(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115664861 B
(45)授权公告日 2023.02.28

(21)申请号 202211679008.6
(22)申请日 2022.12.27
(65)同一申请的已公布的文献号
申请公布号 CN 115664861 A
(43)申请公布日 2023.01.31
(73)专利权人 中国信息通信研究院
地址 100191 北京市海淀区学院路40号
(72)发明人 杨鹏 池程 尹子航 朱斯语
(74)专利代理机构 北京思源智汇知识产权代理有限公司 11657
专利代理师 王晓多
(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 113541970 A,2021.10.22,全文.
CN 115208698 A,2022.10.18,全文.
WO 2020008367 A1,2020.01.09,全文.
WO 2021139605 A1,2021.07.15,全文.

审查员 王侠

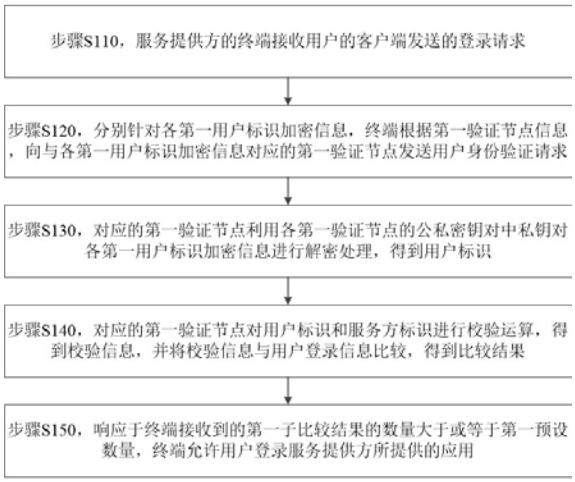
权利要求书3页 说明书16页 附图7页

(54)发明名称

基于区块链的身份信息验证方法和装置、设备和介质

(57)摘要

本公开实施例公开了一种基于区块链的身份信息验证方法和装置、设备和介质，其中，方法包括：服务提供方的终端根据接收到的登录请求中的第一验证节点信息，向各第一验证节点发送用户身份验证请求，其中，用户身份验证请求包括：第一用户标识加密信息、服务提供方的服务方标识和用户登录信息；各第一验证节点利用其公私密钥对中私钥对第一用户标识加密信息进行解密处理，得到用户标识，并对用户标识和服务方标识进行校验运算，得到校验信息，之后将校验信息与用户登录信息比较，得到比较结果；当终端接收到的比较结果中，第一子比较结果的数量大于或等于第一预设数量，终端允许用户登录服务提供方所提供的应用。



CN 115664861 B

1.一种基于区块链的身份信息验证方法,其特征在于,包括:

服务提供方的终端接收用户的客户端发送的登录请求,其中,所述登录请求包括:用户登录信息、至少一个第一用户标识加密信息和第一验证节点信息;所述至少一个第一用户标识加密信息中的各第一用户标识加密信息,利用与所述第一用户标识加密信息对应的区块链的第一验证节点的公私密钥对中公钥加密所述用户的用户标识得到;所述第一验证节点信息包括各第一用户标识加密信息对应的第一验证节点;

分别针对所述各第一用户标识加密信息,所述终端根据所述第一验证节点信息,向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求,其中,所述用户身份验证请求包括:所述第一用户标识加密信息、所述服务提供方的服务方标识和所述用户登录信息;

对应的第一验证节点利用所述各第一验证节点的公私密钥对中私钥对所述各第一用户标识加密信息进行解密处理,得到所述用户标识;

所述对应的第一验证节点对所述用户标识和所述服务方标识进行校验运算,得到校验信息,并将所述校验信息与所述用户登录信息比较,得到比较结果,其中,所述比较结果包括:用于指示所述校验信息和所述用户登录信息相同的第一子比较结果,或者,用于指示所述校验信息和所述用户登录信息不同的第二子比较结果;

响应于所述终端接收到的所述第一子比较结果的数量大于或等于第一预设数量,所述终端允许所述用户登录所述服务提供方所提供的应用。

2.根据权利要求1所述的方法,其特征在于,所述登录请求还包括:第一发送时间;所述方法还包括:

所述终端确定当前时间与所述第一发送时间之间的第一时间间隔;

响应于所述第一时间间隔小于或等于预设时间间隔,执行所述分别针对所述各第一用户标识加密信息,所述终端根据所述第一验证节点信息,向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求的操作。

3.根据权利要求1所述的方法,其特征在于,还包括:

所述客户端利用预设算法对第一预设信息进行处理,得到第一运算结果;

所述客户端获取预设验证节点数量;

所述客户端根据所述预设验证节点数量,对所述第一运算结果执行切分处理,得到所述预设验证节点数量的第一运算子结果;

对于任一第一运算子结果,所述客户端对所述第一运算子结果进行转换处理,以得到所述第一运算子结果对应的数值;

所述客户端基于所述区块链的节点的编号和所述第一运算子结果对应的数值,确定所述第一验证节点。

4.根据权利要求3所述的方法,其特征在于,还包括:

所述客户端根据所述区块链的节点故障率,确定所述区块链的节点可靠概率;

所述客户端根据所述节点可靠概率,基于预设验证成功概率模型和预设模型条件,确定所述预设验证节点数量。

5.根据权利要求1所述的方法,其特征在于,还包括:

所述终端接收所述客户端发送的注册请求,其中,所述注册请求包括:至少一个第二用

户标识加密信息和第二验证节点信息;所述至少一个第二用户标识加密信息中的各第二用户标识加密信息,利用与所述第二用户标识加密信息对应的第二验证节点的公私密钥对中公钥加密所述用户标识得到;所述第二验证节点信息包括各第二用户标识加密信息对应的第二验证节点;

分别针对所述各第二用户标识加密信息,所述终端根据所述第二验证节点信息,向与所述各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求,其中,所述登录信息生成请求包括:所述第二用户标识加密信息和所述服务方标识;

对应的第二验证节点利用所述各第二验证节点的公私密钥对中私钥对所述各第二用户标识加密信息进行解密处理,得到所述用户标识;

所述对应的第二验证节点对所述用户标识和所述服务方标识进行校验运算,得到校验信息,并将所述校验信息反馈所述终端;

响应于所述终端接收到的相同的校验信息的数量大于或等于第二预设数量,所述终端将相同的数量大于或等于所述第二预设数量的所述校验信息确定为所述用户登录信息。

6.根据权利要求5所述的方法,其特征在于,所述注册请求还包括:第二发送时间;所述方法还包括:

所述终端确定当前时间与所述第二发送时间之间的第二时间间隔;

响应于所述第二时间间隔小于或等于预设时间间隔,执行所述分别针对所述各第二用户标识加密信息,所述终端根据所述第二验证节点信息,向与所述各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求的操作。

7.根据权利要求5所述的方法,其特征在于,还包括:

所述客户端利用预设算法对第二预设信息进行处理,得到第二运算结果;

所述客户端获取预设验证节点数量;

所述客户端根据所述预设验证节点数量,对所述第二运算结果执行切分处理,得到所述预设验证节点数量的第二运算子结果;

对于任一第二运算子结果,所述客户端对所述第二运算子结果进行转换处理,以得到所述第二运算子结果对应的数值;

所述客户端基于所述区块链的节点的编号和所述第二运算子结果对应的数值,确定所述第二验证节点。

8.一种基于区块链的身份信息验证装置,其特征在于,包括:

第一接收模块,用于服务提供方的终端接收用户的客户端发送的登录请求,其中,所述登录请求包括:用户登录信息、至少一个第一用户标识加密信息和第一验证节点信息;所述至少一个第一用户标识加密信息中的各第一用户标识加密信息,利用与所述第一用户标识加密信息对应的区块链的第一验证节点的公私密钥对中公钥加密所述用户的用户标识得到;所述第一验证节点信息包括各第一用户标识加密信息对应的第一验证节点;

第一发送模块,用于分别针对所述各第一用户标识加密信息,所述终端根据所述第一验证节点信息,向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求,其中,所述用户身份验证请求包括:所述第一用户标识加密信息、所述服务提供方的服务方标识和所述用户登录信息;

第一解密模块,用于对应的第一验证节点利用所述各第一验证节点的公私密钥对中私

钥对所述各第一用户标识加密信息进行解密处理,得到所述用户标识;

比较模块,用于所述对应的第一验证节点对所述用户标识和所述服务方标识进行校验运算,得到校验信息,并将所述校验信息与所述用户登录信息比较,得到比较结果,其中,所述比较结果包括:用于指示所述校验信息和所述用户登录信息相同的第一子比较结果,或者,用于指示所述校验信息和所述用户登录信息不同的第二子比较结果;

验证模块,用于响应于所述终端接收到的所述第一子比较结果的数量大于或等于第一预设数量,所述终端允许所述用户登录所述服务提供方所提供的应用。

9.一种电子设备,其特征在于,包括:

存储器,用于存储计算机程序;

处理器,用于执行所述存储器中存储的计算机程序,且所述计算机程序被执行时,实现上述权利要求1-7中任一所述的方法。

10.一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该计算机程序被处理器执行时,实现上述权利要求1-7中任一所述的方法。

基于区块链的身份信息验证方法和装置、设备和介质

技术领域

[0001] 本公开涉及区块链技术、身份验证技术，尤其是一种基于区块链的身份信息验证方法和装置、设备和介质。

背景技术

[0002] 数字身份中心化管理方式是当前应用常用的身份管理方式。在现有技术中，数字身份中心化管理方式中主要包括三个角色：用户、服务提供商和身份提供商。通过这种数字身份中心化管理方式实现登录应用的流程主要包括：由用户通过其用户标识发起身份验证请求，服务提供商根据用户标识向身份提供商请求用户信息，用户向身份提供商提供证明信息，如密码、验证码等，然后身份提供商验证并告知应用的服务提供商的安全登陆页面，用户完成登陆。由于登录过程中服务提供商获取了用户标识、密码、验证码等，这使得用户的信息存在泄漏风险。

发明内容

[0003] 本公开实施例提供一种基于区块链的身份信息验证方法和装置、设备和介质，以解决上述问题。

[0004] 本公开实施例的一个方面，提供了一种基于区块链的身份信息验证方法，包括：服务提供方的终端接收用户的客户端发送的登录请求，其中，所述登录请求包括：用户登录信息、至少一个第一用户标识加密信息和第一验证节点信息；所述至少一个第一用户标识加密信息中的各第一用户标识加密信息，利用与所述第一用户标识加密信息对应的区块链的第一验证节点的公私密钥对中公钥加密所述用户的用户标识得到；所述第一验证节点信息包括各第一用户标识加密信息对应的第一验证节点；分别针对所述各第一用户标识加密信息，所述终端根据所述第一验证节点信息，向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求，其中，所述用户身份验证请求包括：所述第一用户标识加密信息、所述服务提供方的服务方标识和所述用户登录信息；对应的第一验证节点利用所述各第一验证节点的公私密钥对中私钥对所述各第一用户标识加密信息进行解密处理，得到所述用户标识；所述对应的第一验证节点对所述用户标识和所述服务方标识进行校验运算，得到校验信息，并将所述校验信息与所述用户登录信息比较，得到比较结果，其中，所述比较结果包括：用于指示所述校验信息和所述用户登录信息相同的第一子比较结果，或者，用于指示所述校验信息和所述用户登录信息不同的第二子比较结果；响应于所述终端接收到的所述第一子比较结果的数量大于或等于第一预设数量，所述终端允许所述用户登录所述服务提供方所提供的应用。

