

基于区块链的 SDP 访问控制方法及系统

相关申请的交叉引用

本申请基于申请号为 202110001453.6、申请日为 2021 年 01 月 04 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及网络安全技术领域，具体涉及一种基于区块链的 SDP 访问控制方法及系统。

背景技术

软件定义边界（Software Defined Perimeter，SDP），目的在于使应用程序所有者能够在需要时部署边界安全，以便将服务与不安全的网络隔离开来。SDP 使用应用所有者可控的逻辑组件取代了物理设备，只有在设备认证和身份认证之后，SDP 才允许访问应用基础设施。

参见图 1，SDP 包含两部分：SDP 主机和 SDP 控制器。SDP 主机可以创建连接或者接受连接。SDP 控制器（Controller）主要进行主机认证和策略下发。SDP 主机和 SDP 控制器之间通过一个安全的控制信道进行交互。SDP 主机又分为 SDP 连接发起主机（IH）和 SDP 连接接受主机（AH）。

SDP 改变了传统的网站连接方式。在传统的连接中，客户端需要建立与服务器端的连接，这一步骤使服务端暴露在公网中，若服务端有漏洞，则有可能被利用；用户通过登录页面输入用户名和密码，该方式有可能使用户名和密码被窃取；另外，除用户名和密码外还可使用多因素认证，通过多因素认证，可以抵抗用户名和密码的丢失，但是多因素认证对于用户

而言不是很友好。

现阶段，SDP 系统中，SDP 控制器控制了 IH 的可访问服务列表，以及 AH 的 IP 地址、连接参数(如端口号、协议等)等信息。由于 SDP 控制器是中心化设备，其被暴露在网络中，容易遭受 DDoS(Distributed Denial of Service, 分布式拒绝服务)等网络攻击。一旦控制器受到网络攻击停止服务，有可能导致整个系统无法正常运行，IH 将无法进行任何数据访问。

发明内容

本公开提供一种基于区块链的 SDP 访问控制方法及系统，以区块链的方式向客户提供 SDP 服务，解决 SDP 控制器遭受 DDoS 攻击和 SDP 控制器实施错误的授权问题。

为了解决上述技术问题，本公开是这样实现的：

第一方面，本公开实施例提供了一种基于区块链的 SDP 访问控制方法，包括：

SDP 连接接受主机将待验证信息发送给区块链系统节点，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略，以使得所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

SDP 连接接受主机接收 SDP 连接发起主机发送的连接请求，所述连接请求中包括区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息；

若所述 SDP 连接接受主机处于 SDP 连接接受主机列表中，所述 SDP 连接接受主机根据所述支持的连接策略验证所述签名信息，验证成功后向所述 SDP 连接发起主机发送请求响应。

较佳地，所述 SDP 连接接受主机信息包括以下至少一项：IP 地址、端口和协议信息；所述支持的连接策略包括以下至少一项：接入用户的登录

ID、IP 地址、地理位置以及区块链节点验证或背书策略。

较佳地，所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息，是一个或多个区块链系统节点的签名，所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。

- 5 较佳地，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

第二方面，本公开实施例提供一种基于区块链的 SDP 访问控制方法，包括：

- 区块链系统节点接收 SDP 连接接受主机发送的待验证信息，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略；

所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

所述区块链系统节点接收 SDP 连接发起主机提交的身份认证请求；

- 所述区块链系统节点对所述身份认证请求信息进行验证，验证通过后，
15 在区块链中查找所述 SDP 连接发起主机能够访问的 SDP 连接接受主机列表，将所述 SDP 连接接受主机列表返回所述 SDP 连接发起主机。

较佳地，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

- 较佳地，若所述身份认证请求中 SDP 连接发起主机采用自身的私钥对
20 时间戳进行签名；

所述区块链系统节点对所述身份认证请求信息进行验证包括：

所述区块链系统节点对 SDP 连接发起主机提交的签名和时间戳进行验证。

- 较佳地，若所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公
25 钥对 KDF 的加密信息；

所述区块链系统节点对所述身份认证请求信息进行验证包括:

所述区块链系统节点验证所述 KDF 是否正确。

较佳地,若所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息;

5 所述区块链系统节点对所述身份认证请求信息进行验证包括:

所述区块链系统节点验证所述令牌是否正确。

第三方面,提供一种基于区块链的 SDP 访问控制方法,包括:

SDP 连接发起主机向区块链系统节点发送身份认证请求;

所述 SDP 连接发起主机接收所述区块链系统节点发送的能够访问的
10 SDP 连接接受主机列表;

所述 SDP 连接发起主机向 SDP 连接接受主机发送连接请求,所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息;

所述 SDP 连接发起主机接收所述 SDP 连接接受主机发送的请求响应。

15 较佳地,在所述身份认证请求中,所述 SDP 连接发起主机采用自身的私钥对时间戳进行签名。

较佳地,若所述 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密信息,所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息。

20 较佳地,若所述 SDP 连接发起主机有认证节点 A2 提供的令牌,所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息。

较佳地,所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息,是一个或多个区块链系统节点的签名,所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。

25 第四方面,提供一种基于区块链的 SDP 访问控制系统,包括:

第一信息验证模块,配置为将待验证信息发送给区块链系统节点,所述待验证信息包括:所述SDP连接接受主机的主机信息和支持的连接策略,以使得所述区块链系统节点验证所述待验证信息,并在验证通过后记录到区块链账本中;

- 5 第一连接请求模块,配置为接收SDP连接发起主机发送的连接请求,所述连接请求中包括区块链系统节点对所述SDP连接接受主机列表中SDP连接接受主机的签名信息;

第一请求响应模块,配置为若所述SDP连接接受主机处于SDP连接接受主机列表中,根据所述支持的连接策略验证所述签名信息,验证成功后
10 向所述SDP连接发起主机发送请求响应。

较佳地,所述SDP连接接受主机信息包括以下至少一项:IP地址、端口和协议信息;所述支持的连接策略包括以下至少一项:接入用户的登录ID、IP地址、地理位置以及区块链节点验证或背书策略。

较佳地,所述区块链系统节点对SDP连接接受主机列表中SDP连接接受主机的签名信息,是一个或多个区块链系统节点的签名,所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。
15

较佳地,所述待验证信息还包括:所述SDP连接接受主机的主机信息和支持的连接策略的签名。

第五方面,提供一种基于区块链的SDP访问控制系统,包括:

- 20 第二信息验证模块,配置为接收SDP连接接受主机发送的待验证信息,所述待验证信息包括:所述SDP连接接受主机的主机信息和支持的连接策略;验证所述待验证信息,并在验证通过后记录到区块链账本中;

第一身份认证请求模块,配置为接收SDP连接发起主机提交的身份认证请求;

- 25 验证反馈模块,配置为对所述身份认证请求信息进行验证,验证通过

后，在区块链中查找所述 SDP 连接发起主机能够访问的 SDP 连接接受主机列表，将所述 SDP 连接接受主机列表返回所述 SDP 连接发起主机。

较佳地，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

- 5 较佳地，若所述身份认证请求中 SDP 连接发起主机采用自身的私钥对时间戳进行签名；

所述对所述身份认证请求信息进行验证包括：对 SDP 连接发起主机提交的签名和时间戳进行验证。

- 较佳地，若所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公
10 钥对 KDF 的加密信息；

所述对所述身份认证请求信息进行验证包括：验证所述 KDF 是否正确。

较佳地，若所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息；

所述对所述身份认证请求信息进行验证包括：验证所述令牌是否正确。

- 15 第六方面，提供一种基于区块链的 SDP 访问控制系统，包括：

第二身份认证请求模块，配置为向区块链系统节点发送身份认证请求；接收所述区块链系统节点发送的能够访问的 SDP 连接接受主机列表；

- 第二连接请求模块，配置为向 SDP 连接接受主机发送连接请求，所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接
20 接受主机的签名信息；

第二请求响应模块，配置为接收所述 SDP 连接接受主机发送的请求响应。

较佳地，在所述身份认证请求中，所述 SDP 连接发起主机采用自身的私钥对时间戳进行签名。

- 25 较佳地，若 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密

信息，所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息。

较佳地，若 SDP 连接发起主机有认证节点 A2 提供的令牌，所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息。

- 5 较佳地，所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息，是一个或多个区块链系统节点的签名，所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。

第七方面，提供一种 SDP 连接接受主机，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器
10 器执行时实现第一方面或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤。

第八方面，提供一种区块链系统节点，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器
15 执行时实现第二方面或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤。

