

通信方法及通信装置

5 本申请要求于 2023 年 11 月 17 日提交国家知识产权局、申请号为 202311556197.2、申请名称为“通信方法及通信装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种通信方法及通信装置。

背景技术

10 在信息技术（communication technology，IT）或通信技术（information technology，CT）中，一个节点可以通过该节点对应的服务信息为其他节点提供服务，或者说，可以通过获取一个节点的服务信息来获取该节点的服务。其中，一个节点的服务信息可以从该节点获取，也可以从生成该服务信息的节点处获取。例如，卡商或终端厂商对应的节点可以生成终端（节点）的服务信息，终端上也可以存储终端的服务信息，因此，若需要获取终端所提供的服务，则需要从终端或者卡商或终端厂商对应的节点获取终端的服务信息。上述方案中，服务信息的获取流程需要依赖提供服务的节点或生成服务信息的节点，应用场景受限。

发明内容

本申请实施例提供一种通信方法及通信装置，能够使得服务信息获取流程不依赖于提供服务的节点或者生成服务信息的节点，可以应用于更多的场景。

20 第一方面，提供一种通信方法。该通信方法包括：第一节点获取第一信息。其中，第一信息包括第一标识和第一标识对应的服务信息。第一节点向存储节点发送第一信息。

基于第一方面所提供的方法，第一节点可以将第一标识和第一标识对应的服务信息发送至存储节点，这样，便使得存储节点中可以获取到第一节点的第一标识和第一标识对应的服务信息，从而使得其他节点可以通过存储节点获取第一标识对应的服务信息，增加了获取服务信息的渠道，减少了对第一节点的依赖，因此，可以应用于更多场景。

25 一种可能的实现方式中，第一节点可以包括一项或多项：卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器。第一节点可以根据实际场景确定，前述多种设备均可以向存储节点中存在自身的标识及服务信息，应用场景更灵活。

30 一种可能的实现方式中，若第一节点为卡商或终端厂商对应的设备，则第一方面所提供的方法还包括：第一节点获取第二信息，第二信息用于指示终端的第二标识和第二标识对应的凭证信息，第二标识对应的凭证信息用于验证终端和/或第二标识对应的属性，第二标识和第二标识对应的凭证信息是由第一节点生成的，第一节点向存储节点发送第二信息和/或第二信息的哈希值。

35 如此，第一节点（即卡商或终端厂商对应的设备）可以将第二信息发送至存储节点，由于第一节点的服务信息也会上传存储节点，而第二标识和第二标识对应的凭证信息由第一节点生成，可以实现第一节点对第二标识以及第二标识对应的凭证信息的背书。例如，第二标识和第二标识对应的凭证信息是由第一节点对应的私钥签名的，因此，在第一节点可信的情况下，便可以实现第二标识和第二标识对应的凭证信息在不同领域之间的信任互通。

40 一种能的实现方式中，第二标识对应的凭证信息包括第二标识对应的认证信息和/或第二标识对应的证明信息，第二标识对应的认证信息用于验证终端。第二标识对应的证明信息用于验证第二标识对应的属性。如此，在第二标识对应的凭证信息包括第二标识对应的认证信息的情况下，可以实现对终端的身份的验证，在第二标识对应的凭证信息包括第二标识对应的证明信息的情况下，可以对第二标识对应的属性进行验证。

45 一种可能的实现方式中，第二信息包括第二标识，和如下一项或多项：第二标识对应的凭证信息，第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息。如此，可以将前述一种或多种信息存储至存储节点，使得其他设备根据存储节点中的前述信息获取或提供相应的服务。

一种可能的实现方式中，第二标识和第二标识对应的凭证信息携带在第二标识对应的标识信息中。在此情况下，第二信息还可以包括文件信息，其中，文件信息中包括如下一项或多项：第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息。这样，第二标识的标识信息中包括用于对终端的进行认证的凭证信息，从而可以根据实际情况生成文件信息，从而使得文件信息更准确，且可以减少存储的数据量。或者，第二标识携带在第二标识对应的标识信息中，第二标识对应的凭证信息、第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息中的一项或多项携带在第二标识对应的文件信息中。这样，第二标识对应的标识信息与其他信息可以独立存储，或者分别读取，可以减少信息的泄漏，从而增强隐私保护，且使得发布方式更灵活。

一种可能的实现方式中，第二标识对应的标识信息包括第一字段和如下一项或多项：第二字段或第三字段，其中，第一字段承载的信息用于指示第二标识，第二字段承载的信息用于指示第二标识的标识类型，第三字段承载的信息用于校验第二标识对应的标识信息中除第三字段之外的字段承载的信息。这样，可以通过第一字段指示第二标识对应的节点。此外，在第二标识对应的标识信息包括第二字段的情况下，可以确定第二标识的类型，进而可以根据第二标识确定第二标识的来源、可信度或使用场景。在第二标识对应的信息包括第三字段的情况下，可以实现对其他字段，如第一字段，或者第一字段和第二字段的校验，从而确保第二标识的准确性。

一种可能的实现方式中，第一方面所提供的方法还可以包括：第一节点向终端发送第三信息。第三信息用于指示第二信息，或者，第三信息用于指示第二信息和第二信息在存储系统中的存储位置。这样，使得终端可以获取到第二信息，从而能够使用第二信息实现其他节点对终端的认证。

一种可能的实现方式中，若第一节点为终端，则第一方面所提供的方法还可以包括：第一节点接收来自卡商或终端厂商对应的设备的第四信息。其中，第四信息用于指示第一标识和第一标识对应的凭证信息。或者，第四信息用于指示第一标识、第一标识对应的凭证信息，以及第一标识和第一标识对应的凭证信息在存储系统中的存储位置。这样，便使得终端可以获取到第四信息，并能够使用第四信息进行认证。

一种可能的实现方式中，第一方面所提供的方法还可以包括：第一节点向存储节点发送第五信息和/或第五信息的哈希值。其中，第五信息用于指示第一节点的第三标识和第三标识对应的凭证信息，第三标识与第一标识不同。这样，第一节点便可以向存储节点指示第一节点的不同标识以及不同标识对应的凭证信息，从而可以针对不同的标识使用不同的服务，从而使得隐私性更好。

一种可能的实现方式中，若第一节点为终端，则第一方面所提供的方法还可以包括：第一节点向卡商或终端厂商对应的设备发送证明请求信息。其中，证明请求信息用于请求第一节点对应的证明信息，第一节点对应的证明信息用于验证第一节点或第一节点的标识对应的属性。第一节点接收第一节点对应的证明信息。第一节点对应的证明信息是卡商或终端厂商对应的设备生成的。例如，可以使得卡商或终端厂商为终端背书，从而使得在卡商或设备厂商可信任的情况下，终端可以通过证明信息进行验证。

一种可能的实现方式中，若第一节点为卡商或终端厂商对应的设备，则第一方面所提供的方法还可以包括：第一节点接收来自终端的证明请求信息。其中，证明请求信息用于请求终端对应的证明信息，终端对应的证明信息用于验证终端或终端的标识对应的属性。第一节点向存储节点发送终端对应的证明信息。第一节点向终端发送终端对应的证明信息。这样，可以由卡商或终端厂商为终端背书，在卡商或设备厂商可信任的情况下，便可以通过区块链上的证明信息验证终端。

第二方面，提供一种通信方法。该通信方法包括：存储节点接收来自第一节点的第二信息。其中，第二信息包括第一标识和第一标识对应的服务信息。存储节点存储第二信息。

基于第二方面所提供的方法，存储节点可以获取第一节点的第二标识和第一标识对应的服务信息，从而使得其他节点可以通过存储节点获取第二标识对应的服务信息，增加了获取服务信息的渠道，减少了对第一节点的依赖，因此，可以应用于更多场景。

一种可能的实现方式中，第一节点可以包括一项或多项：卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器。

一种可能的实现方式中，若第一节点包括卡商或终端厂商对应的设备，则第二方面所提供的方法还可以包括：存储节点接收来自第一节点的第二信息。第二信息用于指示终端的第二标识和第二标识对应的凭证信息，第二标识对应的凭证信息用于验证终端和/或第二标识对应的属性。第二标识和第二标识对应的凭证信息是由第一节点生成的。存储节点存储第四信息。

一种可能的实现方式中，第二标识对应的凭证信息包括第二标识对应的认证信息和/或第二标识对应的证明信息，第二标识对应的认证信息用于验证终端。第二标识对应的证明信息用于验证第二标识对应的属性。

一种可能的实现方式中，第二信息包括第二标识，和如下一项或多项：第二标识对应的凭证信息，第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第二标识和第二标识对应的凭证信息携带在第二标识对应的标识信息中。在此情况下，第二信息还可以包括文件信息，其中，文件信息中包括如下一项或多项：第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息。这样，第二标识的标识信息中包括用于实现对第一节点的认证的凭证信息，从而可以根据实际情况生成文件信息，从而使得文件信息更准确，且可以减少存储的数据量。或者，第二标识携带在第二标识对应的标识信息中，第二标识对应的凭证信息、第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息中的一项或多项携带在第二标识对应的文件信息中。这样，第二标识对应的标识信息与其他信息可以独立存储，或者分别读取，可以减少信息的泄漏，从而增强隐私保护，且使得发布方式更灵活。

一种可能的实现方式中，第二标识对应的标识信息包括第一字段和如下一项或多项：第二字段或第三字段，其中，第一字段承载的信息用于指示第二标识，第二字段承载的信息用于指示第二标识的标识类型，第三字段承载的信息用于校验第二标识对应的标识信息中除第三字段之外的字段承载的信息。

一种可能的实现方式中，第二方面所提供的方法还可以包括：存储节点接收来自第一节点的第五信息。其中，第五信息用于指示第一节点的第三标识和第三标识对应的凭证信息。

一种可能的实现方式中，若第一节点包括卡商或终端厂商对应的设备，则第二方面所提供的方法还可以包括：存储节点接收来自第一节点的终端对应的证明信息。其中，终端对应的证明信息用于验证终端或终端的标识对应的属性。

一种可能的实现方式中，第二方面所提供的方法还可以包括：存储节点接收来自第二节点的第六信息。其中，第六信息用于指示第二节点的第四标识和第四标识对应的凭证信息，第四标识对应的凭证信息用于验证第二节点和/或第四标识对应的属性。第四标识和第四标识对应的凭证信息是由第一节点生成的。存储节点存储第六信息。

一种可能的实现方式中，第四标识对应的凭证信息包括第四标识对应的认证信息和/或第四标识对应的证明信息，第四标识对应的认证信息用于验证第二节点，第四标识对应的证明信息用于验证第四标识对应的属性。

一种可能的实现方式中，第六信息包括第四标识和如下一项或多项：第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第四标识和第四标识对应的凭证信息携带在第四标识对应的标识信息中。这样，第四标识的标识信息中包括用于对第二节点进行认证的凭证信息，从而可以根据实际情况生成文件信息，从而使得文件信息更准确，且可以减少存储的数据量。或者，第四标识携带在第二标识对应的标识信息中，第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息中的一项或多项携带在第四标识对应的文件信息中。这样，第四标识对应的标识信息与其他信息可以独立存储，或者分别读取，可以减少信息的泄漏，从而增强隐私保护，且使得发布方式更灵活。

一种可能的实现方式中，第四标识对应的标识信息包括第四字段和如下一项或多项：第五字段或第六字段，其中，第四字段承载的信息用于指示第四标识，第五字段承载的信息用于指示第四标识的标识类型，第六字段承载的信息用于校验第四标识对应的标识信息中除第六字段之外的字段承载的信息。

5 关于第二方面的技术效果可以参考第一方面所述方法的技术效果，此处不再赘述。

结合第一方面或第二方面的方案，一种可能的实现方式中，第一标识对应的服务信息用于生成第三节点的证明信息和/或第三节点的认证信息。和/或，第一标识对应的服务信息用于验证第三节点的证明信息和/或第三节点的认证信息。和/或，第一标识对应的服务信息用于为第三节点提供如下一项或多项服务：签约服务、网络接入服务、或数据共享服务；其中，第三节点与第一节点不同，第三节点的凭证信息用于验证第三节点，第三节点的证明信息用于验证第三节点的标识对应的属性。这样，可以服务信息的内容更为灵活，例如，可以根据具体的使用场景匹配服务信息。

一种可能的实现方式中，第一信息还用于指示第一标识对应的凭证信息，第一标识对应的凭证信息用于验证第一节点和/或用于验证第一标识对应的属性。

15 一种可能的实现方式中，第一标识对应的凭证信息包括第一标识对应的认证信息和/或第一标识对应的证明信息，第一标识对应的认证信息用于验证第一节点，第一标识对应的证明信息用于验证第一节点对应的属性。如此，可以使得存储节点中存储的第一信息包括第一标识和第一标识对应的凭证信息。由于第一凭证信息可以用于验证第一标识或第一标识对应的属性，如此，便可以使得其他节点可以对第一标识进行验证。

20 一种可能的实现方式中，第一信息包括第一标识和第一标识对应的服务信息，和如下一项或多项：用于指示第一节点的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息公开条件的信息。如此，可以使得第一信息的内容更灵活。

25 一种可能的实现方式中，第一标识和第一标识对应的凭证信息携带在第一标识对应的标识信息中。这样，第一标识的标识信息中包括用于对第一节点的进行认证的凭证信息，从而可以根据实际情况生成文件信息，从而使得文件信息更准确，且可以减少存储的数据量。或者，第一标识携带在第一标识对应的标识信息中，第一标识对应的凭证信息、第一标识对应的服务信息、用于指示终端的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息的公开条件的信息中的一项或多项携带在第一标识对应的文件信息中。这样，第一标识对应的标识信息与其他信息可以独立存储，或者分别读取，可以减少信息的泄漏，从而增强隐私保护，且使得发布方式更灵活。