[0005] 可选地，在本公开上述任一实施例的方法中，所述登录请求还包括：第一发送时间；所述方法还包括：所述终端确定当前时间与所述第一发送时间之间的第一时间间隔；响应于所述第一时间间隔小于或等于预设时间间隔，执行所述分别针对所述各第一用户标识加密信息，所述终端根据所述第一验证节点信息，向与所述各第一用户标识加密信息对应

的第一验证节点发送用户身份验证请求的操作。

[0006] 可选地，在本公开上述任一实施例的方法中，还包括：所述客户端利用预设算法对第一预设信息进行处理，得到第一运算结果；所述客户端获取预设验证节点数量；所述客户端根据所述预设验证节点数量，对所述第一运算结果执行切分处理，得到所述预设验证节点数量的第一运算子结果；对于任一第一运算子结果，所述客户端对所述第一运算子结果进行转换处理，以得到所述第一运算子结果对应的数值；所述客户端基于所述区块链的节点的编号和所述第一运算子结果对应的数值，确定所述第一验证节点。

[0007] 可选地，在本公开上述任一实施例的方法中，还包括：所述客户端根据所述区块链的节点故障率，确定所述区块链的节点可靠概率；所述客户端根据所述节点可靠概率，基于预设验证成功概率模型和预设模型条件，确定所述预设验证节点数量。

[0008] 可选地，在本公开上述任一实施例的方法中，还包括：所述终端接收所述客户端发送的注册请求，其中，所述注册请求包括：至少一个第二用户标识加密信息和第二验证节点信息；所述至少一个第二用户标识加密信息中的各第二用户标识加密信息，利用与所述第二用户标识加密信息对应的第二验证节点的公私密钥对中公钥加密所述用户标识得到；所述第二验证节点信息包括各第二用户标识加密信息对应的第二验证节点；分别针对所述各第二用户标识加密信息，所述终端根据所述第二验证节点信息，向与所述各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求，其中，所述登录信息生成请求包括：所述第二用户标识加密信息和所述服务方标识；对应的第二验证节点利用所述各第二验证节点的公私密钥对中私钥对所述各第二用户标识加密信息进行解密处理，得到所述用户标识；所述对应的第二验证节点对所述用户标识和所述服务方标识进行校验运算，得到校验信息，并将所述校验信息反馈所述终端；响应于所述终端接收到的相同的校验信息的数量大于或等于第二预设数量，所述终端将相同的数量大于或等于所述第二预设数量的所述校验信息确定为所述用户登录信息。

[0009] 可选地，在本公开上述任一实施例的方法中，所述注册请求还包括：第二发送时间；所述方法还包括：所述终端确定当前时间与所述第二发送时间之间的第二时间间隔；响应于所述第二时间间隔小于或等于预设时间间隔，执行所述分别针对所述各第二用户标识加密信息，所述终端根据所述第二验证节点信息，向与所述各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求的操作。

[0010] 可选地，在本公开上述任一实施例的方法中，还包括：所述客户端利用预设算法对第二预设信息进行处理，得到第二运算结果；所述客户端获取预设验证节点数量；所述客户端根据所述预设验证节点数量，对所述第二运算结果执行切分处理，得到所述预设验证节点数量的第二运算子结果；对于任一第二运算子结果，所述客户端对所述第二运算子结果进行转换处理，以得到所述第二运算子结果对应的数值；所述客户端基于所述区块链的节点的编号和所述第二运算子结果对应的数值，确定所述第二验证节点。

[0011] 本公开实施例的一个方面，提供了一种基于区块链的身份信息验证装置，包括：第一接收模块，用于服务提供方的终端接收用户的客户端发送的登录请求，其中，所述登录请求包括：用户登录信息、至少一个第一用户标识加密信息和第一验证节点信息；所述至少一个第一用户标识加密信息中的各第一用户标识加密信息，利用与所述第一用户标识加密信息对应的区块链的第一验证节点的公私密钥对中公钥加密所述用户的用户标识得到；所述

第一验证节点信息包括各第一用户标识加密信息对应的第一验证节点;第一发送模块,用于分别针对所述各第一用户标识加密信息,所述终端根据所述第一验证节点信息,向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求,其中,所述用户身份验证请求包括:所述第一用户标识加密信息、所述服务提供方的服务方标识和所述用户登录信息;第一解密模块,用于对应的第一验证节点利用所述各第一验证节点的公私密钥对中私钥对所述各第一用户标识加密信息进行解密处理,得到所述用户标识;比较模块,用于所述对应的第一验证节点对所述用户标识和所述服务方标识进行校验运算,得到校验信息,并将所述校验信息与所述用户登录信息比较,得到比较结果,其中,所述比较结果包括:用于指示所述校验信息和所述用户登录信息相同的第一子比较结果,或者,用于指示所述校验信息和所述用户登录信息不同的第二子比较结果;验证模块,用于响应于所述终端接收到的所述第一子比较结果的数量大于或等于第一预设数量,所述终端允许所述用户登录所述服务提供方所提供的应用。

[0012] 本公开实施例的一个方面,提供了一种电子设备,包括:存储器,用于存储计算机程序;处理器,用于执行所述存储器中存储的计算机程序,且所述计算机程序被执行时,实现上述基于区块链的身份信息验证方法。

[0013] 本公开实施例的一个方面,提供了一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时,实现上述基于区块链的身份信息验证方法。

[0014] 本公开实施例提供了一种基于区块链的身份信息验证方法和装置、设备和介质,包括:服务提供方的终端根据接收到的登录请求中的第一验证节点信息,向与登录请求中的各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求,其中,该用户身份验证请求包括:第一用户标识加密信息、服务提供方的服务方标识和用户登录信息;之后第一验证节点利用其公私密钥对中私钥对第一用户标识加密信息进行解密处理,得到用户标识,并对用户标识和服务方标识进行校验运算,得到校验信息,之后将校验信息与用户登录信息比较,得到比较结果;当终端接收到的比较结果中,第一子比较结果的数量大于或等于第一预设数量,终端允许用户登录服务提供方所提供的应用。由此,本公开实施例中,通过使用用户登录信息和第一用户标识加密信息实现用户登录服务提供方所提供的应用。在登录过程中,服务提供方仅获得了用户登录信息和第一用户标识加密信息,未获得用户标识,有效的避免了服务提供方之间通过用户标识共享用户信息的问题,降低了用户信息跨站泄漏的风险。另外,采用了多个第一验证节点投票的方式,极大的提升了比较结果的可靠性。

[0015] 下面通过附图和实施例,对本公开的技术方案做进一步的详细描述。

附图说明

[0016] 构成说明书的一部分的附图描述了本公开的实施例,并且连同描述一起用于解释本公开的原理。

[0017] 参照附图,根据下面的详细描述,可以更加清楚地理解本公开,其中:

[0018] 图1是本公开一示例性实施例提供的基于区块链的身份信息验证方法的流程示意图;

[0019] 图2是本公开另一示例性实施例提供的基于区块链的身份信息验证方法的流程示

意图；

[0020] 图3是本公开又一示例性实施例提供的基于区块链的身份信息验证方法的流程示意图；

[0021] 图4是本公开再一示例性实施例提供的基于区块链的身份信息验证方法的流程示意图；

[0022] 图5是本公开又一示例性实施例提供的基于区块链的身份信息验证方法的流程示意图；

[0023] 图6是本公开又一示例性实施例提供的基于区块链的身份信息验证方法的流程示意图；

[0024] 图7是本公开又一示例性实施例提供的基于区块链的身份信息验证方法的流程示意图；

[0025] 图8是本公开再一示例性实施例提供的基于区块链的身份信息验证方法的交互示意图；

[0026] 图9是本公开一示例性实施例提供的基于区块链的身份信息验证装置的结构示意图；

[0027] 图10为本公开电子设备一个应用实施例的结构示意图。

具体实施方式

[0028] 现在将参照附图来详细描述本公开的各种示例性实施例。应注意到：除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本公开的范围。

[0029] 本领域技术人员可以理解，本公开实施例中的“第一”、“第二”等术语仅用于区别不同步骤、设备或模块等，既不代表任何特定技术含义，也不表示它们之间的必然逻辑顺序。

[0030] 还应理解，在本公开实施例中，“多个”可以指两个或两个以上，“至少一个”可以指一个、两个或两个以上。

[0031] 还应理解，对于本公开实施例中提及的任一部件、数据或结构，在没有明确限定或者在前后文给出相反启示的情况下，一般可以理解为一个或多个。

[0032] 另外，本公开中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本公开中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0033] 还应理解，本公开对各个实施例的描述着重强调各个实施例之间的不同之处，其相同或相似之处可以相互参考，为了简洁，不再一一赘述。

[0034] 同时，应当明白，为了便于描述，附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0035] 以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本公开及其应用或使用的任何限制。

[0036] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为说明书的一部分。

[0037] 应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步讨论。

[0038] 本公开实施例可以应用于终端设备、计算机系统、服务器等电子设备,其可与众多其它通用或专用计算系统环境或配置一起操作。适于与终端设备、计算机系统、服务器等电子设备一起使用的众所周知的终端设备、计算系统、环境和/或配置的例子包括但不限于:个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境,等等。

[0039] 终端设备、计算机系统、服务器等电子设备可以在由计算机系统执行的计算机系统可执行指令(诸如程序模块)的一般语境下描述。通常,程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等,它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施,分布式云计算环境中,任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中,程序模块可以位于包括存储设备的本地或远程计算系统存储介质上。

[0040] 图1示出本公开实施例中基于区块链的身份信息验证方法的流程示意图。本实施例可应用在电子设备上,如图1所示,本实施例的基于区块链的身份信息验证方法包括如下步骤:

[0041] 步骤S110,服务提供方的终端接收用户的客户端发送的登录请求。

[0042] 其中,该登录请求包括:用户登录信息、至少一个第一用户标识加密信息和第一验证节点信息;该至少一个第一用户标识加密信息中的各第一用户标识加密信息,利用与该第一用户标识加密信息对应的区块链的第一验证节点的公私密钥对中公钥加密所述用户的用户标识得到;该第一验证节点信息包括各第一用户标识加密信息对应的第一验证节点。