第九方面，提供一种 SDP 连接发起主机，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器
20 器执行时实现第三方面或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤。

- 第十方面，一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现第一方面或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤；

或者，所述计算机程序被处理器执行时实现第二方面或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤；

- 25 或者，所述计算机程序被处理器执行时实现第三方面或其任意可能实

现方式的基于区块链的 SDP 访问控制方法的步骤。

在本公开实施例中，SDP 连接接受主机将 SDP 连接接受主机信息、支持的连接策略发送到区块链系统节点；将 SDP 连接接受主机信息和支持的连接策略进行区块链节点验证及共识，区块链节点验证及共识之后的 SDP 连接接受主机信息和支持的连接策略记录到区块链账本中；SDP 连接发起主机向区块链系统节点提交身份认证请求；区块链系统节点对 SDP 连接发起主机提交的身份认证请求信息进行验证，身份认证信息的验证包括在区块链中查找 SDP 连接发起主机可以访问的 SDP 连接接受主机列表，将 SDP 连接接受主机列表返回 SDP 连接发起主机；SDP 连接发起主机向 SDP 连接接受主机列表中的 SDP 连接接受主机发起连接请求，连接请求包括区块链系统节点对 SDP 连接接受主机列表中的 SDP 连接接受主机的签名；SDP 连接接受主机对 SDP 连接发起主机发起的连接请求进行验证，验证成功后向 SDP 连接发起主机提供接入服务。本公开实施例以区块链的方式向客户提供 SDP 服务，认证和请求等均进行验证，一方面可以避免 SDP 控制器遭受 DDoS 攻击，另一方面可以防止 SDP 控制器实施错误的授权。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本公开的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为现有技术中的 SDP 控制示意图；

图 2 为本公开实施例中提供的区块链系统架构；

图 3 为本公开实施例中提供的基于区块链的 SDP 访问控制流程图；

图 4 为本公开实施例中提供的一种基于区块链的 SDP 访问控制方法流程图；

图 5 为本公开实施例中提供的另一种基于区块链的 SDP 访问控制方法流程图；

图 6 为本公开实施例中提供的再一种基于区块链的 SDP 访问控制方法流程图；

5 图 7 为本公开实施例中提供的一种基于区块链的 SDP 访问控制系统示意图；

图 8 为本公开实施例中提供的另一种基于区块链的 SDP 访问控制系统示意图；

10 图 9 为本公开实施例中提供的再一种基于区块链的 SDP 访问控制系统示意图。

具体实施方式

下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本公开一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本公开保护的范

15 围。

辅助图 1、图 2、图 3，参见图 4，提供一种基于区块链的 SDP 访问控制方法，包括以下步骤：

S11: SDP 连接接受主机将待验证信息发送给区块链系统节点，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略，以使得所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

20

S12: SDP 连接接受主机接收 SDP 连接发起主机发送的连接请求，所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息；

25

S13: 若所述 SDP 连接接受主机处于 SDP 连接接受主机列表中, 所述 SDP 连接接受主机根据所述支持的连接策略验证所述签名信息, 验证成功后向所述 SDP 连接发起主机发送请求响应。

本实施例中, 所述 SDP 连接接受主机信息包括 IP 地址、端口和协议信息; 所述支持的连接策略包括接入用户的登录 ID、IP 地址、地理位置以及区块链节点验证、背书策略。SDP 连接接受主机将 SDP 连接接受主机信息 (例如 IP 地址、端口和协议信息等)、支持的连接策略 (例如支持接入的用户登录 ID、IP 地址、地理位置, 以及区块链节点验证/背书策略等信息) 发送到区块链系统节点。

10 较佳地, 所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息, 是一个或多个区块链系统节点的签名, 所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。

较佳地, 还可将 SDP 连接接受主机对 SDP 连接接受主机信息和支持的连接策略的签名发送到区块链系统节点, 区块链节点验证 SDP 连接接受主机提交的信息及其签名。验证通过后, 区块链节点将 SDP 连接接受主机提交的 SDP 连接接受主机信息以及支持的连接策略记录到区块链账本中。

辅助图 2, 区块链系统节点由 SDP 控制器与认证节点相互连接构成, SDP 控制器和认证节点都是区块链节点, SDP 连接接受主机和 SDP 连接发起主机都可以向区块链提交交易, 并且可以从区块链读取账本数据。

