凭据属性结构版本、凭据属性结构的描述说明、凭据属性结构创建者身份标识、凭据属性结构创建时间以及凭据属性集合;所述凭据属性集合的每个元素包含:属性名称、属性值的类型以及属性描述说明。

4.根据权利要求1所述的基于原子性签名的可验证凭据实现方法,其特征在于:所述可验证凭据元数据包含:凭据唯一标识、凭据类型、凭据属性结构唯一标识、凭据颁发者身份

标识、凭据颁发时间、凭据有效期起始时间以及凭据有效期终止时间;所述唯一编号是指在一个完整可验证凭据的构成范围内,对每个可验证凭据属性的编号是唯一的,即在该完整可验证凭据内可验证凭据属性的编号两两不同。

5.根据权利要求1所述的基于原子性签名的可验证凭据实现方法,其特征在于:所述完整可验证凭据包含:可验证凭据元数据、可验证凭据属性信息以及可验证凭据签名信息;所述可验证凭据属性信息,包含若干可验证凭据属性及其对应属性编号;所述可验证凭据签名信息包含:签名信息元数据、若干原子签名信息以及对应属性编号;所述签名信息元数据包含:签名算法、签名时间以及验签公钥信息,所述验签公钥信息是公钥本身或者公钥的标识;

所述完整可验证凭据的状态信息包含:可验证凭据唯一标识以及可验证凭据状态值,所述可验证凭据状态值为满足不同需要的状态表示信息;所述可验证凭据属性的状态信息包含:可验证凭据唯一标识、可验证凭据属性编号以及可验证凭据属性状态值,所述可验证凭据属性状态值,为表示该可验证凭据属性有效或无效的状态信息。

6.根据权利要求1所述的基于原子性签名的可验证凭据实现方法,其特征在于:在所述凭据颁发者根据可验证凭据属性结构信息,基于原子性签名机制构建含若干原子签名信息的完整可验证凭据之后,增加以下步骤:

凭据持有者获取构建的完整可验证凭据,并从数据系统中获取可验证凭据属性结构信息,验证完整可验证凭据中的属性信息是否符合可验证凭据属性结构信息的定义,若不符合,则判定该完整可验证凭据不正确,不进行后续步骤;若符合,则再验证完整可验证凭据中的签名信息是否正确。

7.根据权利要求1所述的基于原子性签名的可验证凭据实现方法,其特征在于:凭据颁发者基于撤销原凭据再签发完整新凭据的方式更新完整可验证凭据,或者只更新部分可验证凭据属性;所述只更新部分可验证凭据属性的步骤包括:

根据可验证凭据的唯一标识以及待被更新的可验证凭据属性的原始编号,向数据系统提交请求,将待被更新的可验证凭据属性的状态置为无效;

为待被更新的可验凭据属性填写新的属性值,并且赋予新的唯一编号;

基于原子性签名机制产生新的原子签名信息,并将新的可验证凭据属性、新的可验证凭据属性编号以及新的原子签名信息提交给凭据持有者;

根据可验证凭据的唯一标识以及已被更新的可验证凭据属性的新编号向数据系统提交请求,将具有新编号的可验证凭据属性的状态初始化为有效。

8.一种采用权利要求1～7中任一权利要求所述方法的基于原子性签名的可验证凭据实现系统,其特征在于,包括数据系统模块、凭据属性结构创建者模块、凭据颁发者模块、凭据持有者模块以及凭据验证者模块;

所述凭据属性结构创建者模块,用于定义和创建可验证凭据属性结构,并且将可验证凭据属性结构信息记录于数据系统模块中;

所述凭据颁发者模块,用于签发完整的可验证凭据以及更新可验证凭据属性;

所述凭据持有者模块,用于管理和验证接收到的可验证凭据的正确性,以及按照凭据验证者的需要选择性披露可验证凭据属性信息以出示提交给凭据验证者;

所述凭据验证者模块,用于验证凭据持有者出示提交的可验证凭据信息的真实性及有

效性；

所述数据系统模块，用于为其它模块提供可信数据访问服务，包括可验证凭据属性结构信息的记录及查询，可验证凭据及可验证凭据属性状态信息的记录及查询。

9.一种电子装置，其特征在于，包括存储器和处理器，所述存储器存储计算机程序，所述计算机程序被配置为由所述处理器执行，所述计算机程序包括用于执行权利要求1～7中任一权利要求所述方法的指令。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储计算机程序，所述计算机程序被计算机执行时，实现权利要求1～7中任一权利要求所述的方法。

一种基于原子性签名的可验证凭据实现方法和系统

技术领域

[0001] 本发明涉及计算机技术领域，具体涉及一种基于原子性签名的可验证凭据实现方法和系统。

背景技术

[0002] 在现实世界的日常生活中，我们需要用到各种凭据以及证件，可验证凭据(Verifiable Credentials)提供了一种对实体凭据及证件进行数字化表示和使用的方案，该方案兼具密码学安全、隐私保护及机器可验证的特点，以支持凭据在数字世界中能被更方便和更安全地使用。相较于传统的实体凭据，可验证凭据以数字化方式呈现，更便于保存和传输，并且基于密码学机制，能更安全可靠地验证其真实性。

[0003] 在实现可验证凭据时，需要能够支持选择性披露可验证凭据属性信息以保护用户隐私，已有的可验证凭据实现方法通常基于Camenisch-Lysyanskaya(CL)签名机制或者披露隐私属性哈希值机制。基于CL签名机制的实现方法通常计算过程较为复杂，更适用于有强匿名性需求的场景。而基于披露隐私属性哈希值的实现方法，针对待披露的属性提供明文信息，对隐私属性只提供其密码学哈希值，但该方法受到被暴力破解及彩虹表攻击的威胁，因此有泄露隐私信息的隐患。此外，在需要更新可验证凭据的部分属性时，现有方法都需要通过先撤销原凭据再签发完整新凭据的方式来实现，比较低效。