30 一种可能的实现方式中，第一标识对应的证明信息是由第四节点根据第四节点对应的服务信息生成的，第一标识对应的证明信息由第四节点对应的私钥签名。第四节点与第一节点不同。

一种可能的实现方式中，第四节点对应的服务信息用于生成服务结果信息，服务结果信息包括第五节点的凭证信息。第五节点与第四节点不同。第五节点的凭证信息用于验证第五节点和/或用于验证第五节点的标识对应的属性。

35 一种可能的实现方式中，第一标识对应的标识信息是经过卡商或终端厂商生成的第一节点的标识对应的私钥签名的信息。

一种可能的实现方式中，存储节点为如下一项或多项：区块链节点、分布式存储节点、或通信设备。通信设备与第一节点不同。

40 第三方面，提供一种通信方法。该通信方法包括：第二节点获取第六信息。其中，第六信息用于指示第二节点的第四标识和第四标识对应的凭证信息，第四标识对应的凭证信息用于验证第二节点和/或第四标识对应的属性。第四标识和第四标识对应的凭证信息是由第一节点生成的。第二节点向存储节点发送第六信息和/或第六信息的哈希值。

基于第三方面所提供的方法，第二节点可以获取第六信息并自行上传第六信息，可以提高第二节点对自身标识和凭证信息的把控程度。

45 一种可能的实现方式中，第四标识对应的凭证信息包括第四标识对应的认证信息和/或第四标识对应的证明信息，第四标识对应的认证信息用于验证第二节点，第四标识对应的证明信息用于验证第四标识对应的属性。

一种可能的实现方式中，第六信息包括第四标识和如下一项或多项：第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第四标识和第四标识对应的凭证信息携带在第四标识对应的标识信息中；或者，第四标识携带在第二标识对应的标识信息中，第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息中的一项或多项携带在第四标识对应的文件信息中。

可选地，第四标识对应的标识信息包括第四字段和如下一项或多项：第五字段或第六字段，其中，第四字段承载的信息用于指示第四标识，第五字段承载的信息用于指示第四标识的标识类型，第六字段承载的信息用于校验第四标识对应的标识信息中除第六字段之外的字段承载的信息。

一种可能的实现方式中，存储节点为如下一项或多项：区块链节点、分布式存储节点、或通信设备。通信设备与第一节不同。

第四方面，提供一种通信方法。该通信方法包括：运营商对应的设备获取第七信息。其中，第七信息用于指示终端的第五标识和第五标识对应的凭证信息，第五标识对应的凭证信息用于验证终端和/或第五标识对应的属性，第五标识与运营商对应的设备中终端的用户永久标识不同，且第五标识与终端的用户永久标识对应，用户永久标识用于运营商对应的设备与终端之间的通信。运营商对应的设备向终端发送第七信息。

基于第四方面所提供的方法，运营商对应的设备可以生成终端的第五标识和第五标识对应的凭证信息，由于第五标识与终端的用户永久标识对应，因此，运营商对应的设备可以对终端的信息进行集中管理。

第五方面，提供一种通信方法。该通信方法包括：终端接收来自运营商对应的设备的第七信息。其中，第七信息用于指示终端的第五标识和第五标识对应的凭证信息，第五标识对应的凭证信息用于验证终端和/或第五标识对应的属性，第五标识与终端的用户永久标识不同，且第五标识与终端的用户永久标识对应，用户永久标识用于运营商对应的设备与终端之间的通信。终端存储第七信息。

此外，第五方面所述的通信方法的技术效果可以参考第四方面所述的通信方法的技术效果，此处不再赘述。

一种可能的实现方式中，第五标识对应的凭证信息包括第五标识对应的认证信息和/或第五标识对应的证明信息，第五标识对应的认证信息用于验证终端，第五标识对应的证明信息用于验证终端对应的属性。

一种可能的实现方式中，第七信息包括第五标识，和如下一项或多项：第五标识对应的凭证信息、第五标识对应的证明信息、用于指示终端的类型的信息、第五标识的签发者的信息、用于指示第五标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第五标识和第五标识对应的凭证信息携带在第五标识对应的标识信息中；或者，第五标识对应的凭证信息、第五标识对应的服务信息、用于指示终端的类型的信息、第五标识的签发者的信息、用于指示第五标识对应的凭证信息的公开条件的信息中的一项或多项携带在第五标识对应的文件信息中。

一种可能的实现方式中，第五标识对应的标识信息包括第七字段和如下一项或多项：第八字段或第九字段，其中，第七字段承载的信息用于指示第五标识，第八字段承载的信息用于指示第五标识的标识类型，第九字段承载的信息用于校验第五标识对应的标识信息中除第九字段之外的字段承载的信息。这样，可以通过第七字段指示第五标识对应的节点。此外，在第五标识对应的标识信息包括第八字段的情况下，可以确定第五标识的类型，进而可以根据第五标识确定第五标识的来源、可信度或使用场景。在第五标识对应的信息包括第九字段的情况下，可以实现对其他字段，如第七字段，或者第七字段和第八字段的校验，从而确保第五标识的准确性。

第六方面，提供一种通信方法，该通信方法包括：卡商或终端厂商对应的设备获取第八信息和第九信息。其中，第八信息包括用于指示卡商或终端厂商对应的设备的第七标识，以及第七标识对应的凭证信息，第七标识对应的凭证信息用于验证卡商或终端厂商对应的设备和/或用于验证

第七标识对应的属性。第九信息用于指示终端的第八标识和第八标识对应的凭证信息，第八标识对应的凭证信息用于验证终端和/或第八标识对应的属性。第八标识和第八标识对应的凭证信息是由卡商或终端厂商对应的设备生成的即第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的。卡商或终端厂商对应的设备向存储节点发送第八信息和第九信息。

5 基于第六方面所提供的方法，卡商或终端厂商对应的设备可以将第八信息和第九信息发送至存储节点，而第八标识和第八标识对应的凭证信息由卡商或终端厂商对应的设备生成，可以实现卡商或终端厂商对应的设备对第八标识以及第八标识对应的凭证信息的背书。例如，第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的，因此，在卡商或终端厂商对应的设备可信的情况下，便可以实现第八标识和第八标识对应的凭证信息在不同领域之间的信任互通。

10 一种可能的实现方式中，第六方面所提供的方法还可以包括：卡商或终端厂商对应的设备向终端发送第九信息。

第七方面，提供一种通信方法，该通信方法包括：存储节点接收第八信息和第九信息。其中，第八信息包括用于指示卡商或终端厂商对应的设备的第七标识，以及第七标识对应的凭证信息，第七标识对应的凭证信息用于验证卡商或终端厂商对应的设备和/或用于验证第七标识对应的属性。第九信息用于指示终端的第八标识和第八标识对应的凭证信息，第八标识对应的凭证信息用于验证终端和/或第八标识对应的属性。第八标识和第八标识对应的凭证信息是由卡商或终端厂商对应的设备生成的，即第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的。存储节点存储第八信息和第九信息。

15 基于第七方面所提供的方法，存储节点可以接收第八信息和第九信息，而第八标识和第八标识对应的凭证信息由卡商或终端厂商对应的设备生成，可以实现卡商或终端厂商对应的设备对第八标识以及第八标识对应的凭证信息的背书。例如，第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的，因此，在卡商或终端厂商对应的设备可信的情况下，便可以实现第八标识和第八标识对应的凭证信息在不同领域之间的信任互通。

20 一种可能的实现方式中，存储节点接收第八信息和第九信息，包括：存储节点接收来自卡商或终端厂商对应的设备的第八信息和第九信息。

25 一种可能的实现方式中，存储节点接收第八信息和第九信息，包括：存储节点接收来自卡商或终端厂商对应的设备的第八信息，以及接收来自终端的第九信息。在一些可能的示例中，卡商或终端厂商对应的设备可以是卡商或终端厂商对应的设备，终端可以是终端。

第八方面，提供一种通信装置。该通信装置用于执行第一方面至第七方面中任意一种实现方式所述的通信方法。

30 在本申请中，第八方面所述的通信装置可以为终端或网络设备，或者可设置于该终端或网络设备中的芯片（系统）、或其他部件或组件或者软件模块，或者包含该终端或网络设备的装置。

应理解，第八方面所述的通信装置包括实现上述第一方面至第七方面中任一方面所述的通信方法相应的模块、单元、或手段（means），该模块、单元、或手段可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个用于执行上述通信方法所涉及的功能的模块或单元。

第九方面，提供一种通信装置。该通信装置包括：处理器，该处理器用于执行第一方面至第七方面中任意一种可能的实现方式所述的通信方法。

40 在一种可能的实现方式中，第九方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第九方面所述的通信装置与其他通信装置通信。

在一种可能的实现方式中，第九方面所述的通信装置还可以包括存储器。该存储器可以与处理器集成在一起，也可以分开设置。该存储器可以用于存储第一方面至第七方面中任一方面所述的通信方法所涉及的计算机程序和/或数据。

45 该处理器与存储器耦合，该处理器用于执行存储器中存储的计算机程序，以使得该通信装置执行第一方面至第七方面中任意一种可能的实现方式所述的通信方法。

在本申请中，第九方面所述的通信装置可以为第一节点、第二节点、卡商或终端厂商对应的设备、存储节点、终端、卡商或设备厂商对应的设备，或者可设置于该第一节点、第二节点、卡商或终端厂商

对应的设备、存储节点、终端、卡商或设备厂商对应的设备中的芯片（系统）、其他部件或组件或者软件模块，或者包含该第一节点、第二节点、卡商或终端厂商对应的设备、存储节点、终端、卡商或设备厂商对应的设备的装置。

第十方面，提供一种通信系统。该通信系统包括一个或多个终端，以及一个或多个网络设备。

5 第十一方面，提供一种计算机可读存储介质，包括：计算机程序或指令；当该计算机程序或指令在计算机上运行时，使得该计算机执行第一方面至第七方面中任意一种可能的实现方式所述的通信方法。

第十二方面，提供一种计算机程序产品，包括计算机程序或指令，当该计算机程序或指令在计算机上运行时，使得该计算机执行第一方面至第七方面中任意一种可能的实现方式所述的通信方法。

10 此外，上述第八方面至第十二方面所述的通信装置的技术效果，可以参考上述第一方面至第七方面所述的通信方法的技术效果，此处不再赘述。

附图说明

图 1 为本申请实施例提供的通信系统的架构示意图；

图 2 为本申请实施例提供的通信方法的流程示意图一；

图 3 为本申请实施例提供的标识的结构示意图；

15 图 4 为本申请实施例提供的通信方法的流程示意图二；

图 5 为本申请实施例提供的标识信息的示意图；

图 6 为本申请实施例提供的终端中存储的信息的示意图；

图 7 为本申请实施例提供的不同标识以及不同标识之间的文件信息的关系示意图；

图 8 为本申请实施例提供的通信方法的流程示意图三；

20 图 9 为本申请实施例提供的通信方法的流程示意图四；

图 10 为本申请实施例提供的通信方法的流程示意图五；

图 11 为本申请实施例提供的通信装置的结构示意图一；

图 12 为本申请实施例提供的通信装置的结构示意图二。

具体实施方式

25 用户可以通过身份标识，如用户的去中心化身份标识（decentralized Identifier， DID）标识其身份。

在信息技术（communication technology， IT）或通信技术（information technology， CT）中，一个节点可以通过该节点对应的服务信息为其他节点提供服务，或者说，可以通过获取一个节点的服务信息来获取该节点的服务。其中，一个节点的服务信息可以从该节点获取，也可以从生成该节点的服务信息的节点处获取。例如，卡商或终端厂商对应的节点可以生成终端对应的（节点）的服务信息，终端对应的节点上也可以存储终端对应的节点的服务信息，因此，若需要获取终端所提供的服务，则需要从终端对应的节点或者卡商或终端厂商对应的节点获取终端的服务信息。上述方案中，服务信息的获取需要依赖提供服务的节点或生成服务信息的节点，应用场景受限。

30 此外，在一个领域或行业中，用户若需要获取商家的服务，则需要先提供用户的身份相关的信息并在商家处注册账号，商家会保存用户的身份相关的信息和账号。用户可以基于用户注册的账号和密码获取商家的服务。而对于其他未存储有用户的身份相关信息、账号（即用户的标识）、密码的商家，则无法确定用户是否可信，在不同领域中用户需要采用不同的标识进行验证，因此，不同领域之间无法信任互通，即终端的同一个标识不能在不同领域中使用。

下面将结合附图，对本申请实施例中的技术方案进行描述。

40 本申请实施例的技术方案可以应用于各种通信系统，例如无线保真（wireless fidelity， WiFi）系统，车到任意物体（vehicle to everything， V2X）通信系统、设备间（device-to-device， D2D）通信系统、车联网通信系统、第 4 代（4th generation， 4G）移动通信系统，如长期演进（long term evolution， LTE）系统、第五代（5th generation， 5G）移动通信系统，如新空口（new radio， NR）系统，以及 5G 之后演进的通信系统，如第六代（6th generation， 6G）移动通信系统等。

45 本申请将围绕可包括多个设备、组件、模块等的系统来呈现各个方面、实施例或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等，并且/或者可以并不包括结合附图讨论的所

有设备、组件、模块等。此外，还可以使用这些方案的组合。

另外，在本申请实施例中，“示例地”、“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例”的任何实施例或实现方式不应被解释为比其它实施例或实现方式更优选或更具优势。确切而言，使用示例一词旨在以具体方式呈现概念。