20 具体的, SDP 连接发起主机向所述区块链系统节点提交身份认证请求的方式为: SDP 连接发起主机采用自身的私钥对时间戳进行签名;

具体的, 区块链系统节点对 SDP 连接发起主机提交的身份认证请求信息进行签名和时间戳验证。SDP 连接发起主机用自己的私钥对时间戳签名, 如果 SDP 连接发起主机用自己的私钥对时间戳进行签名, 那么验证签名和时间戳。

本实施例中，当 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密信息时，身份认证请求中包括 KDF(timestamp, username, password)，使用认证节点 A1 的公钥对 KDF(timestamp, username, password)进行加密。步骤 S4 中，区块链系统节点对 SDP 连接发起主机提交的身份认证请求信息

5 验证 KDF(timestamp, username, password)是否正确。

具体的，如果 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密信息如用户口令，那么认证请求中包含 KDF(timestamp, username, password)，使用认证节点 A1 的公钥对其加密，例如，Epk_A1(KDF(timestamp, username, password))。

10 KDF 是实现 key stretching 的方法，具体就是从一个 master key, password 或者 passphrase 派生出一个或者多个密钥，派生的过程，使用 PRF (Pseudo Random Function 伪随机函数)可以是某种哈希算法。

比如，PBKDF2 是基于密码派生出密钥的算法，需要消耗很多算力，为了是防止暴力破解加密。Scrypt 是一种 基于 password 的 KDF 算法，比

15 起 PBKDF2 需要消耗更多的资源，有效防止专有硬件 ASIC/ FPGA 的暴力破解。Scrypt 内部用的是 PBKDF2 算法，不过内部会长时间地维护一组比特数据，这些数据会在生成复杂的 salt 的过程中反复加密 (Salsa20, 一种流密码) 得到。

具体的，当 SDP 连接发起主机拥有认证节点 A2 提供的令牌时，身份

20 认证请求中包含令牌 Token，使用认证节点 A2 的公钥对令牌 Token 进行加密；区块链系统节点对 SDP 连接发起主机提交的身份认证请求信息验证令牌 Token 是否正确。身份认证成功后，区块链节点查找账本中的 SDP 连接接受主机以及策略信息，将 SDP 连接发起主机能够访问的 SDP 连接接受主机列表作为响应结果返回给 SDP 连接发起主机，其中包括区块链节点对响

25 应结果的签名，可以是一个节点或多个节点的签名。如果 SDP 连接接受主

机在策略中指定了验证/背书节点，那么需要 SDP 连接接受主机指定的节点对响应结果进行签名。

具体的，Token 即标志、记号的意思，在 IT 领域也叫作令牌。在计算机身份认证中是令牌（临时）的意思，一般作为邀请、登录系统使用。在
5 一些数据传输之前，要先进行暗号的核对，不同的暗号被授权不同的数据操作。例如在 USB1.1 协议中定义了 4 类数据包：Token 包、data 包、handshake 包和 special 包。主机和 USB 设备之间连续数据的交换可以分为三个阶段，第一个阶段由主机发送 Token 包，不同的 Token 包内容不一样（暗号不一样）可以告诉设备做不同的工作，第二个阶段发送 data 包，第三个阶段由
10 设备返回一个 handshake 包。

本实施例中，SDP 连接发起主机向 SDP 连接接受主机提交访问请求，其中包括 SDP 连接发起主机能够访问的 SDP 连接接受主机列表以及区块链节点的签名信息。如果 SDP 连接接受主机位于 SDP 连接发起主机能够访问的 SDP 连接接受主机列表中，则 SDP 连接接受主机根据自己在区块链账本
15 中发布的策略验证签名信息，例如签名是否由策略中指定的节点产生，如果验证成功则建立连接；否则不予响应。

在本实施例中，SDP 连接接受主机将 SDP 连接接受主机信息、支持的连接策略发送到区块链系统节点；将 SDP 连接接受主机信息和支持的连接策略进行区块链节点验证及共识，区块链节点验证及共识之后的 SDP 连接
20 接受主机信息和支持的连接策略记录到区块链账本中；SDP 连接发起主机向区块链系统节点提交身份认证请求；区块链系统节点对 SDP 连接发起主机提交的身份认证请求信息进行验证，身份认证信息的验证包括在区块链中查找 SDP 连接发起主机可以访问的 SDP 连接接受主机列表，将 SDP 连接接受主机列表返回 SDP 连接发起主机；SDP 连接发起主机向 SDP 连接接
25 受主机列表中的 SDP 连接接受主机发起连接请求，连接请求包括区块链系