[0004] 因此，如何兼顾可验证凭据实现方法的实现简单性、选择性披露属性时的安全性以及更新可验证凭据属性时的灵活高效性是一个亟待解决的问题。

发明内容

[0005] 本发明解决的技术问题：针对现有方法的不足，提供一种基于原子性签名的可验证凭据实现方法，以兼顾实现简单性、选择性披露信息时的安全性以及更新可验证凭据属性时的灵活高效性。

[0006] 本发明采用的技术方案：

[0007] 一种基于原子性签名的可验证凭据实现方法，包括以下步骤：

[0008] 凭据属性结构创建者定义和创建可验证凭据属性结构，并且将可验证凭据属性结构信息记录于数据系统中；

[0009] 凭据颁发者根据可验证凭据属性结构信息，基于原子性签名机制构建含若干原子签名信息的完整可验证凭据；

[0010] 凭据持有者从完整可验证凭据中选择待披露的若干属性信息及其对应的原子签名信息，形成可验证凭据出示信息，提交给凭据验证者；

[0011] 凭据验证者对接收到的可验证凭据出示信息进行真实性和有效性验证。

[0012] 进一步地，上述方法具体包括以下步骤，其中步骤S3、步骤S6可被省略。

[0013] 步骤S1：凭据属性结构创建者对特定类型的可验证凭据属性结构进行定义，并且将可验证凭据属性结构信息(不妨记为CCS)记录于数据系统中，所述可验证凭据属性是指

在可验证凭据中用以描述对象实体的声明信息(Claims),所述可验证凭据属性结构即是指上述声明信息的数据结构,所述对象实体可以是人、物或组织等;

[0014] 步骤S2:凭据颁发者根据步骤S1中创建的可验证凭据属性结构信息CCS,并基于原子性签名机制,构建含若干原子签名信息的完整可验证凭据,不妨记为VC;

[0015] 步骤S3:凭据持有者获取步骤S2构建的完整可验证凭据VC,并从数据系统中获取可验证凭据属性结构信息CCS,验证VC中的属性信息是否符合CCS的定义,若不符合,则判定该VC不正确,不进行后续步骤;若符合,则再验证VC中的签名信息是否正确;

[0016] 步骤S4:凭据持有者从可验证凭据VC中选择待披露的若干属性信息及其对应的原子签名信息,将上述被选择披露的可验证凭据属性信息和对应原子签名信息进行封装,形成可验证凭据出示信息,不妨记为VCP,提交给凭据验证者;

[0017] 步骤S5:对于从步骤S4中接收到的可验证凭据出示信息VCP,凭据验证者验证VCP提交者的签名,若签名不正确,则判定VCP无效;若签名正确,则继续对VCP所封装的可验证凭据进行验证;

[0018] 步骤S6:根据具体需要,凭据颁发者可基于撤销原凭据再签发完整新凭据的方式更新完整可验证凭据,或者只更新部分可验证凭据属性。

[0019] 上述步骤中,所述数据系统可以是中心化的数据服务系统,也可以是去中心化的区块链系统。

[0020] 所述步骤S1中,所述可验证凭据属性结构信息CCS包含:凭据属性结构唯一标识、凭据类型名称、凭据属性结构版本、凭据属性结构的描述说明、凭据属性结构创建者身份标识、凭据属性结构创建时间以及凭据属性集合,所述凭据属性集合的每个元素包含信息:属性名称、属性值的类型以及属性描述说明。

[0021] 所述步骤S2具体实现如下:

[0022] (2.1):获取数据系统中记录的可验证凭据属性结构信息CCS,填写可验证凭据元数据(不妨记为M)以及相应属性的属性值;

[0023] (2.2):对每个可验证凭据属性进行唯一编号;

[0024] (2.3):基于原子性签名机制,针对每个可验证凭据属性生成各自对应的原子签名信息;

[0025] (2.4):构建完整的可验证凭据VC;

[0026] (2.5):在数据系统中初始化可验证凭据VC的状态信息以及各可验证凭据属性的状态信息。

[0027] 所述步骤(2.1)中,所述可验证凭据元数据M包含:凭据唯一标识、凭据类型、凭据属性结构唯一标识、凭据颁发者身份标识、凭据颁发时间、凭据有效期起始时间以及凭据有效期终止时间。

[0028] 所述步骤(2.2)中,所述唯一编号是指在一个可验证凭据VC的构成范围内,对每个可验证凭据属性的编号是唯一的,即在该可验证凭据VC内可验证凭据属性的编号两两不同。

[0029] 所述步骤(2.3)中,所述原子性签名机制是指对于每一个可验证凭据属性及其编号,凭据颁发者使用基于非对称密钥的数字签名算法,单独对其与可验证凭据元数据M所组成的信息进行签名以生成原子签名信息,原子签名信息的生成与当前可验证凭据属性之外

的其他任何可验证凭据属性均无关。

[0030] 所述步骤(2.4)中,所述完整的可验证凭据VC包含:可验证凭据元数据、可验证凭据属性信息以及可验证凭据签名信息。所述可验证凭据属性信息,包含若干可验证凭据属性及其对应属性编号;所述可验证凭据签名信息包含:签名信息元数据、若干原子签名信息以及对应属性编号,所述签名信息元数据包含:签名算法、签名时间以及验签公钥信息,所述验签公钥信息可以是公钥本身或者公钥的标识。