5 本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

为便于理解本申请实施例，首先以图1中示出的通信系统为例详细说明适用于本申请实施例的通信系统。示例性地，图1为本申请实施例提供的通信方法所适用的一种通信系统的架构示意图。

10 如图1所示，该通信系统包括至少一个节点（节点101a至101i）和存储系统102。

存储系统102可以包括一个或多个存储节点。

存储系统102可以包括如下一项或多项：区块链系统（在此情况下，存储节点可以是区块链节点）、分布式存储系统（存储节点为分布式系统中的节点）或通信设备（存储节点即通信设备）。

15 其中，区块链系统可以包括一个或多个区块链节点，分布式存储系统可以包括一个或多个分布式的存储设备，通信设备可以包括运营商对应的设备。

应理解，区块链节点可以是终端或网络设备，分布式存储系统中的存储设备可以是终端或网络设备，通信设备可以是终端或网络设备。

20 至少一个节点（节点101a至101i）中的节点可以与存储系统进行信息交互。若至少一个节点包括多个节点，那么，该多个节点中的两个节点直接可以进行信息交互。至少一个节点（节点101a至101i）中的节点可以包括终端和网络设备。其中，至少一个节点中的节点（节点101a至101i）可以是用户对应的设备，网络设备可以是卡商或终端厂商对应的设备、可信的第三方对应的设备、空中写卡服务器、运营商对应的设备或权威机构对应的设备。终端厂商也可以称为设备商、设备提供商等。可理解，卡商、终端厂商、可信的第三方、运营商或权威机构均用于举例，在实际实施中，还可以存在其他组织或机构。

25 其中，卡商或终端厂商对应的设备，可以是用于实现卡商或终端厂商的业务及设备，如卡商或终端厂商写卡的设备。

运营商对应的设备是用于提供运营商的业务及设备，如运营商的服务器、核心网中的网元，或者接入网设备等。权威机构对应的设备是可以用于提供权威机构的业务及设备，如属于权威机构的服务器、或主机等。

30 第三方可信机构对应的设备可以用于提供第三方可信机构的业务及设备，如属于第三方可信机构的服务器、或主机等。

上述终端为接入上述通信系统，且具有收发功能的终端或可设置于该终端的芯片或芯片系统，或者具有终端功能的单元或模块。该终端也可以称为终端设备，又可以称之为用户设备（user equipment, UE）、移动台（mobile station, MS）、移动终端（mobile terminal, MT）等，或是用于向用户提供语音或数据连通性的设备，也可以是物联网设备。例如，终端包括具有无线连接功能的手持式设备、车载设备。目前，终端可以是：手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备（mobile internet device, MID）、可穿戴设备（例如智能手表、智能手环、计步器、智能眼镜等），车载设备（例如，汽车、自行车、电动车、飞机、船舶、火车、高铁等）、卫星终端、虚拟现实（virtual reality, VR）设备、增强现实（augmented reality, AR）设备、智能销售点（point of sale, POS）机、客户终端设备（customer-premises equipment, CPE）、工业控制中的无线终端、智能家居设备（例如，冰箱、电视、空调、电表等）、智能机器人、机械臂、车间设备、无人驾驶中的无线终端、远程医疗中的无线终端、智能电网（smart grid）中的无线终端、运输安全中的无线终端、智慧城市中的无线终端，或智慧家庭中的无线终端、飞行设备（例如，智能机器人、热气球、无人机、飞机）等。终端还可以是车辆装置，例如整车装置、车载模组、车载芯片、车载单元（on board unit, OBU）或车联网终端盒子（telematics box, T-BOX）等，终端还可以是其他具有终端功能的设备，例如，终端还可以是D2D通信中担任终端功能的设备。

45 本申请的终端还可以是可用于实现终端功能的模块或单元，例如，终端还可以是通用集成电路卡（universal integrated circuit card, UICC）。应理解，本申请实施例中的UICC卡仅用于举例，实际实施

中, UICC 卡还可以替换为与 UICC 卡功能的设备。此外, UICC 卡还可以存在其他名称, 如区块链通用集成电路卡 (blockchain UICC, B-UICC), 本申请实施例中对此不作限定。

本申请的实施例对终端的设备形态不做限定, 用于实现终端的功能的装置可以是终端; 也可以是能够支持终端实现该功能的装置, 例如芯片系统。该装置可以被安装在终端中或者和终端匹配使用。本申请实施例中, 芯片系统可以由芯片构成, 也可以包括芯片和其他分立器件。

在一种可能的场景中, 网络设备可以是基站 (base station)、演进型基站 (evolved NodeB, eNodeB)、传输接收点 (transmitting and receiving point, TRP)、发射点 (transmitting point, TP)、下一代基站 (next generation NodeB, gNB)、第六代 (6th generation, 6G) 移动通信系统中的下一代基站、未来移动通信系统中的基站、卫星、或 WiFi 系统中的接入点 (access point, AP)、接入回传一体化 (integrated access and backhaul, IAB) 节点、移动交换中心非陆地通信网络 (non-terrestrial network, NTN) 通信系统中的网络设备, 即可以部署于高空平台或者卫星等。网络设备可以是宏基站 (如图 1 中的 110a)、微基站或室内站 (如图 1 中的 110b)、中继节点或施主节点、或者是云无线接入网络 (cloud radio access network, CRAN) 场景下的无线控制器。网络设备还可以是设备到设备 (device to device, D2D) 通信、车联网通信、无人机通信、机器通信中担任基站功能的设备。可选的, 网络设备还可以是服务器、可穿戴设备, 车辆或车载设备等。例如, 车辆外联 (vehicle to everything, V2X) 技术中的接入网设备可以为路侧单元 (road side unit, RSU)。

在另一种可能的场景中, 由多个网络设备协作协助终端实现无线接入, 不同网络设备分别实现基站的部分功能。例如, 网络设备可以是集中式单元 (central unit, CU), 分布式单元 (distributed unit, DU), CU-控制面 (control plane, CP), CU-用户面 (user plane, UP), 或者无线单元 (radio unit, RU) 等。CU 和 DU 可以是单独设置, 或者也可以包括在同一个网元中, 例如基带单元 (baseband unit, BBU) 中。RU 可以包括在射频设备或者射频单元中, 例如包括在射频拉远单元 (remote radio unit, RRU)、有源天线处理单元 (active antenna unit, AAU) 或远程射频头 (remote radio head, RRH) 中。可以理解的是, 网络设备可以为 CU 节点、或 DU 节点、或包括 CU 节点和 DU 节点的设备。此外, CU 可以划分为无线接入网 (radio access network, RAN) 中的网络设备, 也可以将 CU 划分为核心网 (core network, CN) 中的网络设备, 在此不做限制。

在不同系统中, CU (或 CU-CP 和 CU-UP)、DU 或 RU 也可以有不同的名称, 但是本领域的技术人员可以理解其含义。例如, 在开放式接入网 (open RAN, ORAN) 系统中, CU 也可以称为 O-CU (开放式 CU), DU 也可以称为 O-DU, CU-CP 也可以称为 O-CU-CP, CU-UP 也可以称为 O-CU-UP, RU 也可以称为 O-RU。为描述方便, 本申请中以 CU, CU-CP, CU-UP, DU 和 RU 为例进行描述。本申请中的 CU (或 CU-CP、CU-UP)、DU 和 RU 中的任一单元, 可以通过软件模块、硬件模块、或者软件模块与硬件模块结合来实现。

又一种可能的场景中, 上述网络设备还可以是核心网中的网元或设备。

再一些可能的场景中, 上述网络设备可以是有线网络中的网元或设备, 如服务器等。

本申请实施例中, 对网络设备的形态不作限定, 用于实现网络设备的功能的装置可以是网络设备; 也可以是能够支持网络设备实现该功能的装置, 例如芯片系统。该装置可以被安装在网络设备中或者和网络设备匹配使用。应理解, 本申请实施例中的节点仅用于举例, 实际实施中, 本申请实施例中的节点还可以是其他组织或机构对应的设备, 此处不再赘述。应理解, 本申请实施例所述的区块链节点可以包括多个通信设备, 本申请实施例所述的分布式系统可以包括多个通信设备。

需要说明的是, 本申请实施例提供的通信方法, 可以适用于图 1 所示的节点与存储节点之间, 具体实现可以参考下述方法实施例, 此处不再赘述。

应当指出的是, 本申请实施例中的方案还可以应用于其他通信系统中, 相应的名称也可以用其他通信系统中的对应功能的名称进行替代。

应理解, 图 1 仅为便于理解而示例的简化示意图, 该通信系统中还可以包括其他网络设备, 和/或, 其他终端, 图 1 中未予以画出。

下面将结合图 2-图 10 对本申请实施例提供的通信方法进行具体阐述。

示例性地, 图 2 为本申请实施例提供的通信方法的流程示意图一。该通信方法可以适用于图 2 所示的节点与存储节点之间的通信。

如图 2 所示, 该通信方法包括如下步骤:

S201, 第一节点获取第一信息。

其中, 第一信息包括第一标识和第一标识对应的服务信息。

一种可能的实现方式中, 第一节点可以包括如下一项或多项: 卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器。这样, 第一节点可以根据实际场景确定, 前述多种设备均可以向存储节点中存在自身的标识及服务信息, 应用场景更灵活。

关于卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备的实现可以参考图 1 所提供的通信系统中的相关介绍, 此处不再赘述。

第一标识是用于标识第一节点的信息, 或者, 第一标识是用于标识第一标识对应的属性的信息。第一标识可以复用全球移动通信系统协会(groupe speciale mobile association, GSMA)规定的UICC 的嵌入式通用集成电路卡(embedded universal integrated circuit card, eUICC)形式。例如, 第一标识可以是“0x12345678”, 此处第一标识仅用于举例, 实际实施中, 第一标识还可以是其他可能的实现方式, 此处不再赘述。应理解, 第一标识可以是去中心化根凭证/信任状(decentralized root credentials, DRC)、或去中心化身份凭证/信任状(decentralized identity credentials, DIC)、或去中心化自控身份(decentralized self-control credentials, DSCC)。其中, DRC、DIC 和 DSCC 均可以称为自控身份标识(self-control identity, scID)。可理解, 本申请实施例中, 与节点的标识对应的属性, 也与该节点对应, 也就是说, 与节点的标识对应的属性也可以说是与节点对应的属性。一个节点可以由多个标识, 不同的标识均可以存在各自对应的属性。

一些可能的实现方式中, 第一标识可以由除第一节点之外的其他可信任的节点生成的用于标识第一节点的信息。例如, 若第一标识是 DRC, 该 DRC 可以由除第一节点之外的其他可信任节点生成的。另一些可能的实施例中, 第一标识可以由第一节点根据根凭证生成的用于标识该节点或标识节点的对应的属性的信息, 如去中心化身份凭证(decentralized identity credentials, DIC)。

再一些可能的实现方式中, 第一标识可以由第一节点生成的用于标识该第一节点或标识第一节点的属性的信息, 如去中心化自控身份(decentralized self-control credentials, DSCC)。如此, 可以根据不同的业务场景使用不同类型的标识, 例如, 在对个人信息保密要求高的业务场景中, 可以使用 DIC 完成业务。又如, 在对第一节点信任要求低的场景中, 可以使用 DSCC 完成业务。

一些可能的实现方式中, 第一节点对应的属性, 可以包括社会属性, 如第一节点是一个合法的公民, 第一节点完成了实名认证、第一节点的学历, 第一节点的工作等。

一些可能的实施方式中, 第一节点对应的属性还可以包括其他的客观属性, 如第一节点的所在的位置、年龄、具备某种权限等。

一种可能的实现方式中, 第一标识对应的服务信息包括第一节点能够提供的服务的信息, 例如, 服务的位置(以服务通过智能合约实现为例, 则服务的位置可以是实现服务的功能的智能合约的地址)、或调用服务所需要的参数(如调用签约服务或身份证明服务的参数)。以下结合情形 1 至情形 4 说明。

情形 1, 第一标识对应的服务信息用于生成第三节点的证明信息和/或第三节点的认证信息。

情形 2, 第一标识对应的服务信息用于验证第三节点的证明信息和/或第三节点的认证信息。

情形 3, 第三节点使用第一标识对应的服务可以调用服务信息中的服务。或者说, 第一标识对应的服务信息可以用于为第三节点提供该服务信息中的服务。例如, 第一标识对应的服务信息用于为第三节点提供如下一项或多项服务: 签约服务、网络接入服务、或数据共享服务。其中, 第三节点与第一节点不同, 第三节点的凭证信息用于验证第三节点, 第三节点的证明信息用于验证第三节点的标识对应的属性。

若第一节点是卡商, 第一标识对应的服务信息为卡商的服务信息, 该服务信息可以用于实现情形 1 或情形 2 中的服务信息的功能。以第三节点是终端, 该终端为卡举例, 卡商通过卡商的服务信息可以为卡生成证明信息, 用于证明卡的安全等级。或者, 卡商通过卡商的服务信息可以为

卡生成认证信息，也就是为卡生成证书，该证书可以用于为卡的公钥背书。或者，卡商通过卡商的服务信息可以完成对卡的验证，即当其他节点验证卡的时，可以用卡商的服务信息进行验证。

类似地，若第一节点是运营商，第一标识对应的服务信息为卡商的服务信息，该服务信息可以用于实现情形 1 或情形 2 中的服务信息的功能。此外，该服务信息可以用于实现情形 3 中的服务信息的功能。例如，第二节点可以运行服务信息中的服务从而证明用户的身份或者用于所在区域。