统节点对 SDP 连接接受主机列表中的 SDP 连接接受主机的签名； SDP 连接接受主机对 SDP 连接发起主机发起的连接请求进行验证，验证成功后向 SDP 连接发起主机提供接入服务。本公开实施例以区块链的方式向客户提供 SDP 服务，认证和请求等均进行验证，一方面可以避免 SDP 控制器遭受 DDoS 攻击，另一方面可以防止 SDP 控制器实施错误的授权。

辅助图 1、图 2、图 3，参见图 5，提供另一种基于区块链的 SDP 访问控制方法，包括：

S21：区块链系统节点接收 SDP 连接接受主机发送的待验证信息，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略；

10 S22：所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

S23：所述区块链系统节点接收 SDP 连接发起主机提交的身份认证请求；

S24：所述区块链系统节点对所述身份认证请求信息进行验证，验证通

15 过后，在区块链中查找所述 SDP 连接发起主机能够访问的 SDP 连接接受主机列表，将所述 SDP 连接接受主机列表返回所述 SDP 连接发起主机。

本实施例中，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

具体的，若所述身份认证请求中 SDP 连接发起主机采用自身的私钥对

20 时间戳进行签名；

所述区块链系统节点对所述身份认证请求信息进行验证包括：

所述区块链系统节点对 SDP 连接发起主机提交的签名和时间戳进行验证。

具体的，若所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公

25 钥对 KDF 的加密信息；

所述区块链系统节点对所述身份认证请求信息进行验证包括:

所述区块链系统节点验证所述 KDF 是否正确。

具体的,若所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息;

5 所述区块链系统节点对所述身份认证请求信息进行验证包括:

所述区块链系统节点验证所述令牌是否正确。

本实施例中的基于区块链的 SDP 访问控制方法,为对应于图 4 所示方法中的区块链系统节点侧的实施方案,具体的实施细节同图 4 所示方法的说明,在此不再赘述。

10 辅助图 1、图 2、图 3,参见图 6,提供再一种基于区块链的 SDP 访问控制方法,包括:

S31: SDP 连接发起主机向区块链系统节点发送身份认证请求;

S32: 所述 SDP 连接发起主机接收所述区块链系统节点发送的能够访问的 SDP 连接接受主机列表;

15 S32: 所述 SDP 连接发起主机向 SDP 连接接受主机发送连接请求,所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息;

S34: 所述 SDP 连接发起主机接收所述 SDP 连接接受主机发送的请求响应。

20 具体的,在所述身份认证请求中,所述 SDP 连接发起主机采用自身的私钥对时间戳进行签名。

具体的,若所述 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密信息,所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息。若所述 SDP 连接发起主机有认证节点 A2 提供的令牌,

25 所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密

信息。

较佳地，所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息，是一个或多个区块链系统节点的签名，所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。

- 5 本实施例中的基于区块链的 SDP 访问控制方法，为对应于图 4 所示方法中的 SDP 连接发起主机侧的实施方案，具体的实施细节同图 4 所示方法的说明，在此不再赘述。

辅助图 1、图 2、图 3，参见图 7，提供一种基于区块链的 SDP 访问控制系统，包括：

- 10 第一信息验证模块 41，配置为 SDP 连接接受主机将待验证信息发送给区块链系统节点，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略，以使得所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

- 15 第一连接请求模块 42，配置为 SDP 连接接受主机接收 SDP 连接发起主机发送的连接请求，所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息；

第一请求响应模块 43，配置为若所述 SDP 连接接受主机处于 SDP 连接接受主机列表中，所述 SDP 连接接受主机根据所述支持的连接策略验证所述签名信息，验证成功后向所述 SDP 连接发起主机发送请求响应。

- 20 具体的，所述 SDP 连接接受主机信息包括以下至少一项：IP 地址、端口和协议信息；所述支持的连接策略包括以下至少一项：接入用户的登录 ID、IP 地址、地理位置以及区块链节点验证或背书策略。

- 25 较佳地，所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息，是一个或多个区块链系统节点的签名，所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。