[0031] 所述步骤(2.5)中,所述可验证凭据VC的状态信息包含:可验证凭据唯一标识以及可验证凭据状态值,所述可验证凭据状态值,可为满足不同需要的状态表示信息,如有效、已冻结或已撤销等;所述可验证凭据属性的状态信息包含:可验证凭据唯一标识、可验证凭据属性编号以及可验证凭据属性状态值,所述可验证凭据属性状态值,可为表示该可验证凭据属性有效或无效的状态信息。

[0032] 所述步骤S4中,所述可验证凭据出示信息VCP包含:可验证凭据出示元数据、可验证凭据信息以及可验证凭据出示签名,所述可验证凭据出示元数据包含:凭据出示唯一标识、凭据出示类型以及凭据持有者身份标识,所述可验证凭据信息可以是单个或多个完整的可验证凭据,也可以是单个或多个被选择性披露信息的非完整可验证凭据。

[0033] 所述步骤S5中,所述对可验证凭据出示VCP所封装的可验证凭据进行验证的具体实现如下:

[0034] (5.1):根据可验证凭据元数据中的凭据有效期起始时间以及凭据有效期终止时间,验证可验证凭据当前是否处于有效期内,若未处于,则不进行后续操作;若处于,则执行步骤(5.2);

[0035] (5.2):向数据系统获取可验证凭据的状态信息,验证是否符合要求,若不符合,则不进行后续步骤;若符合,则执行步骤(5.3);

[0036] (5.3):向数据系统获取可验证凭据中每个可验证凭据属性的状态信息,验证是否都有效,若存在无效的可验证凭据属性,则不进行后续步骤;若都有效,则执行步骤(5.4);

[0037] (5.4):根据可验证凭据中的签名算法以及验签公钥信息,对每一个被披露出来的可验证凭据属性及其对应原子签名进行基于非对称密钥的数字验签操作。若每个验签操作均正确,则通过对可验证凭据的验证,否则不通过。

[0038] 所述步骤S6中,所述只更新部分可验证凭据属性的具体实现如下:

[0039] (6.1):根据可验证凭据的唯一标识以及待被更新的可验证凭据属性的原始编号,向数据系统提交请求,将待被更新的可验证凭据属性的状态置为无效;

[0040] (6.2):为待被更新的可验凭据属性填写新的属性值,并且赋予新的唯一编号;

[0041] (6.3):基于原子性签名机制产生新的原子签名信息,并将新的可验证凭据属性、新的可验证凭据属性编号以及新的原子签名信息提交给凭据持有者;

[0042] (6.4):根据可验证凭据的唯一标识以及已被更新的可验证凭据属性的新编号向数据系统提交请求,将具有新编号的可验证凭据属性的状态初始化为有效。

[0043] 基于同一发明构思,本发明还提供一种采用上述方法的基于原子性签名的可验证凭据实现系统,其包括数据系统模块、凭据属性结构创建者模块、凭据颁发者模块、凭据持有者模块以及凭据验证者模块;

[0044] 凭据属性结构创建者模块,用于定义和创建可验证凭据属性结构,并且将可验证

凭据属性结构信息记录于数据系统模块中；

[0045] 凭据颁发者模块，用于签发完整的可验证凭据以及更新可验证凭据属性；

[0046] 凭据持有者模块，用于管理和验证接收到的可验证凭据的正确性，以及按照凭据验证者的需要选择性披露可验证凭据属性信息以出示提交给凭据验证者；

[0047] 凭据验证者模块，用于验证凭据持有者出示提交的可验证凭据信息的真实性及有效性；

[0048] 数据系统模块，用于为其它模块提供可信数据访问服务，包括可验证凭据属性结构信息的记录及查询，可验证凭据及可验证凭据属性状态信息的记录及查询。

[0049] 本发明与现有技术相比的优点在于：

[0050] (1)原子性签名机制可直接基于各种流行的公钥密码算法来实现，在无强匿名性需求的场景下，与基于CL签名机制的方法相比更易于理解和实现；

[0051] (2)针对可验证凭据中的每个可验证凭据属性，基于原子性签名机制产生独立的原子签名信息，在验证某个原子签名信息时，不需要与该签名信息的产生过程无关的任何其它可验证凭据属性及其变体的参与，相应地，当选择性披露某些可验证凭据属性时，并不需要披露任何隐私属性的任何关联信息，因此，相较于现有基于披露隐私属性哈希值的方法，具有更高的安全性。

[0052] (3)基于原子性签名机制，在更新可验证凭据时，可以只更新部分可验证凭据属性，而不需要撤销整个可验证凭据再重新签发完整的可验证凭据，因此相较于现有技术，在更新可验证凭据属性时具有更高的灵活性和效率。

附图说明

[0053] 图1为可验证凭据应用系统结构图；

[0054] 图2为本发明方法实现流程图；

[0055] 图3为可验证凭据属性结构信息示例图；

[0056] 图4为原子性签名机制示意图；

[0057] 图5为完整的可验证凭据示例图；

[0058] 图6为可验证凭据及其可验证凭据属性状态信息示例图；

[0059] 图7为可验证凭据出示信息示例图。

具体实施方式

[0060] 为使本发明更加容易理解，结合一个实例对本发明作进一步阐述，但该实施例不构成对本发明的任何限制。

[0061] 如图1所示，一个可验证凭据应用系统，主要由区块链系统模块、凭据属性结构创建者模块、凭据颁发者模块、凭据持有者模块以及凭据验证者模块组成。其中，区块链系统模块作为数据系统，为其它模块提供可信数据访问服务，如可验证凭据属性结构信息的记录及查询，可验证凭据及可验证凭据属性状态信息的记录及查询等；凭据属性结构创建者模块定义和创建可验证凭据属性结构，并且将可验证凭据属性结构信息记录于区块链系统模块中；凭据颁发者模块，可签发完整的可验证凭据以及更新可验证凭据属性等；凭据持有者模块，管理和验证接收到的可验证凭据的正确性，以及按照凭据验证者的需要选择性披