第三节点的标识对应的属性，是指第三节点和/或第三节点的拥有者（使用者）所满足的条件，如第三节点所在的区域、或者第三节点的拥有者（使用者）的身份。或者，关于第三节点的标识对应的属性的实现原理可以参考第一标识对应的属性的相关介绍，后续不再赘述。

下述实施例中，关于标识对应的属性、节点对应的属性、的实现可以参考第一标识对应的属性的相关介绍，不再赘述。

第三节点的标识是用于标识第三节点的信息，第三节点的标识可以为一个或多个，其中，第三节点的标识均存在对应的属性。

验证第三节点，是指验证一个节点是否为第三节点、或者验证第三节点的合法性、或者有效性等。验证第三节点的标识对应的属性，是指验证第三节点的标识对应的属性是否真实。

可选地，第一信息还用于指示第一标识对应的凭证信息，第一标识对应的凭证信息用于验证第一节点和/或用于验证第一标识对应的属性。或者说，第一标识对应的凭证信息包括用于验证第一节点的信息，即第一标识对应的认证信息，和/或，用于验证第一标识对应的属性的信息，即第一标识对应的证明信息。可理解，第一标识对应的认证信息用于验证第一节点，第一标识对应的证明信息用于验证第一节点对应的属性。

验证第一节点，是指验证一个节点是否为第一节点、或者验证第三节点的合法性、或者有效性等。关于验证第一节点的实现原理可以参考验证第三节点的相关介绍，此处不再赘述。

验证第一标识对应的属性可以参考验证第三标识对应的属性的相关介绍，此处不再赘述。

在一些可能的例子中，第一标识对应的认证信息可以包括：第一标识对应的公钥、第一标识对应的主体的信息、第一标识对应的签名、第一标识对应的密码算法、第一标识的签发者的信息、第一标识对应的认证信息的有效时间、用于指示第一标识对应的认证信息是否已经撤销的信息。

其中，第一标识对应的公钥可以用于验证信息是否经过第一标识对应的私钥签名。第一标识对应的主体是指第一标识所属的对象。第一标识对应的签名是指对第一标识进行签名得到的信息。第一标识对应的密码算法，也可以称为第一标识对应的密码学套件，包括如下一项或多项：密钥长度、加密算法、解密算法、签名算法、或公共参数等。第一标识的签发者的信息可以用于验证第一标识的签发者的信息，例如，第一标识的签发者的信息可以是第一标识的签发者的公钥。用于指示第一标识对应的认证信息是否已经撤销的信息可以是指示已经被撤销的所有认证信息的信息，如撤销列表（包括所有已经被撤销的认证信息的标识）。

第一标识对应的证明信息也可以称为第一标识对应的证书、第一标识对应的可验证凭证、第一标识对应的可验证证明（verifiable credential, VC）等，此处不再赘述。

第一标识对应的证明信息是根据第四节点的服务信息生成的。

一种可能的设计方案中，第一标识对应的证明信息是由第四节点根据第四节点对应的服务信息生成的，若第一标识是由第四节点生成的，则第一标识对应的证明信息由第四节点对应的私钥签名。第四节点与第一节点不同。

一种可能的实现中，在存储节点为区块链节点的情况下，第四节点可以将第四节点对应的服务信息存储到区块链系统中。服务信息中可以用于指示生成节点的证明信息的服务。

一种可能的实现中，服务信息中指示生成节点的证明信息的服务通过智能合约实现，在此情况下，第一标识的证明信息可以由第四节点调用该智能合约得到。可理解，在此情况下，第一标识的证明信息还可以由第四节点之外的其他节点调用智能合约得到。

一种可能的实现中，第四信息的服务信息中可以指示用于生成标识对应的证明信息的网站的地址，在此情况下，第一标识对应的证明信息可以由第四节点根据网站的地址访问该网站得到的。在此情况下，第一标识对应的证明信息可以由第四节点的私钥签名。

若第一标识是由第一节点的其他标识生成的，则第一标识可以由生成该第一标识的标识所对应的私钥签名。

第四节点对应的服务信息可以是第四节点的标识对应的服务信息，关于第四节点对应的服务信息可以参考第一标识对应的服务信息，此处不再赘述。

5 可选地，第四节点对应的服务信息用于生成服务结果信息，服务结果信息包括第五节点的凭证信息。第五节点与第四节点不同。第五节点的凭证信息用于验证第五节点和/或用于验证第五节点的标识对应的属性。关于第四节点对应的服务信息的实现可以参考第一标识对应的服务信息的实现原理，此处不再赘述。

10 一种可能的实现方式中，第一信息包括第一标识、第一标识对应的服务信息和如下一项或多项：第一标识对应的认证信息、第一标识对应的证明信息用于指示第一节点的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息的公开条件的信息。

可理解，本申请实施例中，信息 A 包括信息 B 可以是指信息 A 包括用于指示信息 B 的信息。

15 其中，第一节点的类型可以是根据第一节点对应的设备的拥有者进行划分的，例如，第一节点的类型可以指第一节点是终端、运营商对应的设备、还是其他的商家对应的设备。可理解，第一节点的类型还可以采用其他方式划分，例如，可以根据第一节点的实现的业务或功能划分，本申请实施例中对此不作限定。

第一标识的签发者也可以说是生成第一标识的主体，如个人、组织或机构。第一标识的签发者的信息可以是用于识别第一标识的签发者的信息，如第一标识的签发者的标识。

20 第一标识对应的凭证信息的公开条件，即可以展示或提供（披露）第一标识对应的凭证信息的条件。例如，第一标识对应的凭证信息的公开条件可以是：可以展示或提供第一标识对应的凭证信息的时间（如时间段），展示或提供第一标识对应的凭证信息的范围（如网络域）、可以展示或提供第一标识对应的凭证信息的场景等。

为便于理解，以下结合第一信息的不同实现方式说明第一信息。

25 实现方式一：第一信息包括第一标识对应的标识信息，第一标识对应的标识信息包括第一标识和第一标识对应的凭证信息。

30 可选地，第一信息还可以包括如下一项或多项：用于指示第一节点的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息公开条件的信息。例如，第一信息还可以包括第一标识对应的文件信息（profile），其中，第一标识对应的文件信息包括：用于指示第一节点的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息公开条件的信息。

可理解，第一标识对应的文件信息可以包括第一标识对应的服务信息。此外，若第一标识对应的凭证信息包括第一标识对应的认证信息，则第一信息还可以包括第一标识对应的证明信息。例如，在第一信息还包括第一标识对应的文件信息的情况下，第一标识对应的文件信息还可以包括第一标识对应的证明信息。

35 以下以第一标识对应的标识信息包括第一认证信息举例进一步说明第一信息。假设第一节点为运营商对应的设备，第一标识为运营商对应的设备的 DRC1，那么，如图 3 中的（a）所示，DRC1 对应的标识信息包括：DRC1、DRC1 对应的公钥、DRC1 对应的有效时间（也可以称为时间戳）、DRC1 对应的签名、DRC1 对应的密码算法（也可以称为验证算法）、用于指示 DRC1 对应的认证信息是否已经撤销的信息等。DRC1 对应的文件信息包括：第一标识对应的主体，如运营商的名称；第一标识对应的服务地域 DRC1 对应的服务信息（即运营商所提供的服务的信息）。其中，DRC1 对应的服务信息中的服务可以包括签约服务、业务服务和证明服务。其中，签约服务是用于为用户提供办理套餐或者办理业务的服务，业务服务是用于为用户进行如下一项或多项的服务：话单查询、资费查询、或位置查询。

40 又如，假设第一节点为终端，第一标识为终端的 DRC2，那么，如图 3 中的（b）所示，第一标识对应的标识信息包括：DRC2、DRC2 对应的公钥、DRC2 对应的有效时间、DRC2 对应的签名、DRC2 对应的密码算法、用于指示 DRC2 对应的认证信息是否已经撤销的信息等。DRC2 对应的文件信息包括：DRC2 对应的证明信息和 DRC2 对应的属性。例如，DRC2 的证明信息可以包括

如下一项或多项：年龄证明、身份证明、学历证明、运营商接入证明。年龄证明用于证明用户的年龄、身份证明用于证明用户的身份、学历证明用于证明用户的学历、运营商接入证明用于证明用户具有接入运营商的权限。第一标识对应的属性用于表示用户是个人用户，还是组织或机构。

5 实现方式二，第一信息包括第一标识对应的标识信息和第一标识对应的文件信息，第一标识对应的标识信息包括第一标识，第一标识对应的文件信息包括第一标识对应的凭证信息。

第一标识对应的文件信息还包括如下一项或多项：用于指示第一节点的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息的公开条件的信息。可理解，第一标识对应的文件信息还包括第一标识的服务信息。

10 应理解，实施方式一和实施方式二中，若第一标识对应的凭证信息中包括第一标识对应的认证信息，则第一标识对应的文件信息中还可以包括第一标识对应的证明信息。若第一标识对应的凭证信息中包括第一标识对应的证明信息，则第一标识对应的文件信息中还可以包括第一标识对应的认证信息。上述实现方式一和实现方式二中的第一信息仅用于举例，实际实施中，第一信息还可以采用其他方式实现，此处不再赘述。

15 一种可能的实现中，若第一节点是终端，则第一标识对应的标识信息是经过卡商或终端厂商生成的第一节点的标识（如，DRC）对应的私钥签名的信息。其中，卡商或终端厂商还可以生成第一节点的标识对应的公钥，且卡商或终端厂商还可以将该第一节点的标识对应的公钥或公钥哈希上传至存储节点，这样，验证节点（如图1中的节点101i）可以从存储节点获取第一节点的标识对应的公钥或公钥哈希，并根据第一节点的标识对应的公钥对第一标识对应的标识信息进行验证，从而实现第一节点的验证或对第一标识对应的属性的验证。

20 S202，第一节点向存储节点发送第一信息。相应的，存储节点接收来自第一节点的第一信息。

本申请实施例中，存储节点为如下一项或多项：区块链节点、分布式存储节点、或通信设备。通信设备与第一节点不同。

25 关于存储节点的实现原理可以参考上述图1所提供的通信系统中的相关介绍，此处不再赘述。以区块链节点为例，在此情况下，S202可以包括：第一节点向区块链节点发送第一信息。相应的，区块链节点接收来自第一节点的第一信息。

以分布式存储节点为例，在此情况下，S202可以包括：第一节点向分布式存储节点中的节点发送第一信息。相应的，分布式存储节点中的节点接收来自第一节点的第一信息。

S203，存储节点存储第一信息。

30 第一信息若存储节点为区块链节点，则第一信息可以按照区块的方式存储在区块链节点内的节点上。若存储节点为分布式存储节点，则第一信息可以存储在分布式存储节点内的节点上。在一些可能的场景下，分布式存储节点可以为区块链节点。

35 基于图2所提供的方法，第一节点可以将第一标识和第一标识对应的服务信息发送至存储节点，这样，便使得存储节点中可以获取到第一节点的第一标识和第一标识对应的服务信息，从而使得其他节点可以通过存储节点获取第一标识对应的服务信息，增加了获取服务信息的渠道，减少了对第一节点的依赖，因此，可以应用于更多场景。

为便于理解，以下结合卡商或终端厂商对应的设备、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器、终端为例，结合不同场景说明上述图2所提供的通信方法。

40 在一些场景中，卡商或终端厂商为终端生成终端的标识和终端的标识对应的凭证信息，图2所提供方法中的第一节点可以为卡商或终端厂商对应的设备、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、空中写卡服务器（图4中未示出）、或终端，在此情况下，本申请实施例提供的通信方法如下图4所示。应理解，实际实施中，第一节点还可以是其他的设备，此处不再赘述。图4为本申请实施例提供的一种通信方法。该通信方法包括：

S401，卡商或终端厂商对应的设备获取信息#1。

45 其中，信息#1包括卡商或终端厂商对应的设备的标识#1和标识#1对应的服务信息，关于标识#1的实现原理可以参考上述图2所提供方法中第一标识的相关介绍，关于标识#1对应的服务信息可以参考上述图2所提供方法中第一标识对应的服务信息的相关介绍，关于信息#1的实现原理

可以参考上述图 2 所提供方法中第一信息的相关介绍，此处不再赘述。

S402，卡商或终端厂商对应的设备向区块链节点发送信息#1。相应的，区块链节点接收来自卡商或终端厂商对应的设备的信息#1。

S403，区块链节点存储信息#1。

5 可理解，信息#1 可以以区块的方式进行存储。应理解，本申请实施例中，在不作特殊说明的情况下，区块链节点存储信息均可以采用区块的方式存储。

S404，卡商或终端厂商对应的设备获取信息#2。

信息#2 用于指示终端的标识#2 和标识#2 对应的凭证信息。其中，信息#2 用于指示终端的标识#2 和标识#2 对应的凭证信息，标识#2 对应的凭证信息用于验证终端和/或标识#2 对应的属性。
10 标识#2 和标识#2 对应的凭证信息是由第一节点生成的。

一种可能的实现方式中，标识#2 对应的凭证信息包括标识#2 对应的认证信息和/或标识#2 对应的证明信息，标识#2 对应的认证信息用于验证终端，标识#2 对应的证明信息用于验证标识#2 对应的属性。标识#2 对应的证明信息由卡商或终端厂商对应的设备的私钥签名。如此，在标识#2 对应的凭证信息包括标识#2 对应的认证信息的情况下，可以实现对终端的身份的验证。在标识#2 对应的凭证信息包括标识#2 对应的证明信息的情况下，可以对标识#2 对应的属性进行验证。
15