具体的，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

本公开实施例中的基于区块链的 SDP 访问控制系统，为对应于图 4 所示方法的产品实施方案，具体的实施细节同图 4 所示方法，在此不再赘述。

5 辅助图 1、图 2、图 3，参见图 8，提供一种基于区块链的 SDP 访问控制系统，包括：

第二信息验证模块 51，配置为接收 SDP 连接接受主机发送的待验证信息，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略；验证所述待验证信息，并在验证通过后记录到区块链账本中；

10 第一身份认证请求模块 52，配置为接收 SDP 连接发起主机提交的身份认证请求；

验证反馈模块 53，配置为对所述身份认证请求信息进行验证，验证通过后，在区块链中查找所述 SDP 连接发起主机能够访问的 SDP 连接接受主机列表，将所述 SDP 连接接受主机列表返回所述 SDP 连接发起主机。

15 具体的，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

具体的，若所述身份认证请求中 SDP 连接发起主机采用自身的私钥对时间戳进行签名；

所述对所述身份认证请求信息进行验证包括：对 SDP 连接发起主机提交的签名和时间戳进行验证。

具体的，若所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息；

所述对所述身份认证请求信息进行验证包括：验证所述 KDF 是否正确。

具体的，若所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息；

所述对所述身份认证请求信息进行验证包括：验证所述令牌是否正确。

本公开实施例中的基于区块链的 SDP 访问控制系统，为对应于图 5 所示方法的产品实施方案，具体的实施细节同图 5 所示方法，在此不再赘述。

辅助图 1、图 2、图 3，参见图 9，提供一种基于区块链的 SDP 访问控制系统，包括：

第二身份认证请求模块 61，配置为向区块链系统节点发送身份认证请求；所述 SDP 连接发起主机接收所述区块链系统节点发送的能够访问的 SDP 连接接受主机列表；

第二连接请求模块 62，配置为向 SDP 连接接受主机发送连接请求，所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息；

第二请求响应模块 63，配置为接收所述 SDP 连接接受主机发送的请求响应。

具体的，在所述身份认证请求中，所述 SDP 连接发起主机采用自身的私钥对时间戳进行签名。

具体的，若所述 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密信息，所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息。

具体的，若所述 SDP 连接发起主机有认证节点 A2 提供的令牌，所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息。

本公开实施例中的基于区块链的 SDP 访问控制系统，为对应于图 6 所示方法的产品实施方案，具体的实施细节同图 6 所示方法，在此不再赘述。

本公开实施例提供一种 SDP 连接接受主机，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现图 4 所示方法或其任意可能实现方式的基于区块链的 SDP

访问控制方法的步骤。

本公开实施例提供一种区块链系统节点，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现图 5 所示方法或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤。

本公开实施例提供一种 SDP 连接发起主机，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现图 6 所示方法或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤。

本公开实施例提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现图 4 所示方法或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤；

或者，所述计算机程序被处理器执行时实现图 5 所示方法或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤；

或者，所述计算机程序被处理器执行时实现图 6 所示方法或其任意可能实现方式的基于区块链的 SDP 访问控制方法的步骤。

具体的，计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质(例如固态硬盘(SolidStateDisk、SSD))等。

具体的，处理器可以通过硬件来实现也可以通过软件来实现，当通过硬件实现时，该处理器可以是逻辑电路、集成电路等；当通过软件来实现时，该处理器可以是一个通用处理器，通过读取存储器中存储的软件代码来实现，该存储器可以集成在处理器中，可以位于所述处理器之外，独立存在。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本公开实施

5 例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、

10 无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。

具体的，中央处理单元(CPU)根据只读存储器(ROM)中存储的程序或从存储部分加载到随机存取存储器(RAM)的程序执行各种处理。在 RAM 中，还根据需要存储当 CPU 执行各种处理等等时所需的数据。CPU、ROM 和

15 RAM 经由总线彼此连接。输入/输出接口也连接到总线。

下述部件连接到输入/输出接口：输入部分（包括键盘、鼠标等等）、输出部分（包括显示器，比如阴极射线管(CRT)、液晶显示器(LCD)等，和扬声器等）、存储部分（包括硬盘等）、通信部分（包括网络接口卡比如 LAN 卡、调制解调器等）。通信部分经由网络比如因特网执行通信处理。根据需