[0043] 可以确定利用第一验证节点的公私密钥对中公钥加密用户标识得到的第一用户标识加密信息与该第一验证节点具有对应关系。服务提供方可以为向用户提供应用(Application,APP)的企业、个人或团体等,服务提供方的终端和用户的客户端可以为服务器、计算机、PDA(Personal Digital Assistant,掌上电脑)等,服务提供方的终端和用户的客户端通信连接。

[0044] 用户登录信息用于验证用户身份,以使用户登录服务提供方的提供的应用。用户标识用于唯一标识一个用户,例如,用户标识可以为DIDs(Decentralized Identifiers、分布式标识符)等。区块链(Block Chain)是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证数据不可篡改和不可伪造的分布式账本。区块链的网络结包括多个节点,通过多个节点实现区块链的服务和功能。将用于验证用户登录信息的区块链的节点称为第一验证节点。在一种实现方式中,区块链可以以联盟链的形式组织,其受国家相关机构严格监管。在该区块链上可以保存用户标识以及和该用户标识相关联的其他信息。联盟链只针对某个特定群体的成员和有限的第三方,其内部指定多个预选节点为记账人,每个块的生成由所有的预选节点共同决定。

[0045] 每个第一验证节点的公私密钥对包括公钥和私钥,该第一验证节点的公私密钥对中公钥可以用于对数据或信息等进行加密处理,或者,用于对第一验证节点的公私密钥对

中私钥生成的签名进行验证;该第一验证节点的公私密钥对中私钥可以用于对通过该第一验证节点的公私密钥对中公钥所加密的信息或数据进行解密处理,或者,用于对数据或信息等进行签名处理;第一验证节点可以利用国密SM2算法、对称加密算法或非对称加密算法等生成第一验证节点的公私密钥对。

[0046] 在一种实现方式中,用户可以在其客户端生成登录请求,具体为:用户可以获取区块链公布的节点信息表,该节点信息表包括区块链中每个节点的节点编号、节点的公私密钥对中公钥、节点地址等信息。用户可以随机或按照预设规则选取区块链的多个节点作为第一验证节点。根据节点信息表获取每个第一验证节点的公私密钥对中公钥,利用每个第一验证节点的公私密钥对中公钥分别对用户标识进行加密,得到每个第一验证节点对应的第一用户标识加密信息。例如,可以将所有的第一用户标识加密信息表示为数据包D(即,登录请求包括数据包D),D=[R1(ID),R2(ID),…,Rm(ID)],R1(ID)、R2(ID) …Rm(ID)表示通过m个第一验证节点的公私密钥对中公钥加密后的m个第一用户标识加密信息。其中,第一验证节点信息中还可以包括每个第一验证节点的编号和节点地址等。

[0047] 步骤S120,分别针对各第一用户标识加密信息,终端根据第一验证节点信息,向与各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求。

[0048] 其中,每个用户身份验证请求包括:第一用户标识加密信息、服务提供方的服务方标识和用户登录信息。服务方标识用于唯一标识一个服务提供方,例如,服务方标识可以为DIDs等。

[0049] 在一种实现方式中,终端可以将每个第一用户标识加密信息、服务方标识、用户登录信息拼接形成一个与该第一用户标识加密信息对应的用户身份验证请求,并将该用户身份验证请求发送与该用户身份验证请求中包括的第一用户标识加密信息对应的第一验证节点。例如,用户身份验证请求可以为dsi=[idui,idsp,h(idui,idsp)],其中,dsi为用户身份验证请求,idui为第一用户标识加密信息,idsp为服务方标识,h(idui,idsp)为用户登录信息。

[0050] 步骤S130,对应的第一验证节点利用各第一验证节点的公私密钥对中私钥对各第一用户标识加密信息进行解密处理,得到用户标识。

[0051] 其中,每个第一验证节点利用其公私密钥对中私钥对通过其公私密钥对中公钥加密得到的第一用户标识加密信息进行解密处理,得到用户标识。

[0052] 步骤S140,对应的第一验证节点对用户标识和服务方标识进行校验运算,得到校验信息,并将校验信息与用户登录信息比较,得到比较结果。

[0053] 其中,每个比较结果包括:用于指示校验信息和用户登录信息相同的第一子比较结果,或者,用于指示校验信息和用户登录信息不同的第二子比较结果。例如,第一子比较结果可以表示为yes,第二子比较结果可以表示为no。

[0054] 校验运算可以为哈希运算、循环冗余校验(Cyclic Redundancy Check,CRC)运算、MD5(Message-Digest Algorithm 5)算法等,当校验运算为哈希运算时,相应的,校验信息为用户标识和服务方标识共同的哈希值。例如,用户标识为aa/bb/cc,服务方标识为dd/ee/ff,则校验信息为用户标识+服务方标识(aa/bb/ccdd/ee/ff)的哈希值。

[0055] 在一种实现方式中,每个第一验证节点对其上的用户标识和服务方标识进行校验运算,得到校验信息,并将校验信息与用户登录信息比较,得到该第一验证节点的比较结

果。每个第一验证节点将该第一验证节点的比较结果反馈终端。

[0056] 步骤S150，响应于终端接收到的第一子比较结果的数量大于或等于第一预设数量，终端允许用户登录服务提供方所提供的应用。

[0057] 其中，第一预设数量可以设置为大于第一验证节点的数量半数的数量，例如，第一验证节点的数量为m个，m>0的正整数，则第一预设数量可以为 $\frac{m}{2}+1$ 。

[0058] 在一种实现方式中，终端接收每个第一验证节点反馈的比较结果，当在所有比较结果中，第一子比较结果的数量大于或等于第一预设数量，终端允许用户登录服务提供方所提供的应用，否则，终端拒绝用户登录服务提供方所提供的应用。

[0059] 例如，第一验证节点的数量为m个，相应的，由第一验证节点所反馈的比较结果的数量也为m个，第一预设数量为 $\frac{m}{2}+1$ 。当在m个比较结果中，第一子比较结果的数量大于或等于 $\frac{m}{2}+1$ 时，终端允许用户登录服务提供方所提供的应用。

[0060] 本公开实施例中，通过使用用户登录信息和第一用户标识加密信息实现用户登录服务提供方所提供的应用。在登录过程中，服务提供方仅获得了用户登录信息和第一用户标识加密信息，未获得用户标识，有效的避免了服务提供方之间通过用户标识共享用户信息的问题，降低了用户信息跨站泄漏的风险。另外，采用了多个第一验证节点投票的方式，极大的提升了比较结果的可靠性。

[0061] 在一个可选实施例中，登录请求还包括：第一发送时间。如图2所示，本公开实施例的基于区块链的身份信息验证方法还包括如下步骤：

[0062] 步骤S210，终端确定当前时间与第一发送时间之间的第一时间间隔。

[0063] 其中，第一发送时间可以为客户端生成登录请求时的时间戳，或者，客户端向终端发送登录请求时的时间戳。第一时间间隔可以为当前时间与第一发送时间的差值的绝对值。

[0064] 步骤S220，响应于第一时间间隔小于或等于预设时间间隔，执行分别针对各第一用户标识加密信息，终端根据第一验证节点信息，向与各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求的操作。

[0065] 其中，预设时间间隔可以根据实际情况设定。在一种实现方式中，当终端接收到客户端发送的登录请求，终端确定第一时间间隔，将第一时间间隔与预设时间间隔比较，当第一时间间隔小于或等于预设时间间隔，终端执行步骤S120以及步骤S120之后的操作；当第一时间间隔大于预设时间间隔，终端拒绝用户登录服务提供方所提供的应用。

[0066] 在一个可选实施例中，如图3所示，本公开实施例的基于区块链的身份信息验证方法还包括如下步骤：

[0067] 步骤S310，客户端利用预设算法对第一预设信息进行处理，得到第一运算结果。

[0068] 其中，用户可以根据实际需求设置第一预设信息，例如，可以将第一预设信息设置为第一发送时间。预设算法可以为哈希运算，相应的，第一运算结果为第一预设信息的哈希值。

[0069] 步骤S320，客户端获取预设验证节点数量。

[0070] 其中，用户可以在客户端预先设置预设验证节点数量，预设验证节点数量可以为

奇数。在一种实现方式中，该预设验证节点数量可以为第一验证节点的数量。

[0071] 步骤S330，客户端根据预设验证节点数量，对第一运算结果执行切分处理，得到预设验证节点数量的第一运算子结果。

[0072] 其中，可以将第一运算结果切分成预设验证节点数量的第一运算子结果，即，每个第一运算子结果为第一运算结果的一部分。

[0073] 步骤S340，对于任一第一运算子结果，客户端对第一运算子结果进行转换处理，以得到第一运算子结果对应的数值。

[0074] 其中，第一运算子结果对应的数值可以为第一运算子结果对应的十进制的数值。

[0075] 步骤S350，客户端基于区块链的节点的编号和第一运算子结果对应的数值，确定第一验证节点。

[0076] 其中，区块链的每个节点具有编号，将与第一运算子结果对应的数值相同编号的节点确定为第一验证节点。

[0077] 例如，区块链中共有10000个节点，节点的编号分别为1，2，3…1000。第一验证节点的数量为17个，则预设验证节点数量为17，将第一运算结果切分成17个的第一运算子结果，将每个16位进制的第一运算子结果转换为十进制，即得到每个第一运算子结果对应的数值，该十进制的数值即为第一运算子结果对应的数值，如，第一运算子结果对应的十进制的数值为5000，则将编号为5000的节点确定为第一验证节点。

[0078] 在一个可选实施例中，如图4所示，本公开实施例的基于区块链的身份信息验证方法还包括如下步骤：

[0079] 步骤S410，客户端根据区块链的节点故障率，确定区块链的节点可靠概率。

[0080] 其中，节点故障率可以为区块链中出现故障的节点的比率。节点可靠概率可以为区块链中正常工作的节点的比率，例如，可以通过$p=(1-\alpha)$得到节点可靠概率，其中，p为节点可靠概率，α为节点故障率。节点故障率可以通对区块链的性能测试得到。

[0081] 步骤S420，客户端根据节点可靠概率，基于预设验证成功概率模型和预设模型条件，确定预设验证节点数量。

[0082] 其中，该预设验证节点数量为奇数。

[0083] 在一种实现方式中，预设验证成功概率模型可以为式(1)；预设模型条件可以为$(1-s)\leqslant 0.3\%$；

[0084] $$s=\sum_{i=\frac{m}{2}+1}^{m}p^{i}(1-p)^{m-i} \qquad (1)$$；

[0085] 其中，s为事件成功率，即节点的正确处理数据的成功率，在本实施例中可以理解为对用户登录信息成功验证的成功率，或者，是用户登录信息生成的成功率。m为预设验证节点数量，p为节点可靠概率，i为区块链的节点数量。

[0086] 当事件小于或等于0.3%时，即在满足预设模型条件时，该事件被认为是可能的事件，因此，只需在预设模型条件为$(1-s)\leqslant 0.3\%$下，根据预设验证成功概率模型式(1)，计算m的最小奇数即可，即m的最小奇数即为预设验证节点数量。