一种可能的实现方式中，信息#2 还可以包括如下项或多项：标识#2 对应的服务信息、用于指示终端的类型的信息、标识#2 的签发者的信息、或用于指示标识#2 对应的凭证信息的公开条件的信息。也就是说，信息#2 可以包括标识#2、标识#2 对应的凭证信息，以及如下项或多项：标识#2 对应的服务信息、用于指示终端的类型的信息、标识#2 的签发者的信息、或用于指示标识#2 对应的凭证信息的公开条件的信息。如此，可以将前述一种或多种信息存储至存储节点，使得其他设备根据存储节点中的前述信息获取或提供相应的服务。
20

关于标识#2 对应的认证信息可以参考图 2 所提供方法中第一标识对应的认证信息的相关介绍，标识#2 对应的证明信息可以参考图 2 所提供方法中第一标识对应的证明信息的相关介绍。标识#2 对应的服务信息可以参考图 2 所提供方法中第一标识对应的服务信息的相关介绍，用于指示终端的类型的信息可以参考图 2 所提供方法中用于指示第一节点的类型的信息的相关介绍，标识#2 的签发者的信息可以参考图 2 所提供方法中第一标识的签发者的信息的相关介绍，用于指示标识#2 对应的凭证信息的公开条件的信息可以参考图 2 所提供方法中用于指示第一标识对应的凭证信息的公开条件的信息的相关介绍。
25

为便于理解，以下结合实现方式三和实现方式四说明信息#2。

30 实现方式三，信息#2 包括标识#2 对应的标识信息，标识#2 对应的标识信息包括标识#2 和标识#2 对应的凭证信息。这样，标识#2 的标识信息中就包括认证信息，从而可以根据实际情况构建文件信息，从而使得文件信息更准确。

可选地，信息#2 还包括如下项或多项：标识#2 对应的服务信息、用于指示终端的类型的信息、标识#2 的签发者的信息、或用于指示标识#2 对应的凭证信息的公开条件的信息。可理解，标识#2 对应的服务信息、用于指示终端的类型的信息、标识#2 的签发者的信息、或用于指示标识#2 对应的凭证信息的公开条件的信息均可以位于标识#2 的文件信息中。
35

这样，标识#2 第二标识的标识信息中就包括用于对终端的进行认证的凭证信息，从而可以根据实际情况生成文件信息，从而使得文件信息更准确，且可以减少存储的数据量。

实现方式四，信息#2 包括标识#2 对应的标识信息和标识#2 对应的文件信息，标识#2 对应的标识信息包括标识#2，标识#2 对应的文件信息包括标识#2 对应的凭证信息。
40

例如，标识#2 对应的文件信息还包括如下项或多项：标识#2 对应的服务信息、用于指示终端的类型的信息、标识#2 的签发者的信息、或用于指示标识#2 对应的凭证信息的公开条件的信息。这样，标识#2 的标识信息中仅包括标识#2，可以减小标识#2 对应的标识信息的数据量，降低传输的资源开销。第二标识对应的标识信息与其他信息可以独立存储，或者分别读取，可以减少信息的泄露，从而增强隐私保护，且发布方式更灵活。
45

如图 5 所示，标识#2 对应的标识信息包括第一字段和如下项或多项：第二字段或第三字段，其中，第一字段承载的信息用于指示标识#2，第二字段承载的信息用于指示标识#2 的标识类型，

第三字段承载的信息用于校验标识#2 对应的标识信息中除第三字段之外的字段承载的信息。

其中，标识#2 与标识#2 对应的公钥的哈希值（也可以称为公钥哈希）具有对应关系，或者标识#2 与随机生成的字符之间具有对应关系。第一字段承载的信息可以包括标识#2 对应的公钥的哈希值（简称公钥哈希），或者，第一字段承载的信息可以包括随机生成的字符，从而指示标识#2。

5 应理解，此处公钥哈希和随机生成的字符仅用于举例，实际实施例中，第一字段承载的信息还可以包括其他可以用于指示标识#2 的信息，或者第一字段承载的信息可以包括多种用于指示标识#2 的信息的组合，此处不再赘述。

10 这样，可以通第一字段指示第二标识对应的节点。此外，在第二标识对应的标识信息包括第二字段的情况下，可以确定第二标识的类型，进而可以根据第二标识确定第二标识的来源、可信度或使用场景。在第二标识对应的信息包括第三字段的情况下，可以实现对其他字段，如第一字段，或者第一字段和第二字段的校验，从而确保第二标识的准确性。标识类型是指用于指示标识的生成方式。例如，标识类型可以包括 DRC、DIC、DSCC。其中，不同标识类型可以通过不同的数值或字符串表示。以数值举例，DRC 可以通过数值“0x1101”表示，DIC 可以通过数值“0x1111”表示，DSCC 可以通过数值“0x1001”表示。此处，标识#2 的标识类型可以是 DRC，在此情况下，
15 第二字段中包括数值“0x1101”。

第三字段中承载的信息可以是根据校验方式得到的标识#2 的信息中，除第三字段之外的其他字段的校验值。该校验方式可以是循环冗余校验或者其他可能的校验方式，此处不再赘述。

20 此外，标识#2 对应的标识信息还可以包括用于指示其他信息的字段。例如，标识#2 对应的标识信息还可以包括用于指示标识#2 所属的地区的字段，或者，用于指示生成标识#2 的卡商或设备商的字段。

25 应理解，实施方式三和实施方式四中，若标识#2 对应的凭证信息中只包括标识#2 对应的认证信息，则标识#2 对应的文件信息中还可以包括标识#2 对应的证明信息。若标识#2 对应的凭证信息中只包括标识#2 对应的证明信息，则标识#2 对应的文件信息中还可以包括标识#2 对应的认证信息。此外，实施方式三和实施方式四仅用于举例，实际实施中，信息#2 还可以采用其他方式实现，此处不再赘述。

30 如此，卡商或终端厂商对应的设备可以将信息#2 发送至存储节点，由于卡商或终端厂商对应的设备的服务信息也会上传存储节点，而标识#2 和标识#2 对应的凭证信息由卡商或终端厂商对应的设备生成，可以实现卡商或终端厂商对应的设备对标识#2 以及标识#2 对应的凭证信息的背书，例如，标识#2 和标识#2 对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的，因此，在卡商或终端厂商对应的设备可信的情况下，便可以实现标识#2 和标识#2 对应的凭证信息在不同领域之间的信任互通。

S405，卡商或终端厂商对应的设备向区块链节点发送信息#2。相应的，区块链节点接收来自卡商或终端厂商对应的设备的信息#2。

35 S406，区块链节点存储信息#2。

S407，运营商对应的设备获取信息#3。

其中，信息#3 包括卡商或终端厂商对应的设备的标识#3 和标识#3 对应的服务信息，关于标识#3 的实现原理可以参考上述图 2 所提供方法中第一标识的相关介绍，关于标识#3 对应的服务信息可以参考上述图 2 所提供方法中第一标识对应的服务信息的相关介绍，关于信息#3 的实现原理可以参考上述图 2 所提供方法中第一信息的相关介绍，此处不再赘述。

40 S408，运营商对应的设备向区块链节点发送信息#3。相应的，区块链节点接收来自运营商对应的设备的信息#3。

S409，区块链节点存储信息#3。

S410，权威机构对应的设备获取信息#4。

45 其中，信息#4 包括卡商或终端厂商对应的设备的标识#4 和标识#4 对应的服务信息，关于标识#4 的实现原理可以参考上述图 2 所提供方法中第一标识的相关介绍，关于标识#4 对应的服务信息可以参考上述图 2 所提供方法中第一标识对应的服务信息的相关介绍，关于信息#4 的实现原理可以参考上述图 2 所提供方法中第一信息的相关介绍，此处不再赘述。

S411, 权威机构对应的设备向区块链节点发送信息#4。相应的, 区块链节点接收来自权威机构对应的设备的信息#4。

S412, 区块链节点存储信息#4。

S413, 第三方可信机构对应的设备获取信息#5。

5 其中, 信息#5 包括卡商或终端厂商对应的设备的标识#5 和标识#5 对应的服务信息, 关于标识#5 的实现原理可以参考上述图 2 所提供方法中第一标识的相关介绍, 关于标识#5 对应的服务信息可以参考上述图 2 所提供方法中第一标识对应的服务信息的相关介绍, 关于信息#5 的实现原理可以参考上述图 2 所提供方法中第一信息的相关介绍, 此处不再赘述。

10 S414, 第三方可信机构对应的设备向区块链节点发送信息#5。相应的, 区块链节点接收来自第三方可信机构对应的设备的信息#5。

S415, 区块链节点存储信息#5。

此外, 图 4 所提供的方法还可以包括:

15 S416, 卡商或终端厂商对应的设备获取信息#2 在区块链系统中的存储位置, 即链上地址。也可说是存储系统中的位置。可以理解, 本申请实施例中, 存储节点可以将信息存储至存储系统中的其他存储节点。例如, 区块链节点可以将信息存储至区块链中的其他区块链节点, 信息可以以区块的方式存储, 即将信息上链。

可以理解, 信息#2 在区块链系统中的存储位置可以是区块链系统在接收到信息#2 并存储信息#2 之后, 发送给卡商或终端厂商对应的设备的。

20 S417, 卡商或终端厂商对应的设备向终端发送信息#2。相应的, 终端接收来自卡商或终端厂商对应的设备的信息#2,

可以理解, S417 中与信息#2 一起发送的, 还可以包括信息#2 在区块链系统中的存储位置。

其中, 信息#2 与信息#2 在区块链系统中的存储位置可以携带在同一个消息或不同消息中。

此外, 终端可以存储信息#6。

S418, 终端根据信息#2 获取信息#6。

25 其中, 信息#6 包括标识#6 和标识#6 对应的服务信息。

以 DRC 和 DIC 举例, 一种可能的实现方式中, 终端可以自行生成 DIC 的公私钥, 然后用 DRC 的私钥对 DIC 的信息进行签名背书, 背书的内容包括 DIC 的 ID、公钥、有效期等信息。

一种可能的实现方式中, 也可以是终端生成 DIC 对应的公钥, 用 DIC 对应的公钥哈希做 DIC 的标识, 然后由 DRC 对应的系统密钥和 DIC 的公钥生成 DIC 的私钥。

30 关于信息#6 的实现原理可以参考第一信息的相关介绍, 此处, 标识#6 可以是终端的 DIC。该 DIC 是由终端根据标识#2 生成的。

在 S418 中, 终端根据标识#2 可以生成多个终端的标识。例如, 如图 6 所示, 标识#2 为 DRC, 那么, 终端根据该 DRC 可以生成多个 DIC, 如 DIC1 和 DIC2, 以及 DIC1 对应的文件信息至 DIC2 对应的文件信息。在此情况下, 终端中可以存储 DRC、DRC 对应的文件信息 (文件信息 1)、DIC1 至 DIC3、以及 DIC1 对应的文件信息 (文件信息 2) 和 DIC2 对应的文件信息 (文件信息 3)。其中, 各个文件信息中均可以包括证明标识 (用于标识证明信息, 与证明信息具有对应关系)、证明信息和验证信息 (用于指示证明信息的验证方法, 如验证证明信息的算法) (图中未示出) 例如, 文件信息 1 可以包括证明信息 11, 文件信息 2 可以包括证明信息 21, 文件信息 3 可以包括证明信息 31 和证明信息 32, 文件信息 4 可以包括证明信息 41 和证明信息 42, 文件信息 5 可以包括证明信息 51。在此情况下, 标识#可以是 DIC1 或 DIC2。

35 其中, 终端的 DRC、DIC1、DIC2、文件信息 1 至文件信息 3 之间的关系如图 7 所示。其中, 终端的 DRC 对应的文件信息中的证明信息可以由卡商或终端厂商对应的私钥签名。终端的 DIC 可以由终端的 DRC 对应的私钥签名。

45 一种可能的设计方案中, 信息#6 可以是信息#2。在此情况下, S418 可以是终端从自身存储的信息中读取信息#2。

一些可能的实现方式中, 在验证节点需要对终端进行验证的情况下, 如图 7 所示, 终端可以通过应用程序 (application, APP) 的界面呈现 (展示) 证明信息, 如呈现证明信息 11、证明信息

21、证明信息 31 和证明信息 32 中的一个或多个。验证节点可以获取终端展示的证明信息（如通过扫码获取），验证节点得到终端展示的证明信息后，可以从区块链节点中获取公钥，从而基于该公钥对证明信息进行验证。

S419，终端发送信息#6。相应的，区块链节点接收信息#6。

5 S420，区块链系统存储信息#6。

为便于理解，以下结合图 4 所提供的方法中的标识和信息说明第一节点和第一标识之间的对应关系。图 4 所提供的方法中的标识与图 2 中的第一标识、图 4 所提供的方法中的信息与第一信息之间的对应关系可以参考如表 1 所示。

表 1

第一节点	卡商或终端厂商对应的设备	终端	运营商对应的设备	权威机构对应的设备	第三方可信机构对应的设备
第一标识	信息#1	信息#2 或信息#6	信息#3	信息#4	信息#5

10 以下结合具体文字分别进行说明，对于图 2 所提供的方案而言，一些可能的实现方式中，第一节点可以为卡商或终端厂商对应的设备，此时，信息#1 为第一信息，标识#1 为第一标识，信息#2 为第二信息，标识#2 为第二标识，信息#2、或者信息#2 和信息#2 在区块链系统中的存储位置为第三信息。S417 中，卡商或终端厂商对应的设备向终端发送信息#2、或者信息#2 和信息#2 在区块链节点，也可以说，第一节点向终端发送第三信息。由于第三信息可以指示信息#2，因此终端可以获取并使用第二信息，用于其他节点对终端的认证。这样，使得终端可以获取到第二信息，从而能够使用第二信息实现其他节点对终端的认证。