20 要，驱动器也可连接到输入/输出接口。可拆卸介质比如磁盘、光盘、磁光盘、半导体存储器等等可以根据需要被安装在驱动器上，使得从中读出的计算机程序根据需要被安装到存储部分中。

在通过软件实现上述系列处理的情况下，从网络比如因特网或存储介质比如可拆卸介质安装构成软件的程序。

25 本领域的技术人员应当理解，这种存储介质不局限于其中存储有程序

的、与设备相分离地分发以向用户提供程序的可拆卸介质。可拆卸介质的例子包含磁盘(包含软盘(注册商标))、光盘(包含光盘只读存储器(CD-ROM)和数字通用盘(DVD))、磁光盘(包含迷你盘(MD)(注册商标))和半导体存储器。或者,存储介质可以是 ROM、存储部分中包含的硬盘等等,其中存
5 有程序,并且与包含它们的设备一起被分发给用户。

显然,本领域的技术人员应该明白,上述的本公开实施例的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装
10 置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本公开实施例不限制于任何特定的硬件和软件结合。

上面结合附图对本申请的实施例进行了描述,但是本申请并不局限于
15 上述的具体实施方式,上述的具体实施方式仅仅是示意性的,而不是限制性的,本领域的普通技术人员在本申请的启示下,在不脱离本申请宗旨和权利要求所保护的范围情况下,还可做出很多形式,均属于本申请的保护之内。

权利要求书

1. 一种基于区块链的 SDP 访问控制方法，包括：

SDP 连接接受主机将待验证信息发送给区块链系统节点，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略，以
5 使得所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

SDP 连接接受主机接收 SDP 连接发起主机发送的连接请求，所述连接请求中包括区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息；

10 若所述 SDP 连接接受主机处于所述 SDP 连接接受主机列表中，所述 SDP 连接接受主机根据所述支持的连接策略验证所述签名信息，验证成功后向所述 SDP 连接发起主机发送请求响应。

2. 根据权利要求 1 所述的基于区块链的 SDP 访问控制方法，其中，所述 SDP 连接接受主机信息包括以下至少一项：IP 地址、端口和协议信息；所述支持的连接策略包括以下至少一项：接入用户的登录 ID、IP 地址、地理位置以及区块链节点验证或背书策略。
15

3. 根据权利要求 2 所述的基于区块链的 SDP 访问控制方法，其中，所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息，是一个或多个区块链系统节点的签名，所述一个或多个区块链系统节点根据所述区块链节点验证或背书策略确定。
20

4. 根据权利要求 1 所述的基于区块链的 SDP 访问控制方法，其中，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连接策略的签名。

5. 一种基于区块链的 SDP 访问控制方法，包括：

25 区块链系统节点接收 SDP 连接接受主机发送的待验证信息，所述待

验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略；

所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

所述区块链系统节点接收 SDP 连接发起主机提交的身份认证请求；

5 所述区块链系统节点对所述身份认证请求信息进行验证，验证通过后，在区块链中查找所述 SDP 连接发起主机能够访问的 SDP 连接接受主机列表，将所述 SDP 连接接受主机列表返回所述 SDP 连接发起主机。

6. 根据权利要求 5 所述的基于区块链的 SDP 访问控制方法，其中，所述待验证信息还包括：所述 SDP 连接接受主机的主机信息和支持的连
10 接策略的签名。

7. 根据权利要求 5 所述的基于区块链的 SDP 访问控制方法，其中，若所述身份认证请求中 SDP 连接发起主机采用自身的私钥对时间戳进行签名；

所述区块链系统节点对所述身份认证请求信息进行验证包括：

15 所述区块链系统节点对 SDP 连接发起主机提交的签名和时间戳进行验证。

8. 根据权利要求 5 所述的基于区块链的 SDP 访问控制方法，其中，若所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息；

20 所述区块链系统节点对所述身份认证请求信息进行验证包括：

所述区块链系统节点验证所述 KDF 是否正确。

9. 根据权利要求 5 所述的基于区块链的 SDP 访问控制方法，其中，若所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息；

25 所述区块链系统节点对所述身份认证请求信息进行验证包括：

所述区块链系统节点验证所述令牌是否正确。

10. 一种基于区块链的 SDP 访问控制方法, 包括:

SDP 连接发起主机向区块链系统节点发送身份认证请求;