露可验证凭据属性信息以出示提交给凭据验证者;凭据验证者模块,验证凭据持有者出示提交的可验证凭据信息的真实性及有效性。

[0062] 如图2所示,基于上述结构的应用系统来实现本发明所提出的一种基于原子性签名的可验证凭据实现方法,具体实施步骤如下:

[0063] 步骤S1:凭据属性结构创建者用户(例如某学位学历信息管理部门),使用凭据属性结构创建者模块,对特定类型的可验证凭据属性结构进行定义(例如高等学校学位证书),并且通过构建和提交区块链签名交易将可验证凭据属性结构信息(不妨记为CCS)记录于区块链系统Blockchain中,其中区块链系统可基于Bitcoin、Ethereum、Fabric或RepChain等底层平台实现。例如,某学位学历信息管理部门在区块链系统中创建了如图3所示的,表示高等学校学位证书的可验证凭据属性结构信息,其中凭据属性结构创建者身份标识使用去中心化身份标识DID(Decentralized Identifier)。

[0064] 步骤S2:凭据颁发者用户(例如某大学)针对某对象实体(例如某大学毕业生),使用凭据颁发者模块,根据步骤S1中创建的可验证凭据属性结构信息CCS,并基于原子性签名机制,构建含若干原子签名信息的完整可验证凭据,不妨记为VC。其具体实现为:

[0065] (2.1):获取区块链系统Blockchain中记录的可验证凭据属性结构信息CCS(不妨将CCS的可验证凭据属性个数记为l,在如图3所示的例子中l=5),填写可验证凭据元数据(不妨记为M)以及相应属性的属性值。

[0066] (2.2):对每个可验证凭据属性进行唯一编号(不妨记为N_i,其中$1\leqslant i\leqslant l$,$i\in Z$,Z为自然数集合),例如为保证编号在本可验证凭据范围内的唯一性,可使用编号值从1开始递增1的方式进行编号,即$N_1=\text{"1"}$,$N_2=\text{"2"}$,$N_3=\text{"3"}$,.....。

[0067] (2.3):基于原子性签名机制,针对每个可验证凭据属性(不妨记为C_i,其中$1\leqslant i\leqslant l$,$i\in Z$,Z为自然数集合)生成各自对应的原子签名信息(不妨记为S_i,其中$1\leqslant i\leqslant l$,$i\in Z$,Z为自然数集合)。

[0068] 如图4所示,原子性签名机制即是对每一个可验证凭据属性C_i及其编号N_i,凭据颁发者用户使用凭据颁发者模块,利用基于非对称密钥的数字签名算法(例如EcdsaSecp256k1Signature2019),单独对其与可验证凭据元数据M所组成的信息进行签名以生成原子签名信息S_i。即可表述为:$S_i=\text{Sign}(\text{PrvKey},M,C_i,N_i)$,$1\leqslant i\leqslant l$,$i\in Z$,Z为自然数集合,其中Sign表示基于非对称密钥的数字签名操作,PrvKey表示凭据颁发者用户用来进行签名操作的私钥。

[0069] (2.4):构建完整的可验证凭据VC。

[0070] 图5展示了某大学针对某大学毕业生所构建的一个表示高等学校学位证书的完整可验证凭据VC的示例,主要需包含信息:可验证凭据元数据、可验证凭据属性信息以及可验证凭据签名信息。其中可验证凭据元数据M包含凭据唯一标识、凭据类型、凭据属性结构唯一标识、凭据颁发者身份标识、凭据颁发时间、凭据有效期起始时间以及凭据有效期终止时间;可验证凭据属性信息,包含若干可验证凭据属性及其对应属性编号;可验证凭据签名信息包含签名信息元数据、若干原子签名信息以及对应属性编号,其中签名信息元数据包含签名算法、签名时间以及验签公钥信息。在图5的示例中使用了基于DID的公钥标识作为验签公钥信息。即一个完整的可验证凭据VC可被表述为$VC=(M,C,S)$,其中M表示可验证凭据元数据;C表示由若干可验证凭据属性C_i及其若干编号N_i构成的可验证凭据属性信息,可表

述为C＝{(C_i,N_i)|1≤i≤l,i∈Z},Z为自然数集合;S表示由签名信息元数据(不妨记为SM)、若干原子签名信息S_i及若干对应属性编号N_i构成的可验证凭据签名信息,可表述为S＝(SM,{(S_i,N_i)|1≤i≤l,i∈Z}),Z为自然数集合。

[0071] (2.5):构建及提交区块链签名交易,在区块链系统Blockchain中初始化可验证凭据VC的状态信息以及其各可验证凭据属性C_i的状态信息。

[0072] 图6显示了区块链系统所记录的一个具体的可验证凭据状态信息及其可验证凭据属性状态信息,在该示例中,将二者的状态信息合并为了一条记录,以共享可验证凭据唯一标识信息,使用一个字段status来表示整个可验证凭据的状态,初始化时该字段值为"Valid",表示整个可验证凭据处于有效状态;并且只使用一个数组类型的字段revokedClaimIndex去记录处于无效状态的可验证凭据属性的编号,编号被记录于该数组中的可验证凭据属性处于无效状态,否则相应可验证凭据属性处于有效状态,以此来减少数据存储量,初始化时该数组为空。