15 在此情况下，卡商或终端厂商对应的设备还可以向区块链节点发送信息#2 的哈希值（信息#2 的哈希值可以与信息#2 携带在同一个消息或不同消息中），或者，信息#2 可以替换为信息#2 的哈希值。

20 如此，卡商或终端厂商对应的设备可以将第二信息发送至存储节点，由于卡商或终端厂商对应的设备的服务信息也会上传存储节点，而标识#2 和标识#2 对应的凭证信息由卡商或终端厂商对应的设备生成，可以实现卡商或终端厂商对应的设备对标识#2 和标识#2 对应的凭证信息的背书，例如标识#2 和标识#2 对应的凭证信息可以由卡商或终端厂商对应的设备对应的私钥签名的，可以实现卡商或终端厂商对应的设备对标识#2 以及标识#2 对应的凭证信息的背书，因此，在卡商或终端厂商对应的设备可信的情况下，便可以实现标识#2 和标识#2 对应的凭证信息在不同领域之间的信任互通。

25 一些可能的实现方式中，第一节点为运营商对应的设备，此时，第一信息为信息#3，标识#3 为第一标识。

30 一些可能的实现方式中，第一节点为权威机构对应的设备，此时，第一信息为信息#4，标识#4 为第一标识。

一些可能的实现方式中，第一节点为第三方可信机构对应的设备，此时，第一信息为信息#5，标识#5 为第一标识。

35 一些可能的实现方式中，第一节点为终端，此时，第一信息为信息#6，标识#6 为第一标识，第四信息为信息#2 和/或信息#2 在区块链系统上的存储位置。S417 中，终端接收来自卡商或终端厂商对应的设备的信息#2 和/或信息#2 在区块链系统上的存储位置，即第一节点接收来自卡商或终端厂商对应的设备的第四信息。这样，便使得终端可以获取到信息#6，并能够使用信息#6 进行认证。

40 可理解，上述区块链节点可以替换为存储节点中的任意一种可能实现方式，此处不再赘述。关于图 4 所提供的方法的技术效果可以参考上述图 2 所提供的方法的技术效果，此处不再赘述。

应理解，本申请实施例中并不限定各个步骤的执行顺序，只要符合逻辑即可，例如，区块链节点存储信息的流程位于区块链节点接收该信息之后，一个信息的发送过程位于该信息的获取过

程之后。

在一些可能场景中，上述图 4 所提供方法中的信息#2 可以存储在终端中，例如，可以由卡商或终端厂商对应的设备提供给终端中。图 2 所提供方法中的第一节点可以为卡商或终端厂商对应的设备、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、空中写卡服务器、或终端。在此情况下，本申请实施例所提供的通信方法还可以包括上述图 4 所提供的方法的步骤，其区别在于，一种可能的实现中，该通信方法还包括：卡商或终端厂商对应的设备可以发送信息#2。相应的，终端可以接收来自卡商或终端厂商对应的设备的信息#2。一种可能的实现中，S405 可以替换为：终端发送信息#2。相应的，区块链节点接收信息#2。也就是说，信息#2 可以由终端发送至区块链节点。应理解，在此场景中，可以不包括 S404。即信息#2 由终端生成。若第一节点为终端，则信息#2 为第一信息，标识#2 为第一标识，信息#6 为第五信息，标识#6 为第三标识。这样，第一节点便可以向存储节点发送指示第一节点的不同标识以及不同标识对应的凭证信息，从而可以针对不同的标识使用不同的服务，从而使得隐私性更好。此外，关于该场景中的通信方法技术效果，可以参考图 2 所提供的方法的技术效果，此处不再赘述。此外，终端还可以向存储节点发送信息#6 的哈希值，此时，信息#6 的哈希值与信息#6 可以承载在同一消息或不同消息中。或者，S419 和 S420 中信息#6 也可以替换为信息#6 的哈希值。

可理解，上述区块链节点可以替换为存储节点中的任意一种可能实现方式，此处不再赘述。

在一些可能的场景中，图 4 所提供方法中的第一节点可以为终端，在此情况下，本申请实施例提供的通信方法如图 4 中所提供的方法所示，其区别在于，S403 和 S404 中的信息#2 替换为信息#7，即第六信息。其中，信息#7 的实现可以参考信息#2。信息#7 与第一信息的区别在于，信息#7 中可以不包括服务信息。信息#7 用于指示终端的标识#7，即第四标识和标识#7 对应的凭证信息，标识#7 对应的凭证信息用于验证终端和/或标识#7 对应的属性，标识#7 和标识#7 对应的凭证信息是由卡商或终端厂商对应的设备生成的。此外，终端还可以向存储节点发送信息#7 的哈希值，此时，信息#7 的哈希值与信息#7 可以承载在同一消息或不同消息中。或者，S403 和 S404 中信息#7 也可以替换为信息#7 的哈希值。

其中，信息#7 用于指示终端，即第二节点的标识#7 和标识#7 对应的凭证信息，标识#7 对应的凭证信息用于验证终端和/或标识#7 对应的属性。标识#7 和标识#7 对应的凭证信息是由卡商或终端厂商对应的设备生成的。其中，信息#7 用于指示终端的标识#7 和标识#7 对应的凭证信息，标识#7 对应的凭证信息用于验证终端和/或标识#7 对应的属性。标识#7 和标识#7 对应的凭证信息是由第一节点生成的。

可选地，标识#7 对应的凭证信息包括标识#7 对应的认证信息和/或证明信息，标识#7 对应的认证信息用于验证终端，标识#7 对应的证明信息用于验证标识#7 对应的属性。

一种可能的实现方式中，信息#6 还可以包括如下一项或多项：标识#7 对应的服务信息、用于指示终端的类型的信息、标识#7 的签发者的信息、或用于指示标识#7 对应的凭证信息的公开条件的信息。也就是说，信息#6 可以包括标识#7、标识#7 对应的凭证信息，以及如下一项或多项：标识#7 对应的服务信息、用于指示终端的类型的信息、标识#7 的签发者的信息、或用于指示标识#7 对应的凭证信息的公开条件的信息。

关于标识#7 对应的认证信息可以参考图 2 所提供方法中第一标识对应的认证信息的相关介绍，标识#7 对应的证明信息可以参考图 2 所提供方法中第一标识对应的证明信息的相关介绍。标识#7 对应的服务信息可以参考图 2 所提供方法中第一标识对应的服务信息的相关介绍，用于指示终端的类型的信息可以参考图 2 所提供方法中用于指示第一节点的类型的信息的相关介绍，标识#7 的签发者的信息可以参考图 2 所提供方法中第一标识的签发者的信息的相关介绍，用于指示标识#7 对应的凭证信息的公开条件的信息可以参考图 2 所提供方法中用于指示第一标识对应的凭证信息的公开条件的信息的相关介绍。

一种可能的实现方式中，信息#7 包括标识#7 对应的标识信息，标识#7 对应的标识信息包括标识#7 和标识#7 对应的凭证信息。

进一步地，信息#7 还用于指示如下一项或多项：用于指示终端的类型的信息、标识#7 的签发者的信息、或用于指示标识#7 对应的凭证信息的公开条件的信息。也可以说，标识#7 对应的文件

信息包括如下一项或多项用于指示终端的类型的信息、标识#7的签发者的信息、或用于指示标识#7对应的凭证信息的公开条件的信息。

关于信息#7的实现原理可以参考上述实现方式三中的相关介绍,其区别在于,信息#7中不包括标识#7对应的服务信息。

5 一种可能的实现方式中,信息#7包括标识#7对应的标识信息和标识#7对应的文件信息,标识#7对应的标识信息包括标识#7,标识#7对应的文件信息包括标识#7对应的凭证信息。

可选地,标识#7对应的文件信息还包括如下一项或多项:用于指示终端的类型的信息、标识#7的签发者的信息、用于指示标识#7对应的凭证信息的公开条件的信息。关于信息#7的实现原理可以参考上述实现方式四中的相关介绍,其区别在于,信息#7中不包括标识#7对应的服务信息。

10 可选地,标识#7对应的标识信息包括第四字段和如下一项或多项:第五字段或第六字段,其中,第四字段承载的信息用于指示标识#7,第五字段承载的信息用于指示标识#7的标识类型,第六字段承载的信息用于校验标识#7对应的标识信息中除第六字段之外的字段承载的信息。

关于第五字段的实现原理可以参考第一字段的相关介绍,关于第六字段的实现原理可以参考第二字段的相关介绍,关于第七字段的实现原理可以参考第三字段的相关介绍,关于标识#7对应的标识信息可以参考信息#2对应的标识信息,此处不再赘述。

15 可选地,信息#7包括标识#7和如下一项或多项:标识#7对应的服务信息、用于指示终端的类型的信息、标识#7的签发者的信息、或用于指示标识#7对应的凭证信息的公开条件的信息。

应理解,在此场景下,第一节点为卡商或终端厂商对应的设备、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、空中写卡服务器时,第一信息的实现原理可以对应参考图2中第一节点为卡商或终端厂商对应的设备、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、空中写卡服务器时的相关介绍,此处不再赘述。

20 在一些场景中,第一节点可以是终端自行生成终端的标识和终端的标识对应的凭证信息,图2所提供方法中的第一节点可以为终端,在此情况下,本申请实施例提供的通信方法如下图8所示。如图8所示,该通信方法包括:

25 S801,卡商或终端厂商对应的设备生成信息#1。

关于信息#1的实现原理可以参考上述图4所提供方法中信息#1的相关介绍。

S802,卡商或终端厂商对应的设备向区块链节点发送信息#1。相应的,区块链节点接收来自卡商或终端厂商对应的设备的信息#1。

S803,运营商对应的设备获取信息#3。

30 关于信息#3的实现原理可以参考上述图4所提供方法中信息#3的相关介绍。

S804,运营商对应的设备向区块链节点发送信息#3。相应的,区块链节点接收来自运营商对应的设备的信息#3。

S805,社会权威机构对应的设备获取信息#4。

关于信息#4的实现原理可以参考上述图4所提供方法中信息#4的相关介绍。

35 S806,社会权威机构对应的设备向区块链节点发送信息#4。相应的,区块链节点接收来自权威机构对应的设备的信息#4。

S807,第三方可信机构对应的设备获取信息#5。

关于信息#5的实现原理可以参考上述图4所提供方法中信息#5的相关介绍。

40 S808,第三方可信机构对应的设备向区块链节点发送信息#5。相应的,区块链节点接收来自第三方可信机构对应的设备的信息#5。

S809,终端获取信息#8。

其中,信息#8包括标识#8和标识#8对应的服务信息。

关于信息#8的实现原理可以参考图2所提供方法中第一信息的相关介绍,此处标识#8可以终端自行生成的标识,如DSCC。

45 S810,终端向区块链节点发送信息#8。相应的,区块链节点接收来自终端的信息#8。

S811,终端向卡商或终端厂商对应的设备发送证明请求信息。相应的,卡商或终端厂商对应的设备接收来自终端的证明请求信息。

其中，证明请求信息用于请求终端对应的证明信息，终端对应的证明信息用于验证终端或终端的标识对应的属性。

一些可能的设计中，证明请求信息中可以携带用于可以向卡商或终端厂商证明终端的身份的信息，如终端卡商为终端提供的白名单（包括用于标识卡商或终端厂商生产的设备的信息）或者购买凭证等。例如，可以使得卡商或终端厂商为终端背书，从而使得在卡商或设备厂商可信任的情况下，终端可以通过证明信息进行验证。

S812，卡商或终端厂商对应的设备向区块链节点发送终端对应证明信息。相应的，区块链节点接收终端对应的证明信息。

其中，终端对应的证明信息是由卡商或终端厂商对应的设备根据证明请求信息得到的。

S813，卡商或终端厂商对应的设备发送终端对应的证明信息。相应的，终端接收终端对应的证明信息。

为便于理解，以下结合图 8 所提供的方法中的标识和信息说明第一节点和第一标识之间的对应关系。图 8 所提供的方法中的标识与图 2 中的第一标识、图 4 所提供的方法中的信息与第一信息之间的对应关系可以参考如下表 2 所示。

表 2

第一节点	卡商或终端厂商对应的设备	终端	运营商对应的设备	权威机构对应的设备	第三方可信机构对应的设备
第一标识	信息#1	信息#8	信息#3	信息#4	信息#5

以下结合具体文字分别进行说明，对于图 2 所提供的方案，若第一节点为卡商或终端厂商对应的设备，则信息#1 为第一信息，标识#1 为第一标识，证明请求信息为证明请求信息。

若第一节点为运营商对应的设备，则第一信息为信息#3，标识#3 为第一标识。

若第一节点为权威机构对应的设备，则第一信息为信息#4，标识#4 为第一标识。

若第一节点为第三方可信机构对应的设备，则第一信息为信息#5，标识#5 为第一标识。

若第一节点为终端，则第一信息为信息#8，标识#8 为第一标识。终端对应的证明信息即第一节点对应的证明信息。

图 8 所提供的方案中，标识#8 可以为一个或多个。例如，如图 6 所示，标识#8 可以包括 DSCC1 和 DSCC2。如图 6 所示，终端中可以存储 DSCC1、DSCC1 对应的文件信息 4、DSCC2 和 DSCC2 对应的文件信息 5。文件信息 4 可以包括证明信息 41 和证明信息 42，文件信息 5 可以包括证明信息 51。应理解，图 6 中所示的文件信息和证明信息仅用于举例，实际实施中，还可以包括更多或更少的证明信息。可理解，如图 7，终端可以通过 APP 展示文件信息 5 和文件信息 4 中的证明信息。