所述 SDP 连接发起主机接收所述区块链系统节点发送的能够访问的
5 SDP 连接接受主机列表;

所述 SDP 连接发起主机向 SDP 连接接受主机发送连接请求, 所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息;

所述 SDP 连接发起主机接收所述 SDP 连接接受主机发送的请求响
10 应。

11. 根据权利要求 10 所述的基于区块链的 SDP 访问控制方法, 其中, 在所述身份认证请求中, 所述 SDP 连接发起主机采用自身的私钥对时间戳进行签名。

12. 根据权利要求 10 所述的基于区块链的 SDP 访问控制方法, 其中,
15 若所述 SDP 连接发起主机与认证节点 A1 有共享的用户名和秘密信息, 所述身份认证请求中包含 KDF 或者使用认证节点 A1 的公钥对 KDF 的加密信息。

13. 根据权利要求 10 所述的基于区块链的 SDP 访问控制方法, 其中, 若所述 SDP 连接发起主机有认证节点 A2 提供的令牌, 所述身份认证请求中包含令牌或者使用认证节点 A2 的公钥对令牌的加密信息。
20

14. 根据权利要求 10 所述的基于区块链的 SDP 访问控制方法, 其中, 所述区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息, 是一个或多个区块链系统节点的签名, 所述一个或多个区块链系统节点根据区块链节点验证或背书策略确定。

25 15. 一种基于区块链的 SDP 访问控制系统, 包括:

第一信息验证模块，配置为将待验证信息发送给区块链系统节点，所述待验证信息包括：SDP 连接接受主机的主机信息和支持的连接策略，以使得所述区块链系统节点验证所述待验证信息，并在验证通过后记录到区块链账本中；

- 5 第一连接请求模块，配置为接收 SDP 连接发起主机发送的连接请求，所述连接请求中包括区块链系统节点对 SDP 连接接受主机列表中 SDP 连接接受主机的签名信息；

第一请求响应模块，配置为若所述 SDP 连接接受主机处于 SDP 连接接受主机列表中，根据所述支持的连接策略验证所述签名信息，验证成功
10 后向所述 SDP 连接发起主机发送请求响应。

16. 一种基于区块链的 SDP 访问控制系统，包括：

第二信息验证模块，配置为接收 SDP 连接接受主机发送的待验证信息，所述待验证信息包括：所述 SDP 连接接受主机的主机信息和支持的连接策略；验证所述待验证信息，并在验证通过后记录到区块链账本中；

- 15 第一身份认证请求模块，配置为接收 SDP 连接发起主机提交的身份认证请求；

验证反馈模块，配置为对所述身份认证请求信息进行验证，验证通过后，在区块链中查找所述 SDP 连接发起主机能够访问的 SDP 连接接受主机列表，将所述 SDP 连接接受主机列表返回所述 SDP 连接发起主机。

- 20 17. 一种基于区块链的 SDP 访问控制系统，包括：

第二身份认证请求模块，配置为向区块链系统节点发送身份认证请求；接收所述区块链系统节点发送的能够访问的 SDP 连接接受主机列表；

- 第二连接请求模块，配置为向 SDP 连接接受主机发送连接请求，所述连接请求中包括区块链系统节点对所述 SDP 连接接受主机列表中 SDP
25 连接接受主机的签名信息；

第二请求响应模块，配置为接收所述 SDP 连接接受主机发送的请求响应。

18. 一种 SDP 连接接受主机，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 1 至 4 中任一项所述的基于区块链的 SDP 访问控制方法的步骤。

19. 一种区块链系统节点，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 5 至 9 中任一项所述的基于区块链的 SDP 访问控制方法的步骤。

20. 一种 SDP 连接发起主机，包括：处理器、存储器及存储在所述存储器上并可在所述处理器上运行的程序，所述程序被所述处理器执行时实现如权利要求 10 至 14 中任一项所述的基于区块链的 SDP 访问控制方法的步骤。

21. 一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 4 中任一项所述的基于区块链的 SDP 访问控制方法的步骤；

或者，所述计算机程序被处理器执行时实现如权利要求 5 至 9 中任一项所述的基于区块链的 SDP 访问控制方法的步骤；

或者，所述计算机程序被处理器执行时实现如权利要求 10 至 14 中任一项所述的基于区块链的 SDP 访问控制方法的步骤。