[0073] 步骤S3:在获取到凭据颁发者用户(例如某大学)在步骤S2中构建的完整可验证凭据VC后,凭据持有者用户(例如某大学毕业生)使用凭据持有者模块从区块链系统Blockchain中获取可验证凭据属性结构信息CCS,验证VC中的可验证凭据属性信息是否符合CCS的定义,验证逻辑可为:可验证凭据属性的数量需要一致以及可验证凭据属性的属性名称需要一致等,若验证失败则判定该VC不正确,不进行后续步骤;若符合,则再验证VC中的签名信息是否都正确(验证方法与后续步骤S5中的验证方法相同),若有不正确的签名信息,则判定该VC不正确,不予使用。

[0074] 步骤S4:根据凭据验证者用户(例如某企业招聘部门)所需可验证凭据属性信息的要求,凭据持有者用户(例如作为应聘者的某大学毕业生)使用凭据持有者模块,从可验证凭据VC中选择待披露的若干属性信息及其对应的原子签名信息进行封装,形成可验证凭据出示信息,不妨记为VCP,提交给凭据验证者用户。

[0075] 例如,某企业招聘部门指定应聘者需提供其高等学校学位证书中的部分信息(如学位获得者的DID身份标识、学位获得者的姓名及学位名称),作为应聘者的某大学毕业生,将根据需要使用凭据持有者模块封装如图7所示的可验证凭据出示信息VCP以提交给该企业招聘部门。该VCP中封装的可验证凭据信息,是单个可验证凭据,并且只暴露该企业招聘部门所需的可验证凭据属性:学位获得者的DID身份标识、学位获得者的姓名及学位名称。该企业招聘部门指定了VCP的提交者需在可验证凭据出示签名信息中包含对某个随机挑战信息challenge的签名,以防止重放攻击。其中,随机挑战信息是指由凭据验证方在验证过程中即时地随机生成并传递给凭据持有方的数据信息,比如随机生成的字符串或二进制数据,随机挑战信息的有效期应当被限定在一次验证过程中。

[0076] 步骤S5:对于从步骤S4中接收到的可验证凭据出示信息VCP,凭据验证者用户(例如某企业招聘部门)使用凭据验证者模块验证VCP提交者的签名,即根据VCP中指定的验签公钥信息以及签名算法信息验证签名正确性,并判断随机挑战信息是否正确。若签名信息或随机挑战信息不正确,则判定VCP无效;若签名信息和随机挑战信息均正确,则继续对VCP所封装的可验证凭据进行验证,其具体实现为:

[0077] (5.1):根据可验证凭据元数据M中的凭据有效期起始时间以及凭据有效期终止时间,验证可验证凭据当前是否处于有效期内,若未处于,则不进行后续操作;否则,执行步骤

(5.2)；

[0078] (5.2)：向区块链系统Blockchain获取该可验证凭据的状态信息，验证是否为有效状态，若无效，则不进行后续步骤；若有效，则执行步骤(5.3)；

[0079] (5.3)：向区块链系统Blockchain获取可验证凭据中每个可验证凭据属性的状态信息，验证是否都有效，若存在无效的可验证凭据属性，则不进行后续步骤；若都有效，则执行步骤(5.4)；

[0080] (5.4)：获取基于DID标识的验签公钥信息，根据可验证凭据中的签名算法以及验签公钥信息，对每一个被披露出来的可验证凭据属性(不妨记为SC_i)及其对应原子签名(不妨记为SS_i)进行基于非对称密钥的数字验签操作，验签操作可表示为：Verify(PubKey，M，SC_i，SN_i，SS_i)，1≤i≤ll，i∈Z，其中Verify表示基于非对称密钥的验签操作，PubKey表示用以进行验签操作的公钥，M表示可验证凭据元数据，SN_i表示相应被披露出的可验证凭据属性的编号，ll为被披露出的可验证凭据属性的个数(在如图7所示的示例中ll＝3)，Z为自然数集合。若验签操作结果均正确，则通过对可验证凭据的验证，否则不通过。

[0081] 步骤S6：根据具体需要，凭据颁发者用户(例如某大学)可基于撤销原凭据再签发完整新凭据的方式更新完整可验证凭据，或者只更新部分可验证凭据属性。当更新完整可验证凭据时，需要先向区块链系统Blockchain提交请求将其记录的相应可验证凭据的状态置为无效，然后按照步骤S2的方法重新签发可验证凭据。当需要只更新部分可验证凭据属性时，其具体实现为：

[0082] (6.1)：根据可验证凭据的唯一标识以及待被更新的可验证凭据属性的原始编号，向区块链系统Blockchain提交请求，将待被更新的可验证凭据属性的状态置为无效，即在其状态记录信息中的revokedClaimIndex字段中添加待被更新的可验证属性的编号；

[0083] (6.2)：为待被更新的可验凭据属性填写新的属性值，并且赋予新的唯一编号；

[0084] (6.3)：基于原子性签名机制产生新的原子签名信息，并将新的可验证凭据属性、新的可验证凭据属性编号以及新的原子签名信息提交给凭据持有者；

[0085] (6.4)：根据可验证凭据的唯一标识以及已被更新的可验证凭据属性的新编号向区块链系统提交请求，将具有新编号的可验证凭据属性的状态初始化为有效，在本实施例中可验证凭据属性的状态默认为有效，故可省略本步骤。

[0086] 基于同一发明构思，本发明的另一实施例提供一种电子装置(计算机、服务器、智能手机等)，其包括存储器和处理器，所述存储器存储计算机程序，所述计算机程序被配置为由所述处理器执行，所述计算机程序包括用于执行本发明方法中各步骤的指令。