[0087] 在一个可选实施例中，如图5所示，本公开实施例的基于区块链的身份信息验证方法还包括如下步骤：

[0088] 步骤S510，终端接收客户端发送的注册请求。

[0089] 其中,该注册请求包括:至少一个第二用户标识加密信息和第二验证节点信息;该至少一个第二用户标识加密信息中的各第二用户标识加密信息,利用与第二用户标识加密信息对应的第二验证节点的公私密钥对中公钥加密用户标识得到;第二验证节点信息包括各第二用户标识加密信息对应的第二验证节点。

[0090] 可以确定利用第二验证节点的公私密钥对中公钥加密用户标识得到的第二用户标识加密信息与该第二验证节点具有对应关系。可以将用于注册用户登录信息的区块链的节点称为第二验证节点。

[0091] 每个第二验证节点的公私密钥对包括公钥和私钥,该第二验证节点的公私密钥对中公钥可以用于对数据或信息等进行加密处理,或者,用于对第二验证节点的公私密钥对中私钥生成的签名进行验证;该第二验证节点的公私密钥对中私钥可以用于对通过该第二验证节点的公私密钥对中公钥所加密的信息或数据进行解密处理,或者,用于对数据或信息等进行签名处理;第二验证节点可以利用国密SM2算法、对称加密算法或非对称加密算法等生成第二验证节点的公私密钥对。在一种实现方式中,用户可以随机或按照预设规则从节点信息表中,选取区块链的多个节点作为第二验证节点。根据节点信息列表获取每个第二验证节点的公私密钥对中公钥,利用每个第二验证节点的公私密钥对中公钥分别对用户标识进行加密,得到每个第二验证节点对应的第二用户标识加密信息。其中,第二验证节点信中还可以包括每个第二验证节点的编号和节点地址。

[0092] 步骤S520,分别针对各第二用户标识加密信息,终端根据第二验证节点信息,向与各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求。

[0093] 其中,每个登录信息生成请求包括:第二用户标识加密信息和服务方标识。

[0094] 在一种实现方式中,终端可以将每个第二用户标识加密信息和服务方标识拼接形成一个登录信息生成请求,并将该登录信息生成请求发送与该登录信息生成请求中包括的第二用户标识加密信息对应的第二验证节点。例如,每个登录信息生成请求可以为Dsi=[IDui,idsp],其中,Dsi为登录信息生成请求,IDui为第二用户标识加密信息,idsp为服务方标识。

[0095] 步骤S530,对应的第二验证节点利用各第二验证节点的公私密钥对中私钥对各第二用户标识加密信息进行解密处理,得到用户标识。

[0096] 其中,每个第二验证节点利用其公私密钥对中私钥对通过其公私密钥对中公钥加密得到的第二用户标识加密信息进行解密处理,得到用户标识。

[0097] 步骤S540,对应的第二验证节点对用户标识和服务方标识进行校验运算,得到校验信息,并将校验信息反馈终端。

[0098] 其中,校验运算可为哈希运算,相应的,校验信息为用户标识和服务方标识共同的哈希值。

[0099] 在一种实现方式中,每个第二验证节点对其上的用户标识和服务方标识进行校验运算,得到该第二验证节点的校验信息。每个第二验证节点将该第二验证节点的校验信息反馈终端。

[0100] 步骤S550,响应于终端接收到的相同的校验信息的数量大于或等于第二预设数量,终端将相同的数量大于或等于第二预设数量的校验信息确定为用户登录信息。

[0101] 其中,第二预设数量可以设置为大于第二验证节点的数量半数的数量,例如,第二

验证节点的数量为m个，则第二预设数量可以为$\frac{m}{2}+1$。

[0102] 在一种实现方式中，终端接收每个第二验证节点反馈的校验信息，当在所有校验信息中，相同的校验信息的数量大于或等于第二预设数量时，将该校验信息确定为用户登录信息。终端可以将用户登录信息发送客户端，或将用户登录信息存储在区块链中，并将区块链反馈的用户登录信息的存储地址发送客户端。

[0103] 例如，第二验证节点的数量为m个，相应的，由第二验证节点反馈的校验信息的数量也为m个，第二预设数量为$\frac{m}{2}+1$。当在m个校验信息中有大于或等于$\frac{m}{2}+1$个相同的校验信息时，则将该相同的校验信息中的任意一个校验信息确定为用户登录信息。

[0104] 在一个可选实施例中，注册请求还包括：第二发送时间；如图6所示，本公开实施例的基于区块链的身份信息验证方法还包括如下步骤：

[0105] 步骤S610，终端确定当前时间与第二发送时间之间的第二时间间隔。

[0106] 其中，第二发送时间可以为客户端生成注册请求时的时间戳，或者，客户端向终端发送注册请求时的时间戳。第二时间间隔可以为当前时间与第二发送时间的差值的绝对值。

[0107] 步骤S620，响应于第二时间间隔小于或等于预设时间间隔，执行分别针对各第二用户标识加密信息，终端根据第二验证节点信息，向与各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求的操作。

[0108] 在一种实现方式中，当终端接收到客户端发送的注册请求，终端确定第二时间间隔，并将第二时间间隔与预设时间间隔比较，当第二时间间隔小于或等于预设时间间隔，终端执行步骤S520以及步骤S520之后的操作；当第二时间间隔大于预设时间间隔，终端结束注册操作，并向客户端发送注册失败消息。

[0109] 在一个可选实施例中，如图7所示，本公开实施例的基于区块链的身份信息验证方法还包括如下步骤：

[0110] 步骤S710，客户端利用预设算法对第二预设信息进行处理，得到第二运算结果。

[0111] 其中，用户可以根据实际需求设置第二预设信息，例如，可以将第二预设信息设置为第二发送时间。预设算法可以为哈希运算，相应的，第二运算结果可以为第二预设信息的哈希值。

[0112] 步骤S720，客户端获取预设验证节点数量。

[0113] 在一种实现方式中，该预设验证节点数量可以为第二验证节点的数量。第一验证节点的数量和第二验证节点的数量可以相同。

[0114] 步骤S730，客户端根据预设验证节点数量，对第二运算结果执行切分处理，得到预设验证节点数量的第二运算子结果。

[0115] 其中，可以将第二运算结果切分成预设验证节点数量的第二运算子结果，即，每个第二运算子结果为第二运算结果的一部分。

[0116] 步骤S740，对于任一第二运算子结果，客户端对第二运算子结果进行转换处理，以得到第二运算子结果对应的数值。

[0117] 其中，第二运算子结果对应的数值可以为第二运算子结果对应的十进制的数值。

[0118] 步骤S750，客户端基于区块链的节点的编号和第二运算子结果对应的数值，确定第二验证节点。

[0119] 其中，将与第二运算子结果对应的数值相同编号的节点确定为第二验证节点。

[0120] 例如，区块链中共有10000个节点，节点的编号分别为1，2，3…1000。预设验证节点数量为17，则预设验证节点数量可以为17，可以将第二运算结果切分成17个的第二运算子结果，将每个16位进制的第二运算子结果转换为十进制，即得到每个第二运算子结果对应的数值，该十进制的数值即为第二运算子结果对应的数值，如，第二运算子结果对应的十进制的数值为6000，则将编号为6000的节点确定为第二验证节点。

[0121] 图8示出了本申请实施例中基于区块链的身份信息验证方法的交互示意图。

[0122] 如图8所示，用户获取用户标识的流程可以包括：

[0123] 步骤1，用户可以向身份发布方申请用户标识，其中，身份发布方可以为权威的身份认证机构，例如，身份发布方可以为工商局或公安局等。

[0124] 步骤2，身份发布方向用户颁发可验证声明(Verifiable Credential，VC)和用户的公私密钥对，该可验证声明包括用户标识和用户的公私密钥对中公钥，并且身份发布方将用户的可验证声明存储至区块链中，用户的公私密钥对包括公钥和私钥；同时用户的客户端可以向区块链提供用户证明信息，以使用户的客户端通过区块链的认证，可对用户服务，用户证明信息可以为用户标识、用户的可验证声明等。

[0125] 如图8所示，用户注册登录服务提供方所提供的应用时所需的用户登录信息的流程可以包括：

[0126] 1，在客户端，确定第二验证节点信息、至少一个第二用户标识加密信息和第二发送时间，由第二验证节点信息、至少一个第二用户标识加密信息和第二发送时间形成注册请求，并向终端发送注册请求。

[0127] 2，在终端，生成至少一个第二用户标识加密信息中的各第二用户标识加密信息对应的登录信息生成请求，并将各第二用户标识加密信息对应的登录信息生成请求发送各第二用户标识加密信息对应的第二验证节点，其中，N1，N2，N3，N4，N5，N6，N7，N8，N9，N10，N11分别表示区块链的第一验证节点和/或第二验证节点。

[0128] 3，各第二验证节点分别利用其公私密钥对中私钥对第二用户标识加密信息进行解密处理，得到用户标识，并对用户标识和服务方标识拼接后进行哈希运算，得到校验信息，并将校验信息发送终端。

[0129] 4，当终端接收到相同的校验信息的数量大于或等于第二预设数量，终端将相同的数量大于或等于第二预设数量的校验信息确定为用户登录信息，并将用户登录信息发送客户端。

[0130] 如图8所示，用户登录服务提供方所提供的应用的流程可以包括：

[0131] S1，在客户端，确定用户登录信息、第一验证节点信息、至少一个第一用户标识加密信息和第一发送时间，由用户登录信息、第一验证节点信息至少一个第一用户标识加密信息和第二发送时间形成登录请求，并向终端发送登录请求。

[0132] S2，在终端，生成至少一个第一用户标识加密信息中的各第一用户标识加密信息对应的用户身份验证请求，并将各第一用户标识加密信息对应的用户身份验证请求发送各第一用户标识加密信息对应的第一验证节点。

[0133] S3,各第一验证节点分别利用其公私密钥对中私钥对第一用户标识加密信息进行解密处理,得到用户标识,对用户标识和服务方标识拼接后进行哈希运算,得到校验信息,并将校验信息与用户登录信息比较,得到比较结果,将比较结果发送终端。

[0134] S4,当指示校验信息和用户登录信息相同的比较结果的数量大于或等于第一预设数量,终端允许用户登录服务提供方所提供的应用。

[0135] 图9是本公开一示例性实施例提供的基于区块链的身份信息验证装置的结构示意图。如图9所示,本实施例提供的装置包括:

[0136] 第一接收模块810,用于服务提供方的终端接收用户的客户端发送的登录请求,其中,所述登录请求包括:用户登录信息、至少一个第一用户标识加密信息和第一验证节点信息;所述至少一个第一用户标识加密信息中的各第一用户标识加密信息,利用与所述第一用户标识加密信息对应的区块链的第一验证节点的公私密钥对中公钥加密所述用户的用户标识得到;所述第一验证节点信息包括各第一用户标识加密信息对应的第一验证节点;