可理解，图 8 所提供的方案中，还可以包括图 4 所提供方案中 S416 和 S417。图 8 所提供的方案中，还可以包括图 4 所提供方案中的 S418 至 S420，具体实现可以参考图 4 中的相关介绍，此处不再赘述。在此情况下，终端中可以存储有终端的 DRC、DIC1、DIC2、DSCC1、DSCC1 以及终端的 DRC、DIC1、DIC2、DSCC1、DSCC1 各自对应的文件信息。关于图 8 所提供的方法的技术效果可以参考上述图 2 所提供的方法的技术效果，此处不再赘述。此外，基于图 8 所提供的方案，第二节点可以获取第六信息并自行上传第六信息，可以提高第二节点对自身标识和凭证信息，如第六信息的把控程度。

一种可能的实施例中，运营商对应的设备可以获取与终端的已有标识对应的另一标识，并向终端发送与终端的已有标识对应的另一标识。在此情况下，本申请实施例还提供一种通信方法，以下结合图 9 说明该通信方法。如图 9 所示，该通信方法包括：

S901，运营商对应的设备获取第七信息。

其中，第七信息用于指示终端的第五标识和第五标识对应的凭证信息，第五标识对应的凭证信息用于验证终端和/或第五标识对应的属性，第五标识与运营商对应的设备中终端的用户永久标识，如用户永久标识符（subscription permanent identifier，SUPI）不同，且第五标识与终端的用户永久标识对应，用户永久标识用于运营商对应的设备与终端之间的通信。

运营商对应的设备可以为运营商对应的设备，例如，运营商对应的设备可以是运营商的核心网中的设备（核心网网元），或者，运营商对应的设备可以是运营商的接入网设备。

终端可以是终端。关于终端的实现原理可以参考图 1 所提供的通信系统中的相关介绍，此处不再赘述。

5 终端的第五标识是用于标识终端的信息。例如，终端的第五标识可以是终端的 DSCC。可理解，本申请实施例中，第五标识 DSCC 仅用于举例，实际实施中，第五标识还可以有其他名称，此处不再赘述。

终端的第五标识可以是根据终端的根凭证，如 DRC 生成的。第五标识对应的凭证信息可以包括第五标识对应的认证信息和/或第五标识对应的证明信息。

10 其中，第五标识对应的认证信息用于验证终端，第五标识对应的证明信息用于验证终端对应的属性。

终端的用户永久标识用于在终端与运营商对应的设备通信过程中用于标识终端。例如，在运营商对应的设备为卡商或终端厂商对应的设备，终端为终端时，用户永久标识可以是卡商或终端厂商对应的设备根据 DRC 生成的终端的 SUPI。

15 一种可能的实现方式中，第七信息还可以包括如下项或多项：第五标识对应的服务信息、用于指示终端的类型的信息、第五标识的签发者的信息、或用于指示第五标识对应的凭证信息的公开条件的信息。也就是说，第七信息可以包括第五标识、第五标识对应的凭证信息，以及如下项或多项：第五标识对应的服务信息、用于指示终端的类型的信息、第五标识的签发者的信息、或用于指示第五标识对应的凭证信息的公开条件的信息。

20 关于第五标识对应的认证信息可以参考图 2 所提供方法中第一标识对应的认证信息的相关介绍，第五标识对应的证明信息可以参考图 2 所提供方法中第一标识对应的证明信息的相关介绍。第五标识对应的服务信息可以参考图 2 所提供方法中第一标识对应的服务信息的相关介绍，用于指示终端的类型的信息可以参考图 2 所提供方法中用于指示第一节点的类型的信息的相关介绍，第五标识的签发者的信息可以参考图 2 所提供方法中第一标识的签发者的信息的相关介绍，用于指示第五标识对应的凭证信息的公开条件的信息可以参考图 2 所提供方法中用于指示第一标识对应的凭证信息的公开条件的信息的相关介绍。

25 一种可能的实现方式中，第七信息包括第五标识对应的标识信息，第五标识对应的标识信息包括第五标识和第五标识对应的凭证信息。此外第七信息还可以包括如下项或多项：第五标识对应的服务的信息、用于指示终端的类型的信息、第五标识的签发者的信息、或用于指示第五标识对应的凭证信息的公开条件的信息。在此情况下，第七信息的实现可以参考实现方式三的相关介绍，此处不再赘述。

一种可能的实现方式中，第七信息包括第五标识对应的标识信息和第五标识对应的文件信息，第五标识对应的标识信息包括第五标识，第五标识对应的文件信息包括第五标识对应的凭证信息。

30 可选地，第五标识对应的文件信息还包括如下项或多项：第五标识对应的服务的信息、用于指示终端的类型的信息、第五标识的签发者的信息、用于指示第五标识对应的凭证信息的公开条件的信息。在此情况下，第七信息的实现可以参考实现方式四的相关介绍，此处不再赘述。

可选地，第五标识对应的标识信息包括第七字段和如下项或多项：第八字段或第九字段，其中，第七字段承载的信息用于指示第五标识，第八字段承载的信息用于指示第五标识的标识类型，第九字段承载的信息用于校验第五标识对应的标识信息中除第九字段之外的字段承载的信息。

40 关于第七字段的实现原理可以参考图 2 所提供的方法中第一字段的相关介绍，关于第八字段的介绍可以参考图 2 所提供的方法中第二字段的相关介绍，关于第九字段的介绍可以参考图 2 所提供的方法中第三字段的相关介绍，此处不再赘述。

S902，运营商对应的设备向终端发送第七信息。相应的，终端接收来自运营商对应的设备的第七信息。

45 S903，终端存储第七信息。

应理解，终端可以将第七信息存储在终端的内存中。

基于上述图 9 所提供的通信方法，运营商对应的设备可以生成终端的第五标识和第五标识对

应的凭证信息，由于第五标识与终端的用户永久标识对应，因此，运营商对应的设备可以对终端的信息进行集中管理。

在一些可能实施例中，节点可以上传自身的信息以及该节点生成的其他节点的信息。以下结合图 10 的通信方法说明。如图 10 所示，该通信方法包括：

5 S1001，卡商或终端厂商对应的设备获取第八信息和第九信息。

其中，第八信息包括用于指示卡商或终端厂商对应的设备的第七标识，以及第七标识对应的凭证信息，第七标识对应的凭证信息用于验证卡商或终端厂商对应的设备和/或用于验证第七标识对应的属性；第九信息用于指示终端的第八标识和第八标识对应的凭证信息，第八标识对应的凭证信息用于验证终端和/或第八标识对应的属性；第八标识和第八标识对应的凭证信息是由卡商或终端厂商对应的设备生成的即第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的。卡商或终端厂商对应的设备向存储节点发送第八信息和第九信息。

卡商或终端厂商对应的设备为可以为运营商对应的设备，例如，卡商或终端厂商对应的设备可以是运营商的核心网中的设备（核心网网元），或者，卡商或终端厂商对应的设备可以是运营商的接入网设备。

15 关于终端的实现原理可以参考图 1 所提供的通信系统中的相关介绍，此处不再赘述。关于第八信息、第九信息的实现原理均可以参考上述图 4 所提供方案中信息#2 的相关介绍，此处不再赘述。

可理解，卡商或终端厂商对应的设备可以分别获取第八信息和第九信息。

S1002，卡商或终端厂商对应的设备向区块链节点发送第八信息和第九信息。

20 可理解，第八信息和第九信息可以一起发送，也可以分别发送。也就是说，第八信息和第九信息可以承载于同一个消息或信令中，也可以分别承载于不同的消息或信令中。

S1003，区块链节点存储第八信息和第九信息。

其中，第八信息和第九信息可以按照区块存储。

S1004，卡商或终端厂商对应的设备向终端发送第九信息。

25 可选地，卡商或终端厂商对应的设备还可以向终端发送第九信息的存储位置。其中，第九信息的存储位置与第九信息可以携带在同一个消息中，也可以携带在不同的消息中。第九信息的存储位置是执行 S1003 后确定的，例如，区块链节点可以向卡商或终端厂商对应的设备反馈信息，指示第九信息的存储位置，该位置可以是区块链系统中的位置。

S1005，终端存储第九信息。

30 应理解，图 10 所提供方案中的卡商或终端厂商对应的设备，还可以是其他可以生成第九信息的设备，如运营商对应的设备。终端还可以是其他可以接收第九信息的设备，此处不再赘述。

基于图 10 所提供的方法，卡商或终端厂商对应的设备可以将第八信息和第九信息发送至存储节点，存储节点可以存储第八信息和第九信息，而第八标识和第八标识对应的凭证信息由卡商或终端厂商对应的设备生成，而第八标识和第八标识对应的凭证信息由卡商或终端厂商对应的设备生成，第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的，因此，在卡商或终端厂商对应的设备可信的情况下，便可以实现第八标识和第八标识对应的凭证信息在不同领域之间的信任互通。

40 可理解，图 10 所提供的方案中，还可以包括如图 4 所提供的方案中 S407 至 S415，和/或 S418 至 S420。在图 10 所提供的方案中包括如图 4 所提供的方案中 S407 至 S415 的情况下，信息#1、信息#3、信息#4、信息#5 的实现原理可以参考上述图 4 所提供方案中信息#2 的相关介绍，也就是说，信息#1、信息#3、信息#4、或信息#5 中可以不包括标识对应的服务信息。

以上结合图 3-图 10 详细说明了本申请实施例提供的通信方法。以下结合图 11-图 12 详细说明用于执行本申请实施例提供的通信方法的通信装置。

45 以上结合图 2-图 10 详细说明了本申请实施例提供的通信方法。以下结合图 11-图 12 详细说明用于执行本申请实施例提供的通信方法的通信装置。

示例性地，图 11 是本申请实施例提供的通信装置的结构示意图一。如图 11 所示，通信装置 1100 包括：处理模块 1101 和收发模块 1102。为了便于说明，图 11 仅示出了该通信装置 1100 的

主要部件。

一些实施例中，通信装置 1100 可适用于图 1 中所示出的通信系统中，执行图 2、或图 4 中所示出的通信方法中第一节点的功能。

其中，处理模块 1101，用于获取第一信息。其中，第一信息包括第一标识和第一标识对应的服务信息。收发模块 1102，用于向存储节点发送第一信息。

一种可能的实现方式中，第一节点可以包括一项或多项：卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器。

一种可能的实现方式中，若第一节点为卡商或终端厂商对应的设备，则处理模块 1101，还用于获取第二信息。第二信息用于指示终端的第二标识和第二标识对应的凭证信息，第二标识对应的凭证信息用于验证终端和/或第二标识对应的属性。第二标识和第二标识对应的凭证信息是由第一节点生成的。收发模块 1102，还用于向存储节点发送第二信息和/或第二信息的哈希值。

一种可能的实现方式中，第二标识对应的凭证信息包括第二标识对应的认证信息和/或第二标识对应的证明信息，第二标识对应的认证信息用于验证终端；第二标识对应的证明信息用于验证第二标识对应的属性。

一种可能的实现方式中，第二信息包括第二标识，和如下一项或多项：第二标识对应的凭证信息，第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第二标识和第二标识对应的凭证信息携带在第二标识对应的标识信息中；或者，第二标识携带在第二标识对应的标识信息中，第二标识对应的凭证信息、第二标识对应的服务信息、用于指示终端的类型的信息、第二标识的签发者的信息、或用于指示第二标识对应的凭证信息的公开条件的信息中的一项或多项携带在第二标识对应的文件信息中。

一种可能的实现方式中，第二标识对应的标识信息包括第一字段和如下一项或多项：第二字段或第三字段，其中，第一字段承载的信息用于指示第二标识，第二字段承载的信息用于指示第二标识的标识类型，第三字段承载的信息用于校验第二标识对应的标识信息中除第三字段之外的字段承载的信息。

一种可能的实现方式中，收发模块 1102，还用于向终端发送第三信息。第三信息用于指示第二信息，或者，第三信息用于指示第二信息和第二信息在存储系统中的存储位置。

一种可能的实现方式中，若第一节点为终端，则收发模块 1102，还用于接收来自卡商或终端厂商对应的设备的第四信息。其中，第四信息用于指示第一标识和第一标识对应的凭证信息；或者，第四信息用于指示第一标识、第一标识对应的凭证信息，以及第一标识和第一标识对应的凭证信息在存储系统中的存储位置。

一种可能的实现方式中，收发模块 1102，还用于向存储节点发送第五信息和/或第五信息的哈希值。其中，第五信息用于指示第一节点的第三标识和第三标识对应的凭证信息，第三标识与第一标识不同。

一种可能的实现方式中，若第一节点为终端，则收发模块 1102，还用于向卡商或终端厂商对应的设备发送证明请求信息。其中，证明请求信息用于请求第一节点对应的证明信息，第一节点对应的证明信息用于验证第一节点或第一节点的标识对应的属性。收发模块 1102，还用于接收第一节点对应的证明信息。第一节点对应的证明信息是卡商或终端厂商对应的设备生成的。

一种可能的实现方式中，若第一节点为卡商或终端厂商对应的设备，则收发模块 1102，还用于接收来自终端的证明请求信息。其中，证明请求信息用于请求终端对应的证明信息，终端对应的证明信息用于验证终端或终端的标识对应的属性。收发模块 1102，还用于向存储节点发送终端对应的证明信息。收发模块 1102，还用于向终端发送终端对应的证明信息。

可选地，收发模块 1102 可以包括接收模块和发送模块（图 11 中未示出）。其中，收发模块 1102 用于实现通信装置 1100 的发送功能和接收功能。

可选地，通信装置 1100 还可以包括存储模块（图 11 中未示出），该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时，使得通信装置 1100 可以执行图 2、或图 4 所示出的通信方法中第一节点的功能。