[0087] 基于同一发明构思，本发明的另一实施例提供一种计算机可读存储介质(如ROM/RAM、磁盘、光盘)，所述计算机可读存储介质存储计算机程序，所述计算机程序被计算机执行时，实现本发明方法的各个步骤。

[0088] 本发明未详细阐述部分属于本领域的公知技术。

[0089] 以上公开的本发明的具体实施例，其目的在于帮助理解本发明的内容并据以实施，本领域的普通技术人员可以理解，在不脱离本发明的精神和范围内，各种替换、变化和修改都是可能的。本发明不应局限于本说明书的实施例所公开的内容，本发明的保护范围以权利要求书界定的范围为准。

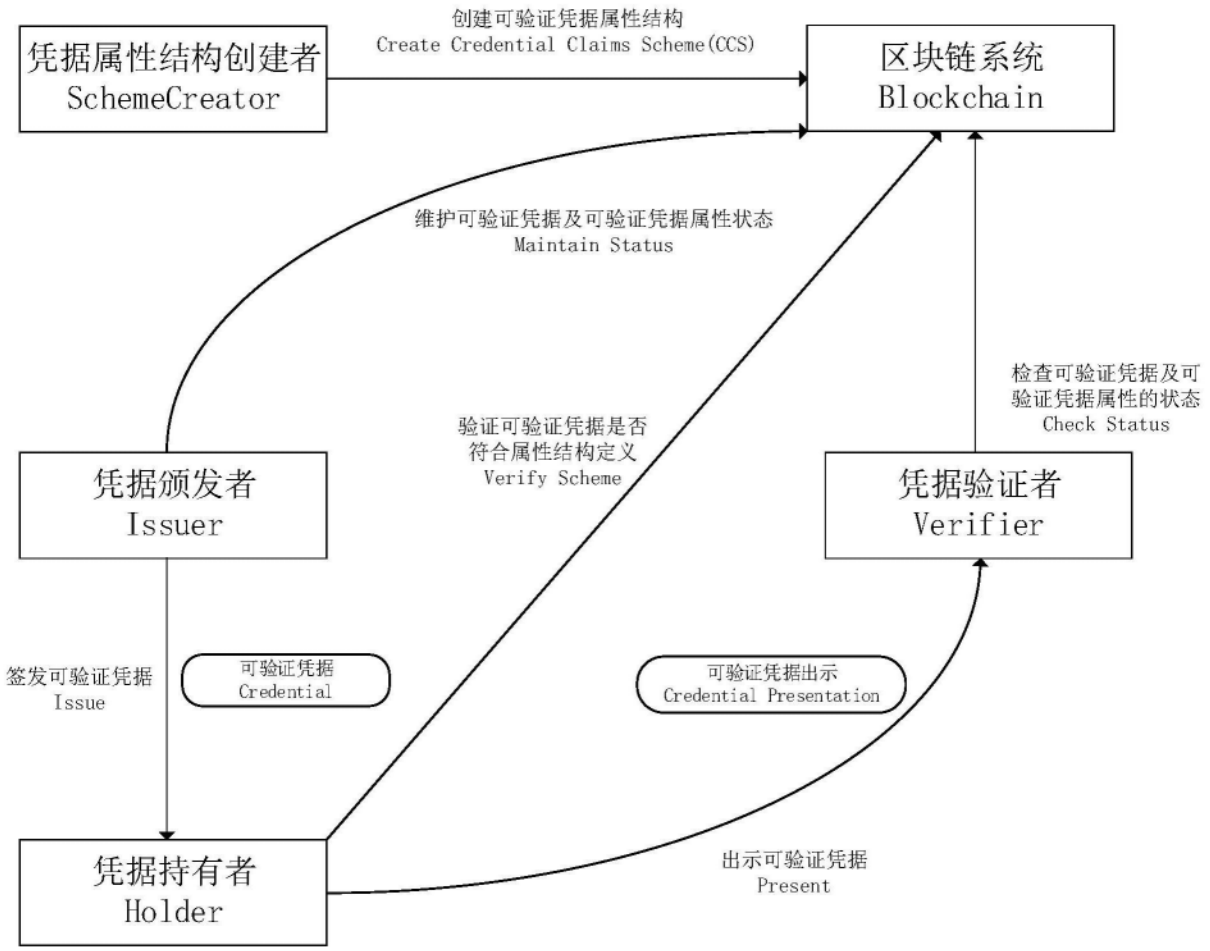

凭据属性结构创建者
SchemeCreator
创建可验证凭据属性结构
Create Credential Claims Scheme(CCS)
区块链系统
Blockchain
维护可验证凭据及可验证凭据属性状态
Maintain Status
检查可验证凭据及可
验证凭据属性的状态
Check Status
验证可验证凭据是否
符合属性结构定义
Verify Scheme
凭据颁发者
Issuer
凭据验证者
Verifier
签发可验证凭据
Issue
可验证凭据
Credential
可验证凭据出示
Credential Presentation
凭据持有者
Holder
出示可验证凭据
Present