[0137] 第一发送模块820,用于分别针对所述各第一用户标识加密信息,所述终端根据所述第一验证节点信息,向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求,其中,所述用户身份验证请求包括:所述第一用户标识加密信息、所述服务提供方的服务方标识和所述用户登录信息;

[0138] 第一解密模块830,用于对应的第一验证节点利用所述各第一验证节点的公私密钥对中私钥对所述各第一用户标识加密信息进行解密处理,得到所述用户标识;

[0139] 比较模块840,用于所述对应的第一验证节点对所述用户标识和所述服务方标识进行校验运算,得到校验信息,并将所述校验信息与所述用户登录信息比较,得到比较结果,其中,所述比较结果包括:用于指示所述校验信息和所述用户登录信息相同的第一子比较结果,或者,用于指示所述校验信息和所述用户登录信息不同的第二子比较结果;

[0140] 验证模块850,用于响应于所述终端接收到的所述第一子比较结果的数量大于或等于第一预设数量,所述终端允许所述用户登录所述服务提供方所提供的应用。

[0141] 在一些可选的实施例中,所述登录请求还包括:第一发送时间;本实施例中的装置还包括:

[0142] 第一时间间隔确定模块,用于所述终端确定当前时间与所述第一发送时间之间的第一时间间隔;

[0143] 第一时效判断模块,用于响应于所述第一时间间隔小于或等于预设时间间隔,执行所述分别针对所述各第一用户标识加密信息,所述终端根据所述第一验证节点信息,向与所述各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求的操作。

[0144] 在一些可选的实施例中,本实施例中的装置还包括:

[0145] 第一运算模块,用于所述客户端利用预设算法对第一预设信息进行处理,得到第一运算结果;

[0146] 第一获取子模块,用于所述客户端获取预设验证节点数量;

[0147] 第一切分模块,用于所述客户端根据所述预设验证节点数量,对所述第一运算结果执行切分处理,得到所述预设验证节点数量的第一运算子结果;

[0148] 第一转换模块,用于对于任一第一运算子结果,所述客户端对所述第一运算子结果进行转换处理,以得到所述第一运算子结果对应的数值;

[0149] 第一验证节点确定模块，用于所述客户端基于所述区块链的节点的编号和所述第一运算子结果对应的数值，确定所述第一验证节点。

[0150] 在一些可选的实施例中，本实施例中的装置还包括：

[0151] 节点可靠概率确定模块，用于所述客户端根据所述区块链的节点故障率，确定所述区块链的节点可靠概率；

[0152] 预设验证节点数量确定模块，用于所述客户端根据所述节点可靠概率，基于预设验证成功概率模型和预设模型条件，确定所述预设验证节点数量。

[0153] 在一些可选的实施例中，本实施例中的装置还包括：

[0154] 第二接收模块，用于所述终端接收所述客户端发送的注册请求，其中，所述注册请求包括：至少一个第二用户标识加密信息和第二验证节点信息；所述至少一个第二用户标识加密信息中的各第二用户标识加密信息，利用与所述第二用户标识加密信息对应的第二验证节点的公私密钥对中公钥加密所述用户标识得到；所述第二验证节点信息包括各第二用户标识加密信息对应的第二验证节点；

[0155] 第二发送模块，用于分别针对所述各第二用户标识加密信息，所述终端根据所述第二验证节点信息，向与所述各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求，其中，所述登录信息生成请求包括：所述第二用户标识加密信息和所述服务方标识；

[0156] 第二解密模块，用于对应的第二验证节点利用所述各第二验证节点的公私密钥对中私钥对所述各第二用户标识加密信息进行解密处理，得到所述用户标识；

[0157] 校验模块，用于所述对应的第二验证节点对所述用户标识和所述服务方标识进行校验运算，得到校验信息，并将所述校验信息反馈所述终端；

[0158] 用户登录信息确定模块，用于响应于所述终端接收到的相同的校验信息的数量大于或等于第二预设数量，所述终端将相同的数量大于或等于所述第二预设数量的所述校验信息确定为所述用户登录信息。

[0159] 在一些可选的实施例中，所述注册请求还包括：第二发送时间；本实施例中的装置还包括：

[0160] 第二时间间隔确定模块，用于所述终端确定当前时间与所述第二发送时间之间的第二时间间隔；

[0161] 第二时效判断模块，用于响应于所述第二时间间隔小于或等于预设时间间隔，执行所述分别针对所述各第二用户标识加密信息，所述终端根据所述第二验证节点信息，向与所述各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求的操作。

[0162] 在一些可选的实施例中，本实施例中的装置还包括：

[0163] 第二运算模块，用于所述客户端利用预设算法对第二预设信息进行处理，得到第二运算结果；

[0164] 第二获取子模块，用于所述客户端获取预设验证节点数量；

[0165] 第二切分模块，用于所述客户端根据所述预设验证节点数量，对所述第二运算结果执行切分处理，得到所述预设验证节点数量的第二运算子结果；

[0166] 第二转换模块，用于对于任一第二运算子结果，所述客户端对所述第二运算子结果进行转换处理，以得到所述第二运算子结果对应的数值；

[0167] 第二验证节点确定模块，用于所述客户端基于所述区块链的节点的编号和所述第二运算子结果对应的数值，确定所述第二验证节点。

[0168] 另外，本公开实施例还提供了一种电子设备，包括：

[0169] 存储器，用于存储计算机程序；

[0170] 处理器，用于执行所述存储器中存储的计算机程序，且所述计算机程序被执行时，实现本公开上述任一实施例所述的基于区块链的身份信息验证方法。

[0171] 图10为本公开电子设备一个应用实施例的结构示意图。下面，参考图10来描述根据本公开实施例的电子设备。该电子设备可以是第一设备和第二设备中的任一个或两者、或与它们独立的单机设备，该单机设备可以与第一设备和第二设备进行通信，以从它们接收所采集到的输入信号。

[0172] 如图10所示，电子设备包括一个或多个处理器和存储器。

[0173] 处理器可以是中央处理单元(CPU)或者具有数据处理能力和/或指令执行能力的其他形式的处理单元，并且可以控制电子设备中的其他组件以执行期望的功能。

[0174] 存储器可以包括一个或多个计算机程序产品，所述计算机程序产品可以包括各种形式的计算机可读存储介质，例如易失性存储器和/或非易失性存储器。所述易失性存储器例如可以包括随机存取存储器(RAM)和/或高速缓冲存储器(cache)等。所述非易失性存储器例如可以包括只读存储器(ROM)、硬盘、闪存等。在所述计算机可读存储介质上可以存储一个或多个计算机程序指令，处理器可以运行所述程序指令，以实现上文所述的本公开的各个实施例的基于区块链的身份信息验证方法以及/或者其他期望的功能。

[0175] 在一个示例中，电子设备还可以包括：输入装置和输出装置，这些组件通过总线系统和/或其他形式的连接机构(未示出)互连。

[0176] 此外，该输入装置还可以包括例如键盘、鼠标等等。

[0177] 该输出装置可以向外部输出各种信息，包括确定出的距离信息、方向信息等。该输出装置可以包括例如显示器、扬声器、打印机、以及通信网络及其所连接的远程输出设备等等。

[0178] 当然，为了简化，图10中仅示出了该电子设备中与本公开有关的组件中的一些，省略了诸如总线、输入/输出接口等等的组件。除此之外，根据具体应用情况，电子设备还可以包括任何其他适当的组件。

[0179] 除了上述方法和设备以外，本公开的实施例还可以是计算机程序产品，其包括计算机程序指令，所述计算机程序指令在被处理器运行时使得所述处理器执行本说明书上述部分中描述的根据本公开各种实施例的基于区块链的身份信息验证方法中的步骤。

[0180] 所述计算机程序产品可以以一种或多种程序设计语言的任意组合来编写用于执行本公开实施例操作的程序代码，所述程序设计语言包括面向对象的程序设计语言，诸如Java、C++等，还包括常规的过程式程序设计语言，诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。

[0181] 此外，本公开的实施例还可以是计算机可读存储介质，其上存储有计算机程序指令，所述计算机程序指令在被处理器运行时使得所述处理器执行本说明书上述部分中描述

的根据本公开各种实施例的基于区块链的身份信息验证方法中的步骤。

[0182] 所述计算机可读存储介质可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以包括但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0183] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0184] 以上结合具体实施例描述了本公开的基本原理，但是，需要指出的是，在本公开中提及的优点、优势、效果等仅是示例而非限制，不能认为这些优点、优势、效果等是本公开的各个实施例必须具备的。另外，上述公开的具体细节仅是为了示例的作用和便于理解的作用，而非限制，上述细节并不限制本公开为必须采用上述具体的细节来实现。

[0185] 本说明书中各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同或相似的部分相互参见即可。对于系统实施例而言，由于其与方法实施例基本对应，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0186] 本公开中涉及的器件、装置、设备、系统的方框图仅作为例示性的例子并且不意图要求或暗示必须按照方框图示出的方式进行连接、布置、配置。如本领域技术人员将认识到的，可以按任意方式连接、布置、配置这些器件、装置、设备、系统。诸如“包括”、“包含”、“具有”等等的词语是开放性词汇，指“包括但不限于”，且可与其互换使用。这里所使用的词汇“或”和“和”指词汇“和/或”，且可与其互换使用，除非上下文明确指示不是如此。这里所使用的词汇“诸如”指词组“诸如但不限于”，且可与其互换使用。

[0187] 可能以许多方式来实现本公开的方法和装置。例如，可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本公开的方法和装置。用于所述方法的步骤的上述顺序仅是为了进行说明，本公开的方法的步骤不限于以上具体描述的顺序，除非以其它方式特别说明。此外，在一些实施例中，还可将本公开实施为记录在记录介质中的程序，这些程序包括用于实现根据本公开的方法的机器可读指令。因而，本公开还覆盖存储用于执行根据本公开的方法的程序的记录介质。

[0188] 还需要指出的是，在本公开的装置、设备和方法中，各部件或各步骤是可以分解和/或重新组合的。这些分解和/或重新组合应视为本公开的等效方案。

[0189] 提供所公开的方面的以上描述以使本领域的任何技术人员能够做出或者使用本公开。对这些方面的各种修改对于本领域技术人员而言是非常显而易见的，并且在此定义的一般原理可以应用于其他方面而不脱离本公开的范围。因此，本公开不意图被限制到在此示出的方面，而是按照与在此公开的原理和新颖的特征一致的最宽范围。

[0190] 为了例示和描述的目的已经给出了以上描述。此外，此描述不意图将本公开的实施例限制到在此公开的形式。尽管以上已经讨论了多个示例方面和实施例，但是本领域技