图1

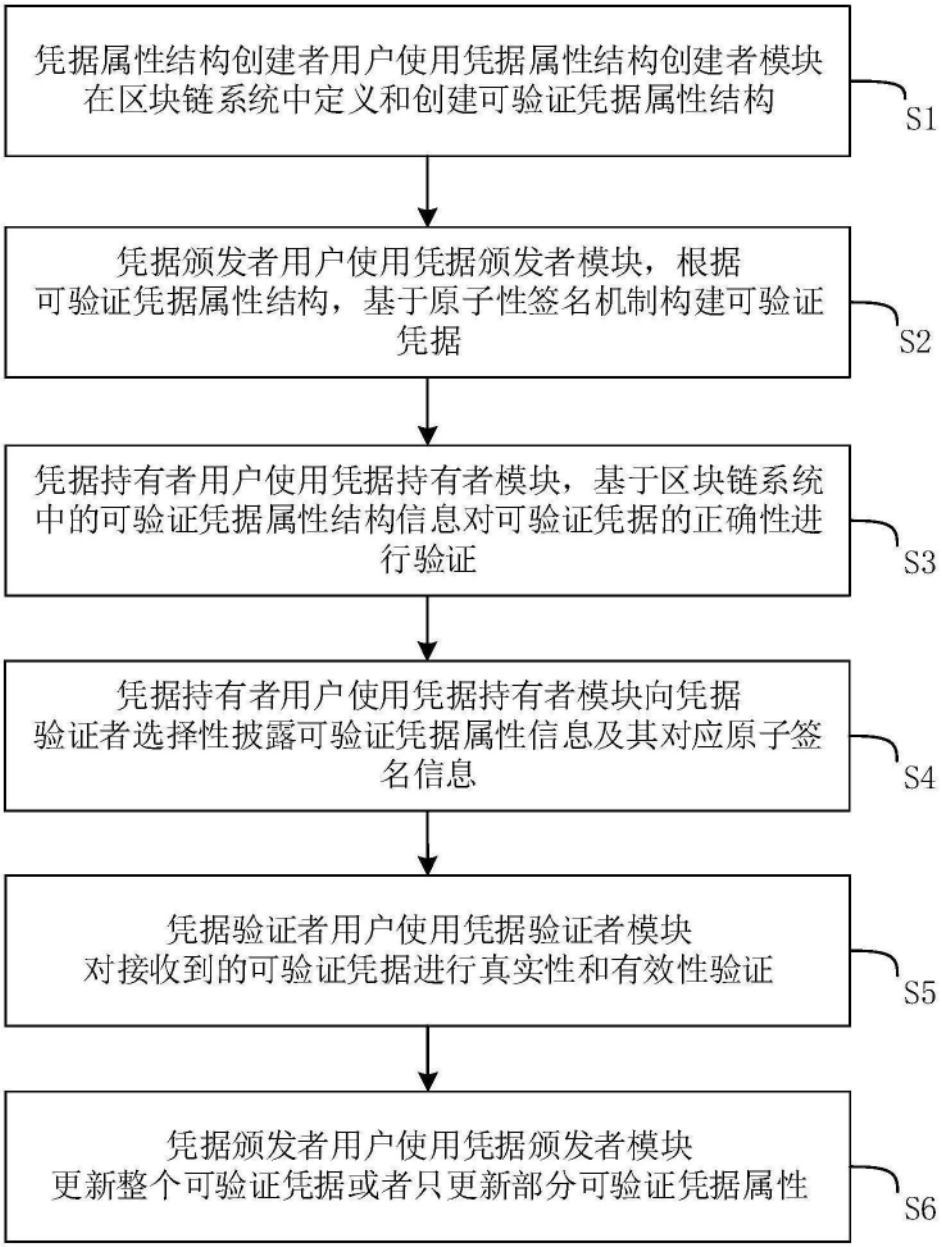

凭据属性结构创建者用户使用凭据属性结构创建者模块在区块链系统中定义和创建可验证凭据属性结构
S1
凭据颁发者用户使用凭据颁发者模块，根据可验证凭据属性结构，基于原子性签名机制构建可验证凭据
S2
凭据持有者用户使用凭据持有者模块，基于区块链系统中的可验证凭据属性结构信息对可验证凭据的正确性进行验证
S3
凭据持有者用户使用凭据持有者模块向凭据验证者选择性披露可验证凭据属性信息及其对应原子签名信息
S4
凭据验证者用户使用凭据验证者模块对接收到的可验证凭据进行真实性和有效性验证
S5
凭据颁发者用户使用凭据颁发者模块更新整个可验证凭据或者只更新部分可验证凭据属性
S6

图2

```
{
    "凭据属性结构唯一标识": "CCS-0001",
    "凭据类型名称": "UniversityDegreeCredential",
    "凭据属性结构版本": "0.1",
    "凭据属性结构的描述说明": "普通高等学校学位证书，可作为普通高等学校颁发给个人的学位获得证明",
    "凭据属性结构创建者身份标识": "did:rep:network_1:98765abcdefg",
    "凭据属性结构创建时间": "2020-01-18T19:05:22Z",
    "凭据属性集合": [
        {
            "属性名称": "id",
            "属性值的类型": "String",
            "属性描述说明": "学位获得者的DID标识"
        },
        {
            "属性名称": "name",
            "属性值的类型": "String",
            "属性描述说明": "学位获得者的姓名"
        },
        {
            "属性名称": "degree",
            "属性值的类型": "String",
            "属性描述说明": "学位名称"
        },
        {
            "属性名称": "university",
            "属性值的类型": "String",
            "属性描述说明": "授予学位的学校名称"
        },
        {
            "属性名称": "graduationDate",
            "属性值的类型": "String",
            "属性描述说明": "获得学位的日期"
        },
    ]
}
```