术人员将认识到其某些变型、修改、改变、添加和子组合。

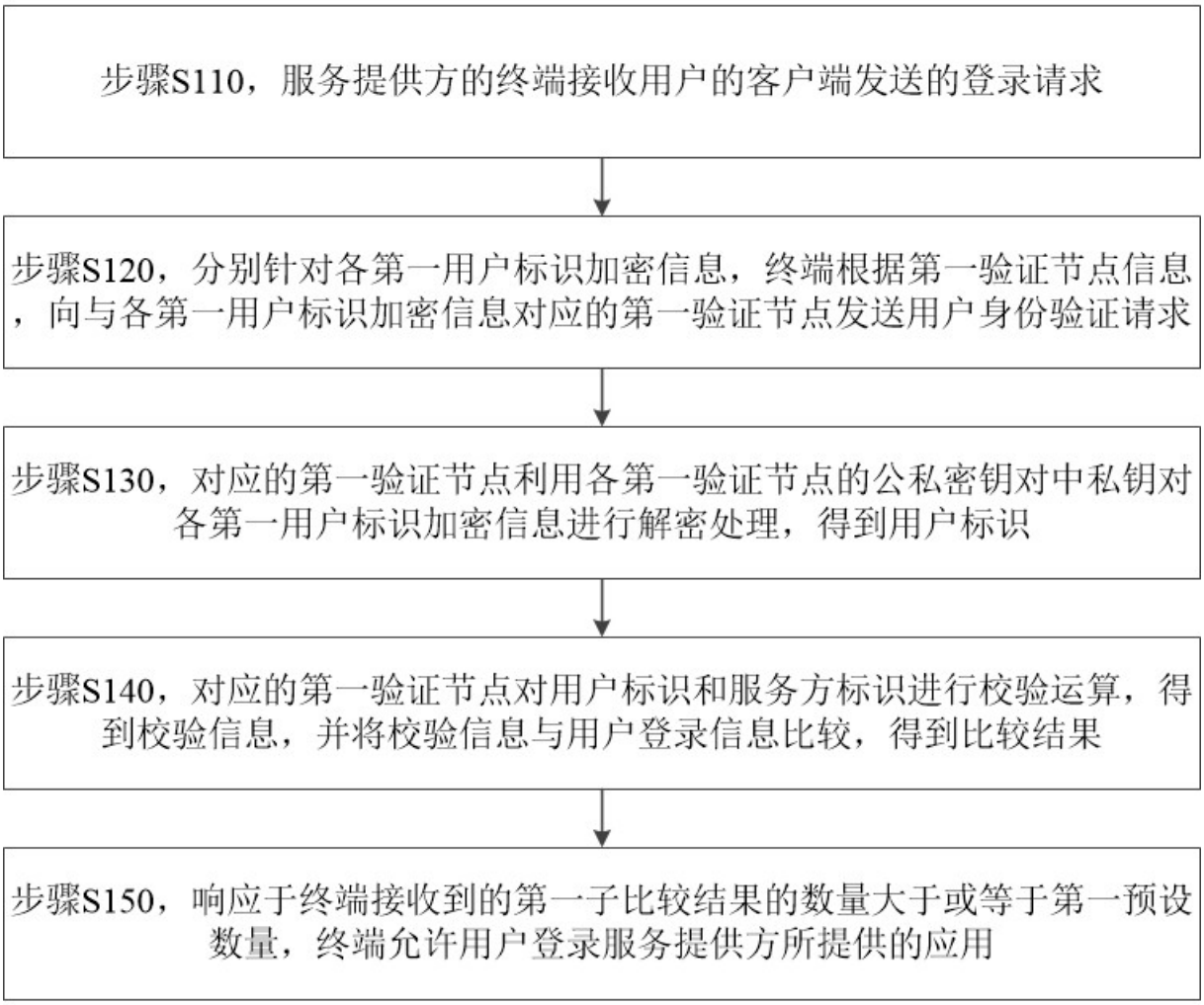

步骤S110，服务提供方的终端接收用户的客户端发送的登录请求
步骤S120，分别针对各第一用户标识加密信息，终端根据第一验证节点信息，向与各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求
步骤S130，对应的第一验证节点利用各第一验证节点的公私密钥对中私钥对各第一用户标识加密信息进行解密处理，得到用户标识
步骤S140，对应的第一验证节点对用户标识和服务方标识进行校验运算，得到校验信息，并将校验信息与用户登录信息比较，得到比较结果
步骤S150，响应于终端接收到的第一子比较结果的数量大于或等于第一预设数量，终端允许用户登录服务提供方所提供的应用

图1

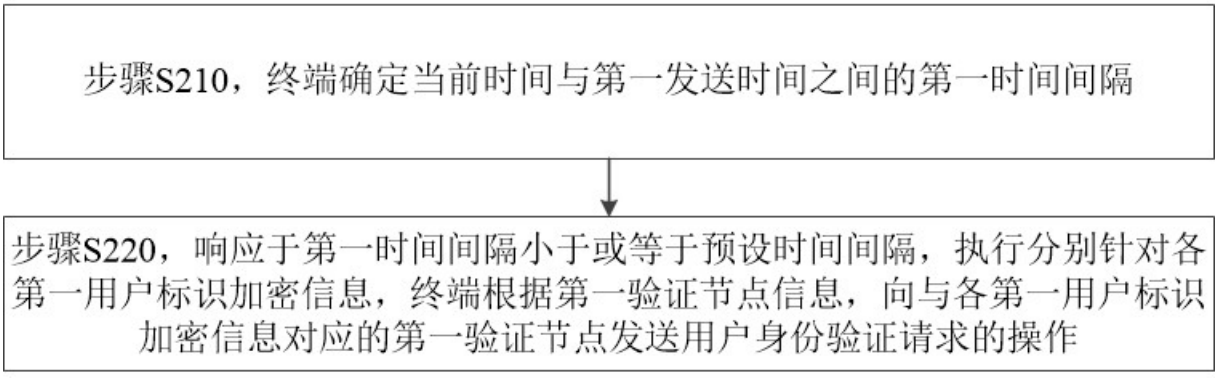

步骤S210，终端确定当前时间与第一发送时间之间的第一时间间隔
步骤S220，响应于第一时间间隔小于或等于预设时间间隔，执行分别针对各第一用户标识加密信息，终端根据第一验证节点信息，向与各第一用户标识加密信息对应的第一验证节点发送用户身份验证请求的操作

图2

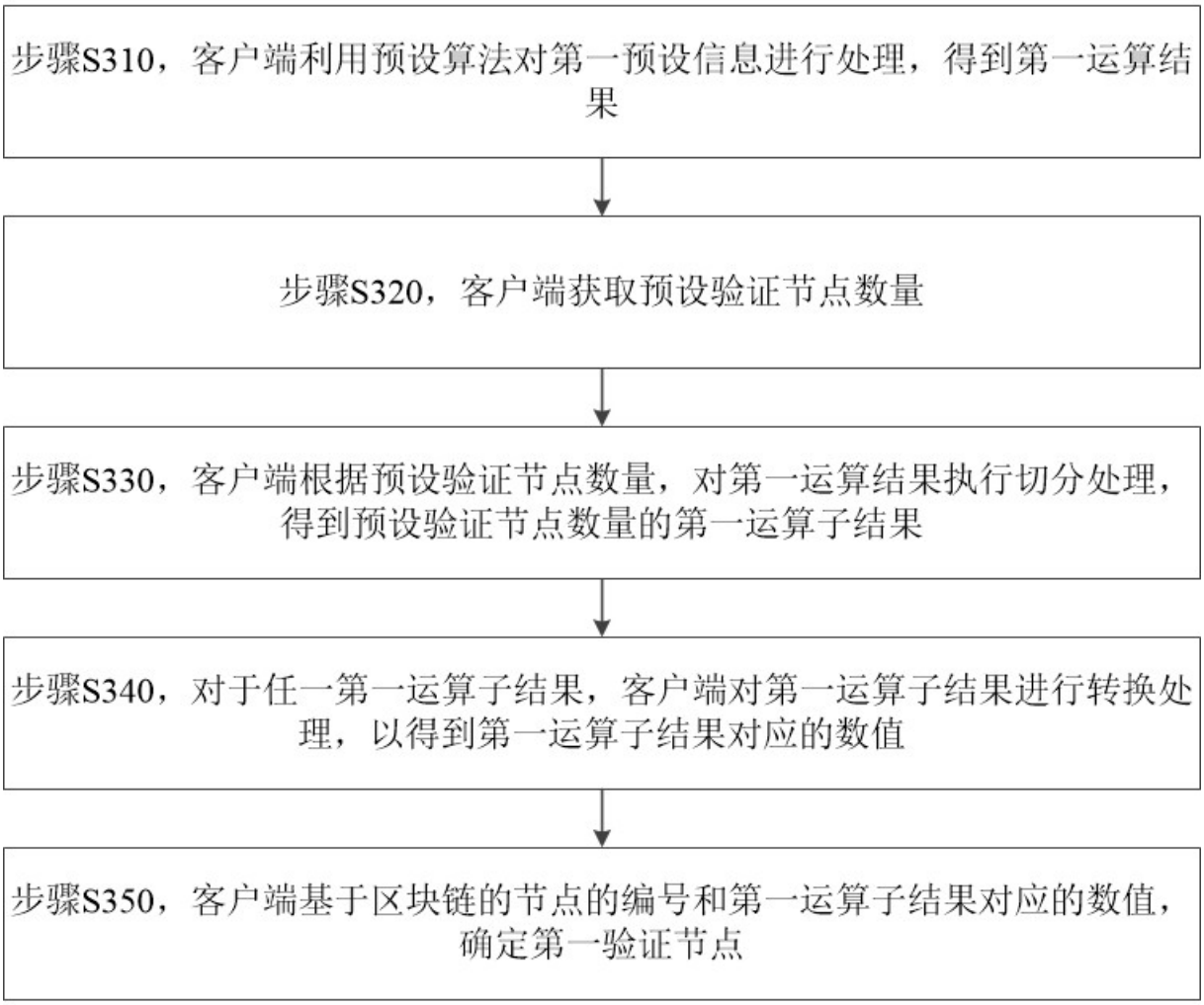

步骤S310，客户端利用预设算法对第一预设信息进行处理，得到第一运算结果
步骤S320，客户端获取预设验证节点数量
步骤S330，客户端根据预设验证节点数量，对第一运算结果执行切分处理，得到预设验证节点数量的第一运算子结果
步骤S340，对于任一第一运算子结果，客户端对第一运算子结果进行转换处理，以得到第一运算子结果对应的数值
步骤S350，客户端基于区块链的节点的编号和第一运算子结果对应的数值，确定第一验证节点

图3

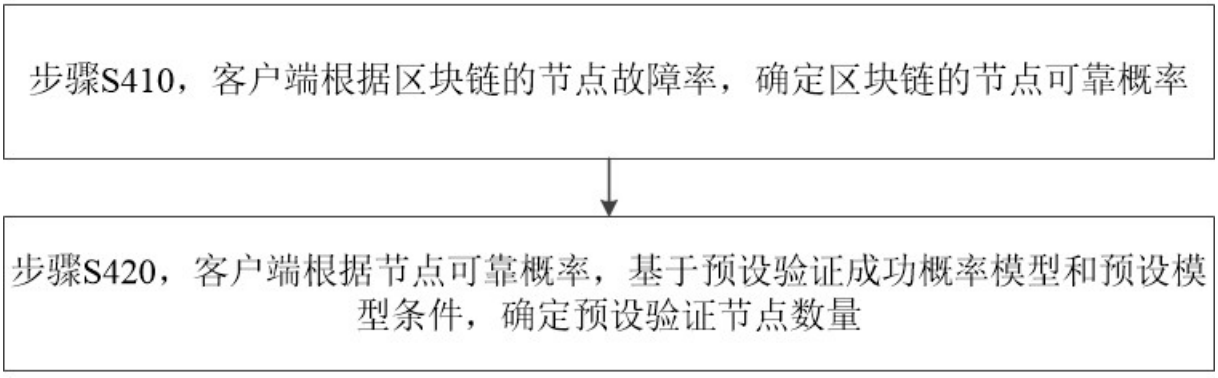

步骤S410，客户端根据区块链的节点故障率，确定区块链的节点可靠概率
步骤S420，客户端根据节点可靠概率，基于预设验证成功概率模型和预设模型条件，确定预设验证节点数量

图4

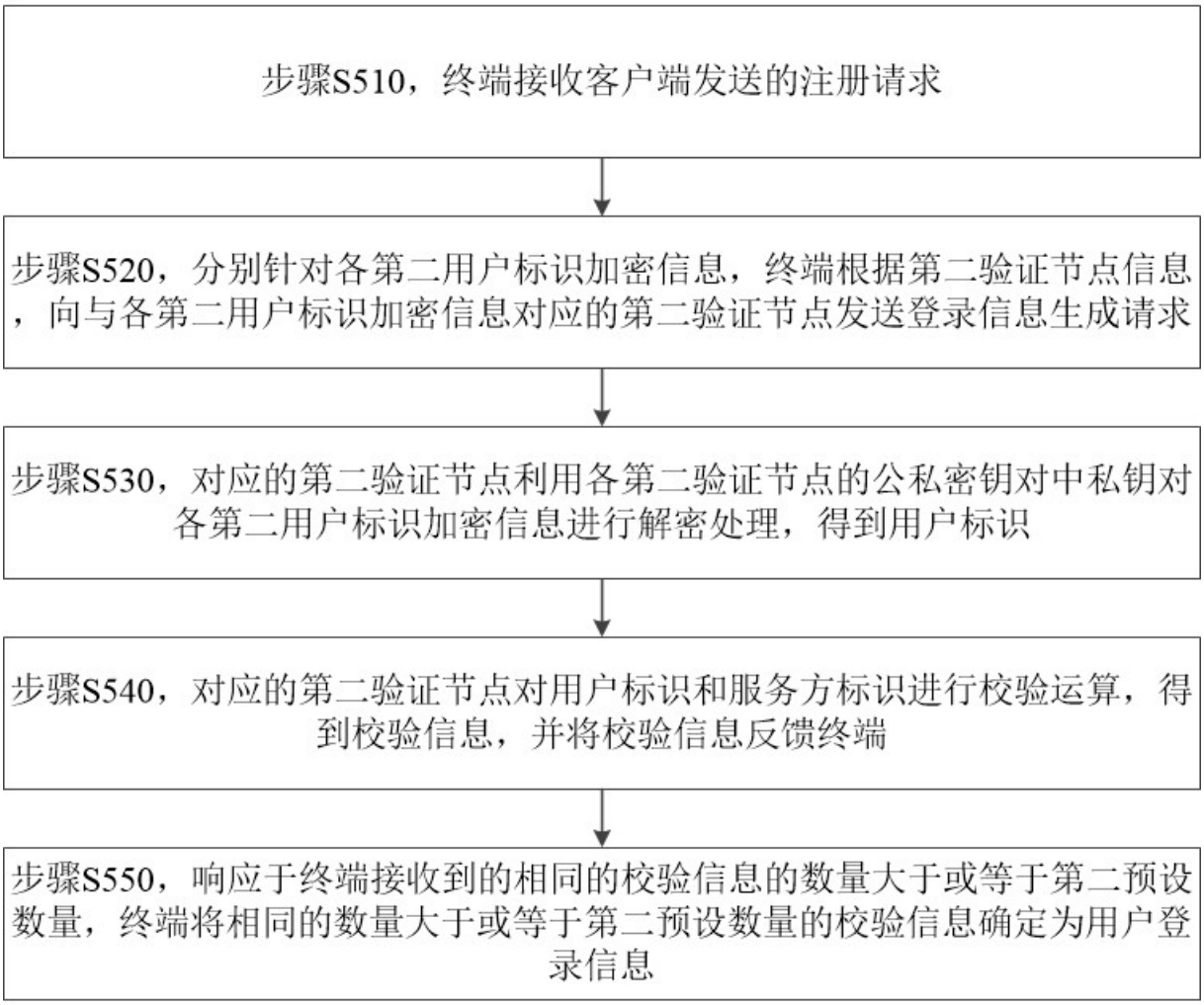

步骤S510，终端接收客户端发送的注册请求
步骤S520，分别针对各第二用户标识加密信息，终端根据第二验证节点信息，向与各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求
步骤S530，对应的第二验证节点利用各第二验证节点的公私密钥对中私钥对各第二用户标识加密信息进行解密处理，得到用户标识
步骤S540，对应的第二验证节点对用户标识和服务方标识进行校验运算，得到校验信息，并将校验信息反馈终端
步骤S550，响应于终端接收到的相同的校验信息的数量大于或等于第二预设数量，终端将相同的数量大于或等于第二预设数量的校验信息确定为用户登录信息

图5

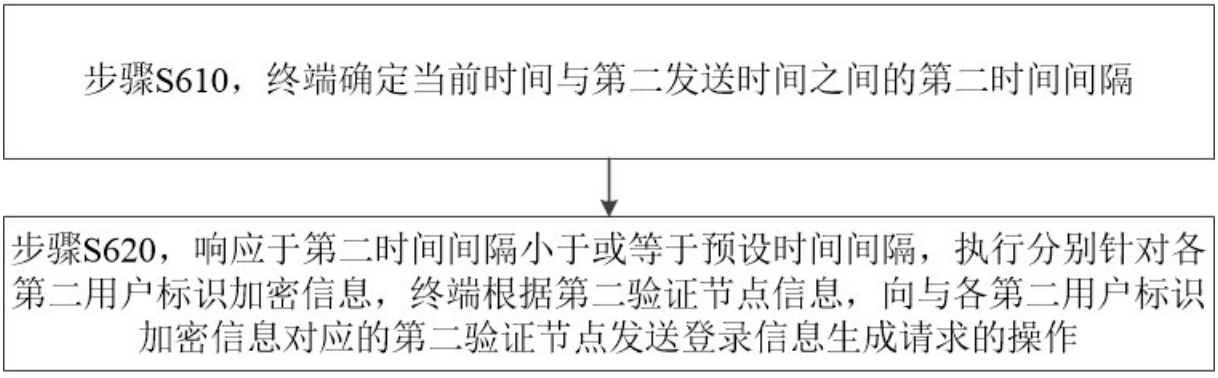

步骤S610，终端确定当前时间与第二发送时间之间的第二时间间隔
步骤S620，响应于第二时间间隔小于或等于预设时间间隔，执行分别针对各第二用户标识加密信息，终端根据第二验证节点信息，向与各第二用户标识加密信息对应的第二验证节点发送登录信息生成请求的操作

图6

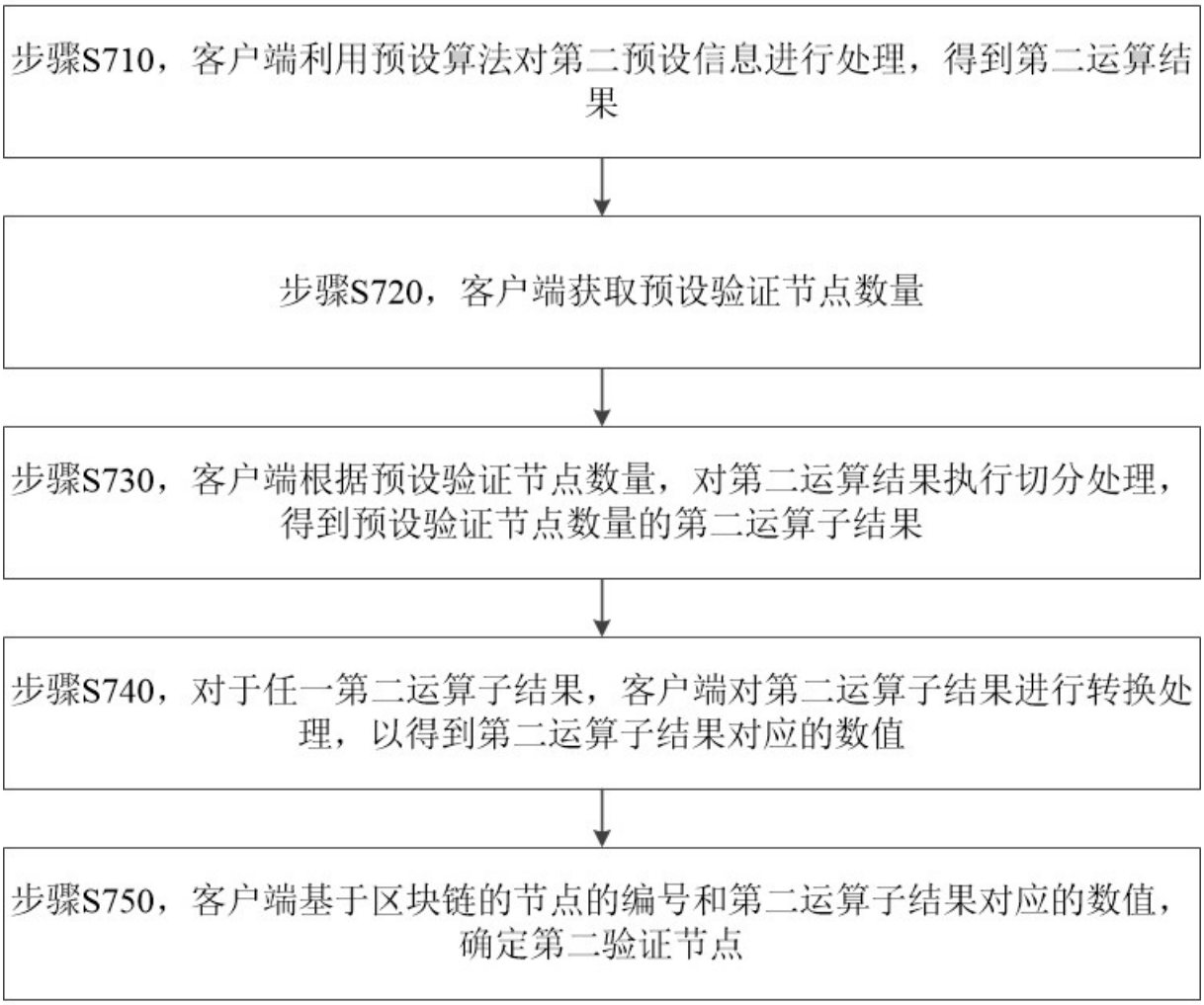

步骤S710，客户端利用预设算法对第二预设信息进行处理，得到第二运算结果
步骤S720，客户端获取预设验证节点数量
步骤S730，客户端根据预设验证节点数量，对第二运算结果执行切分处理，得到预设验证节点数量的第二运算子结果
步骤S740，对于任一第二运算子结果，客户端对第二运算子结果进行转换处理，以得到第二运算子结果对应的数值
步骤S750，客户端基于区块链的节点的编号和第二运算子结果对应的数值，确定第二验证节点