图3

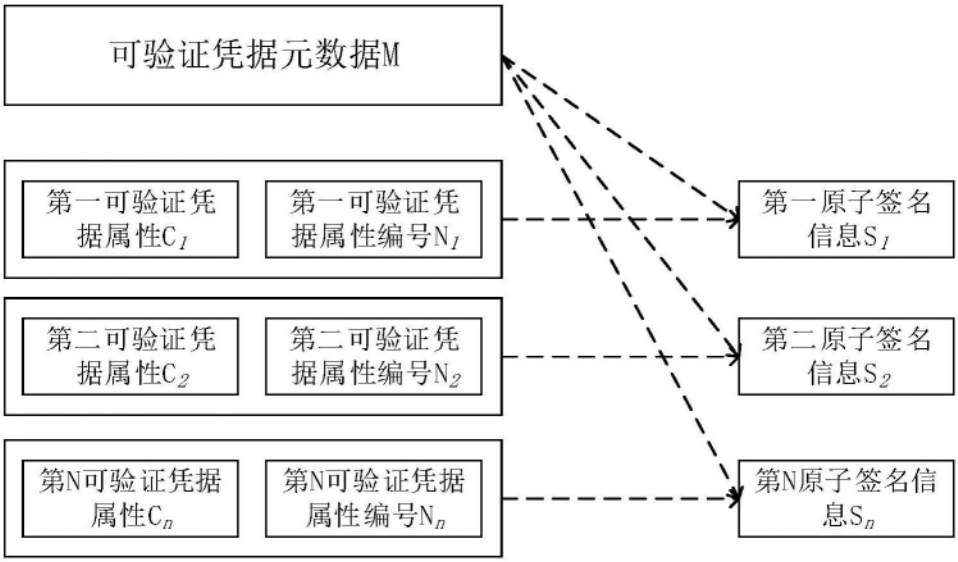

可验证凭据元数据M
第一可验证凭据属性C_1
第一可验证凭据属性编号N_1
第一原子签名信息S_1
第二可验证凭据属性C_2
第二可验证凭据属性编号N_2
第二原子签名信息S_2
第N可验证凭据属性C_n
第N可验证凭据属性编号N_n
第N原子签名信息S_n

图4


{
"@context": "https://www.w3.org/2018/credentials/v1",
"id": "0123456789abcdef",
"type": "UniversityDegreeCredential",
"claimScheme": "CCS-0001",
"issuer": "did:rep:network_1:1234567",
"issued": "2021-01-19T19:05:22Z",
"validFrom": "2021-01-19T19:05:22Z",
"validUntil": "9999-01-19T19:05:22Z",
"credentialSubject": {
"1": { "id": "did:rep:network_1:9876543" },
"2": { "name": "Alice" },
"3": { "degree": "MasterDegree" },
"4": { "university": "RepChain Training University" },
"5": { "graduationDate": "2021-01-19" },
},
"proof": {
"type": "EcdsaSecp256k1Signature2019",
"created": "2021-01-19T09:05:22Z",
"verificationMethod": "did:rep:network_1:1234567#key1",
"signature": {
"1": "gcyudgda898cdcbjsdhGYUGHJGBJHDSHJ&867tHJSGHJ.....JUHBXCYUDyt876732btd67120",
"2": "djskcdjkscds8890210qHJGBYUJHNUIjjjh7sa.....HDYSDHST892BYU",
"3": "JGYUIDHJhdscui91289uxcjdsnjkhujkJNXSKJHK.....987238976sgx67gsGHJSGSH",
"4": "213hdsartGFTTXNJX97t6fSsxbygxs672167HH.....jhsdvhGFRAXNITvxgsh56256GxjxjkUAAF",
"5": "jhjcdsHFGGHSAJAIYTAF72817GShgy2716vt67.....aosjxiuoIOJAJK21w8tzsa89xs45asxjsaHJ",
}
}
}
可验证凭据元数据M
可验证凭据属性信息C
可验证凭据签名信息S
签名信息元数据SM
原子签名信息

图5

```
{
  "id": "0123456789abcdef",
  "status": "Valid",
  "revokedClaimIndex": []
}
```


图6


```
{
  "@context": "https://www.w3.org/2018/credentials/v1",
  "id": "presentation#000101",
  "type": "UniversityDegreeCredentialPresentation",
  "holder": "did:rep:network_1:9876543",
  "verifiableCredential": {
    "@context": "https://www.w3.org/2018/credentials/v1",
    "id": "0123456789abcdef",
    "type": "UniversityDegreeCredential",
    "claimScheme": "CCS-0001",
    "issuer": "did:rep:network_1:1234567",
    "issued": "2021-01-19T19:05:22Z",
    "validFrom": "2021-01-19T19:05:22Z",
    "validUntil": "9999-01-19T19:05:22Z",
    "credentialSubject": {
      "1": { "id": "did:rep:network_1:9876543" },
      "2": { "name": "Alice" },
      "3": { "degree": "MasterDegree" },
    },
    "proof": {
      "type": "EcdsaSecp256k1Signature2019",
      "created": "2021-01-19T09:05:22Z",
      "verificationMethod": "did:rep:network_1:1234567#key1",
      "signature": {
        "1": "gcyudgda898cdcbjsdhGYUGHJGBJHDSHJ&867tHJSGHJ.....JUHBXCYUDyt876732btd67120",
        "2": "djskcdjkscds8890210qHJGBYUJHNUIjjjh7sa.....HDYSDHST892BYU",
        "3": "JGYUIDHJhdscui91289uxcjdsnjkhujkJNXSKJHK.....987238976sgx67gsGHJSGSH"
      }
    }
  }
  "proof": {
    "type": "EcdsaSecp256k1Signature2019",
    "created": "2021-05-01T19:25:23Z",
    "verificationMethod": "did:rep:network_1:9876543#key2",
    "challenge": "xhjgh-8392-ncjds",
    "signature": "kdhsHJKKAuiTRDyqty767w21gygxg16VG91.....hdshhYUGS89789GJGH679GYJGHJGstyaftsfa"
  }
}
```


可验证凭据出示元数据

可验证凭据信息

可验证凭据出示签名

图7