图7

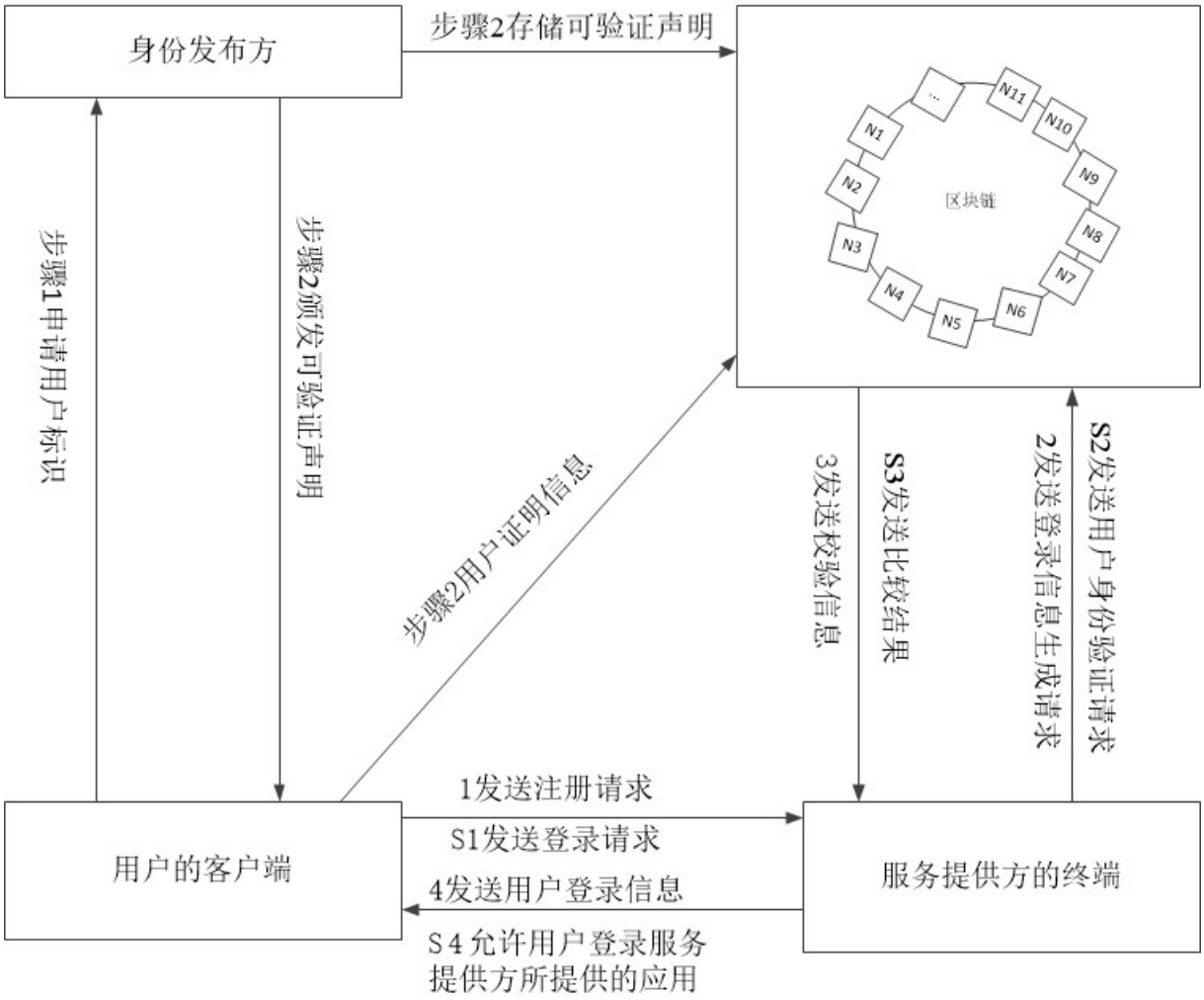

身份发布方
步骤2存储可验证声明
区块链
N1
N2
N3
N4
N5
N6
N7
N8
N9
N10
N11
...
步骤1申请用户标识
步骤2颁发可验证声明
步骤2用户证明信息
3发送校验信息
S3发送比较结果
2发送登录信息生成请求
S2发送用户身份验证请求
1发送注册请求
S1发送登录请求
4发送用户登录信息
S4允许用户登录服务提供方所提供的应用
用户的客户端
服务提供方的终端

图8

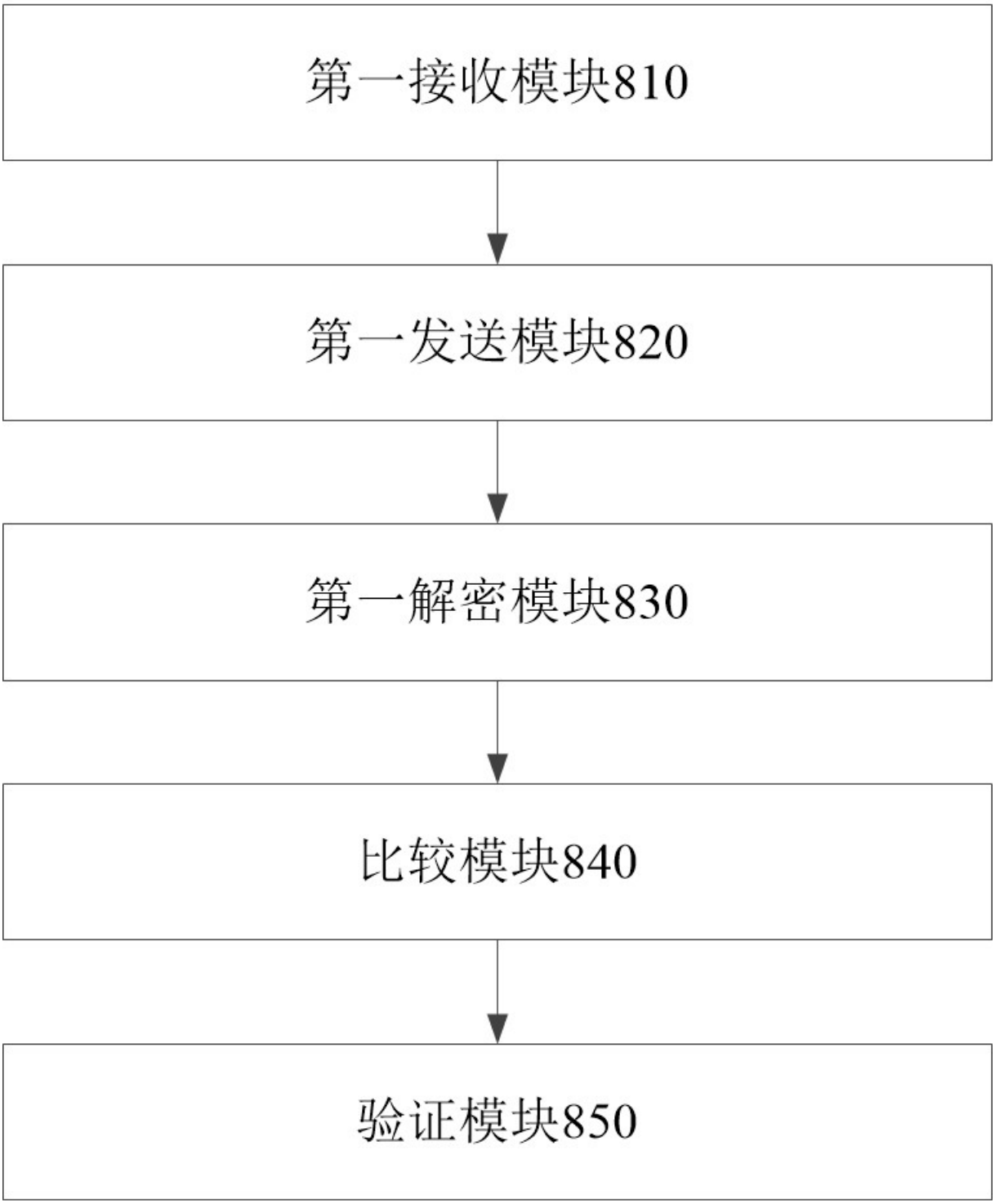


图9

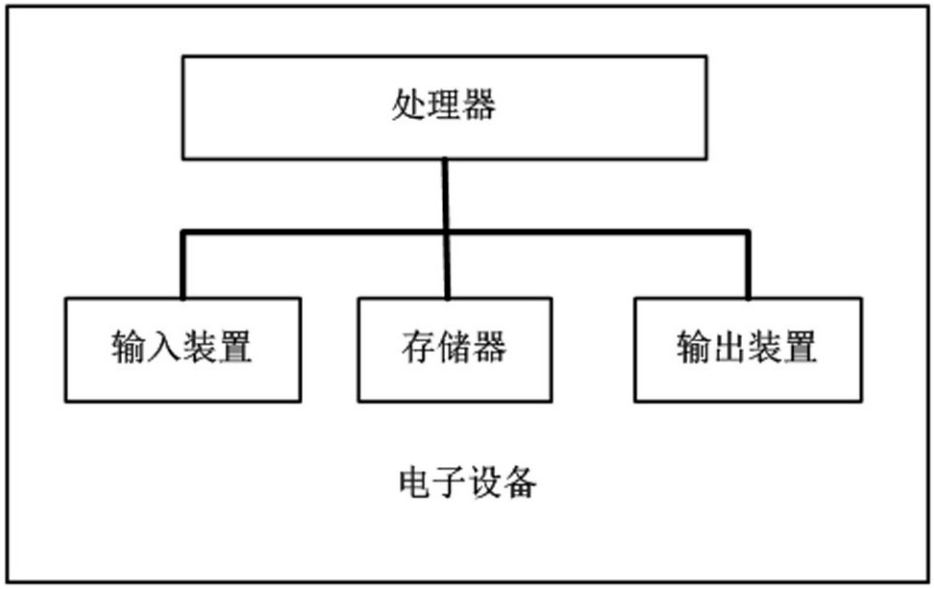


图10