应理解，通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块 1102 可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

5 需要说明的是，通信装置 1100 可以是终端或网络设备，也可以是可设置于终端或网络设备中的芯片（系统）、或其他部件或组件或者软件模块，还可以是包含终端或网络设备的装置，本申请对此不做限定。

此外，通信装置 1100 的技术效果可以参考图 2、或图 4 中任一项所示出的通信方法的技术效果，此处不再赘述。

10 一些实施例中，通信装置 1100 可适用于图 1 中所示出的通信系统中，执行图 2、图 4 或图 8 中所示出的通信方法中存储节点的功能。

处理模块 1101，用于通过收发模块 1102 接收来自第一节点的第二信息。其中，第二信息包括第二标识和第二标识对应的服务信息。处理模块 1101，用于存储第二信息。

一种可能的实现方式中，第一节点可以包括一项或多项：卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器。

15 一种可能的实现方式中，若第一节点包括卡商或终端厂商对应的设备，则收发模块 1102，还用于接收来自第一节点的第三信息。第三信息用于指示终端的第三标识和第三标识对应的凭证信息，第三标识对应的凭证信息用于验证终端和/或第三标识对应的属性。第三标识和第三标识对应的凭证信息是由第一节点生成的。处理模块 1101，还用于存储第四信息。

20 一种可能的实现方式中，第三标识对应的凭证信息包括第三标识对应的认证信息和/或第三标识对应的证明信息，第三标识对应的认证信息用于验证终端；第三标识对应的证明信息用于验证第三标识对应的属性。

一种可能的实现方式中，第三信息包括第三标识，和如下一项或多项：第三标识对应的凭证信息，第三标识对应的服务信息、用于指示终端的类型的信息、第三标识的签发者的信息、或用于指示第三标识对应的凭证信息的公开条件的信息。

25 一种可能的实现方式中，第三标识和第三标识对应的凭证信息携带在第三标识对应的标识信息中；或者，第三标识携带在第三标识对应的标识信息中，第三标识对应的凭证信息、第三标识对应的服务信息、用于指示终端的类型的信息、第三标识的签发者的信息、或用于指示第三标识对应的凭证信息的公开条件的信息中的一项或多项携带在第三标识对应的文件信息中。

30 一种可能的实现方式中，第三标识对应的标识信息包括第一字段和如下一项或多项：第二字段或第三字段，其中，第一字段承载的信息用于指示第三标识，第二字段承载的信息用于指示第三标识的标识类型，第三字段承载的信息用于校验第三标识对应的标识信息中除第三字段之外的字段承载的信息。

一种可能的实现方式中，存储节点接收来自第一节点的第五信息。其中，第五信息用于指示第一节点的第四标识和第四标识对应的凭证信息。

35 一种可能的实现方式中，若第一节点包括卡商或终端厂商对应的设备，则收发模块 1102，还用于接收来自第一节点的终端对应的证明信息。其中，终端对应的证明信息用于验证终端或终端的标识对应的属性。

一种可能的实现方式中，收发模块 1102，还用于接收来自第二节点的第六信息。其中，第六信息用于指示第二节点的第五标识和第五标识对应的凭证信息，第五标识对应的凭证信息用于验证第二节点和/或第五标识对应的属性。第五标识和第五标识对应的凭证信息是由第一节点生成的。处理模块 1101，还用于存储第六信息。

40 一种可能的实现方式中，第五标识对应的凭证信息包括第五标识对应的认证信息和/或第五标识对应的证明信息，第五标识对应的认证信息用于验证第二节点，第五标识对应的证明信息用于验证第五标识对应的属性。

45 一种可能的实现方式中，第六信息包括第五标识和如下一项或多项：第五标识对应的凭证信息，第五标识对应的服务信息、用于指示第二节点的类型的信息、第五标识的签发者的信息、或用于指示第五标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第四标识和第四标识对应的凭证信息携带在第四标识对应的标识信息中。或者，第四标识携带在第二标识对应的标识信息中，第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息中的一项或多项携带在第四标识对应的文件信息中。

一种可能的实现方式中，第四标识对应的标识信息包括第四字段和如下一项或多项：第五字段或第六字段，其中，第四字段承载的信息用于指示第四标识，第五字段承载的信息用于指示第四标识的标识类型，第六字段承载的信息用于校验第四标识对应的标识信息中除第六字段之外的字段承载的信息。

可选地，收发模块 1102 可以包括接收模块和发送模块（图 11 中未示出）。其中，收发模块 1102 用于实现通信装置 1100 的发送功能和接收功能。

可选地，通信装置 1100 还可以包括存储模块（图 11 中未示出），该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时，使得通信装置 1100 可以执行图 2、图 4 或图 8 所示出的通信方法中存储节点的功能。

应理解，通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块 1102 可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1100 可以是终端或网络设备，也可以是可设置于终端或网络设备中的芯片（系统）、或其他部件或组件或者软件模块，还可以是包含终端或网络设备的装置，本申请对此不做限定。

此外，通信装置 1100 的技术效果可以参考图 2、图 4 或图 8 中任一项所示出的通信方法的技术效果，此处不再赘述。

一种可能的实现方式中，第一标识对应的服务信息用于生成第三节点的证明信息和/或第三节点的认证信息。和/或，第一标识对应的服务信息用于验证第三节点的证明信息和/或第三节点的认证信息。和/或，第一标识对应的服务信息用于为第三节点提供如下一项或多项服务：签约服务、网络接入服务、或数据共享服务；其中，第三节点与第一节点不同，第三节点的凭证信息用于验证第三节点，第三节点的证明信息用于验证第三节点的标识对应的属性。

一种可能的实现方式中，第一信息还用于指示第一标识对应的凭证信息，第一标识对应的凭证信息用于验证第一节点和/或用于验证第一标识对应的属性。

一种可能的实现方式中，第一标识对应的凭证信息包括第一标识对应的认证信息和/或第一标识对应的证明信息，第一标识对应的认证信息用于验证第一节点，第一标识对应的证明信息用于验证第一节点对应的属性。

一种可能的实现方式中，第一信息包括第一标识和第一标识对应的服务信息，和如下一项或多项：用于指示第一节点的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息公开条件的信息。

一种可能的实现方式中，第一标识和第一标识对应的凭证信息携带在第一标识对应的标识信息中。或者，第一标识携带在第一标识对应的标识信息中，第一标识对应的凭证信息、第一标识对应的服务信息、用于指示终端的类型的信息、第一标识的签发者的信息、或用于指示第一标识对应的凭证信息的公开条件的信息中的一项或多项携带在第一标识对应的文件信息中。

一种可能的实现方式中，第一标识对应的证明信息是由第四节点根据第四节点对应的服务信息生成的，第一标识对应的证明信息由第四节点对应的私钥签名。第四节点与第一节点不同。

一种可能的实现方式中，第四节点对应的服务信息用于生成服务结果信息，服务结果信息包括第五节点的凭证信息。第五节点与第四节点不同。第五节点的凭证信息用于验证第五节点和/或用于验证第五节点的标识对应的属性。

一种可能的实现方式中，第一标识对应的标识信息是经过卡商或终端厂商生成的第一节点的标识对应的私钥签名的信息。

一种可能的实现方式中，存储节点为如下一项或多项：区块链节点、分布式存储节点、或通信设备。通信设备与第一节点不同。

一些实施例中，通信装置 1100 可适用于图 1 中所示出的通信系统中，执行图 8 中所示出的通信方法中终端的功能。

处理模块 1101，用于获取第六信息。其中，第六信息用于指示第二节点的第四标识和第四标识对应的凭证信息，第四标识对应的凭证信息用于验证第二节点和/或第四标识对应的属性。第四标识和第四标识对应的凭证信息是由第一节点生成的。收发模块 1102，用于向存储节点发送第六信息和/或第六信息的哈希值。

一种可能的实现方式中，第四标识对应的凭证信息包括第四标识对应的认证信息和/或第四标识对应的证明信息，第四标识对应的认证信息用于验证第二节点，第四标识对应的证明信息用于验证第四标识对应的属性。

一种可能的实现方式中，第六信息包括第四标识和如下一项或多项：第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息。

一种可能的实现方式中，第四标识和第四标识对应的凭证信息携带在第四标识对应的标识信息中；或者，第四标识携带在第二标识对应的标识信息中，第四标识对应的凭证信息，第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息中的一项或多项携带在第四标识对应的文件信息中。

可选地，第四标识对应的标识信息包括第四字段和如下一项或多项：第五字段或第六字段，其中，第四字段承载的信息用于指示第四标识，第五字段承载的信息用于指示第四标识的标识类型，第六字段承载的信息用于校验第四标识对应的标识信息中除第六字段之外的字段承载的信息。

一种可能的实现方式中，存储节点为如下一项或多项：区块链节点、分布式存储节点、或电子设备。电子设备与第一节点不同。

可选地，收发模块 1102 可以包括接收模块和发送模块（图 11 中未示出）。其中，收发模块 1102 用于实现通信装置 1100 的发送功能和接收功能。

可选地，通信装置 1100 还可以包括存储模块（图 11 中未示出），该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时，使得通信装置 1100 可以执行图 8 所示出的通信方法中存储节点的功能。

应理解，通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块 1102 可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1100 可以是终端，也可以是可设置于终端中的芯片（系统）或其他部件、或组件或者软件模块，还可以是包含终端的装置，本申请对此不做限定。

此外，通信装置 1100 的技术效果可以参考图 8 中任一项所示出的通信方法的技术效果，此处不再赘述。

一些实施例中，通信装置 1100 可适用于图 1 中所示出的通信系统中，执行图 9 中所示出的通信方法中运营商对应的设备的功能。

其中，处理模块 1101，用于获取第七信息。其中，第七信息用于指示终端的第五标识和第五标识对应的凭证信息，第五标识对应的凭证信息用于验证终端和/或第五标识对应的属性，第五标识与运营商对应的设备中终端的用户永久标识不同，且第五标识与终端的用户永久标识对应，用户永久标识用于运营商对应的设备与终端之间的通信。收发模块 1102，用于向终端发送第七信息。

可选地，收发模块 1102 可以包括接收模块和发送模块（图 11 中未示出）。其中，收发模块 1102 用于实现通信装置 1100 的发送功能和接收功能。

可选地，通信装置 1100 还可以包括存储模块（图 11 中未示出），该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时，使得通信装置 1100 可以执行 9 所示出的通信方法中存储节点的功能。

应理解，通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块 1102 可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是,通信装置 1100 可以是网络设备,也可以是可设置于网络设备中的芯片(系统)其他部件或组件或者软件模块,还可以是包含网络设备的装置,本申请对此不做限定。

此外,通信装置 1100 的技术效果可以参考图 9 中任一项所示出的通信方法的技术效果,此处不再赘述。

5 一些实施例中,通信装置 1100 可适用于图 1 中所示出的通信系统中,执行图 9 中所示出的通信方法中终端的功能。

其中,收发模块 1102,用于接收来自运营商对应的设备的第七信息。其中,第七信息用于指示终端的第五标识和第五标识对应的凭证信息,第五标识对应的凭证信息用于验证终端和/或第五标识对应的属性,第五标识与终端的用户永久标识不同,且第五标识与终端的用户永久标识对应,用户永久标识用于运营商对应的设备与终端之间的通信。处理模块 1101,用于存储第七信息。

10 可选地,收发模块 1102 可以包括接收模块和发送模块(图 11 中未示出)。其中,收发模块 1102 用于实现通信装置 1100 的发送功能和接收功能。

15 可选地,通信装置 1100 还可以包括存储模块(图 11 中未示出),该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时,使得通信装置 1100 可以执行 9 所示出的通信方法中存储节点的功能。

应理解,通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现,可以为处理器或处理单元;收发模块 1102 可以由收发器或收发器相关电路组件实现,可以为收发器或收发单元。

20 需要说明的是,通信装置 1100 可以是终端,也可以是可设置于终端中的芯片(系统)、或其他部件或组件或者软件模块,还可以是包含终端的装置,本申请对此不做限定。

此外,通信装置 1100 的技术效果可以参考图 9 中任一项所示出的通信方法的技术效果,此处不再赘述。

25 一种可能的实现方式中,第五标识对应的凭证信息包括第五标识对应的认证信息和/或第五标识对应的证明信息,第五标识对应的认证信息用于验证终端,第五标识对应的证明信息用于验证终端对应的属性。

一种可能的实现方式中,第七信息包括第五标识,和如下一项或多项:第五标识对应的凭证信息、第五标识对应的证明信息、用于指示终端的类型的信息、第五标识的签发者的信息、用于指示第五标识对应的凭证信息的公开条件的信息。

30 一种可能的实现方式中,第五标识和第五标识对应的凭证信息携带在第五标识对应的标识信息中;或者,第五标识对应的凭证信息、第五标识对应的服务信息、用于指示终端的类型的信息、第五标识的签发者的信息、用于指示第五标识对应的凭证信息的公开条件的信息中的一项或多项携带在第五标识对应的文件信息中。

35 一种可能的实现方式中,第五标识对应的标识信息包括第七字段和如下一项或多项:第八字段或第九字段,其中,第七字段承载的信息用于指示第五标识,第八字段承载的信息用于指示第五标识的标识类型,第九字段承载的信息用于校验第五标识对应的标识信息中除第九字段之外的字段承载的信息。

一些实施例中,通信装置 1100 可适用于图 1 中所示出的通信系统中,执行图 2 中所示出的通信方法中卡商或终端厂商对应的设备的功能。

40 其中,处理模块 1101,用于获取第八信息和第九信息。其中,第八信息包括用于指示卡商或终端厂商对应的设备的第七标识,以及第七标识对应的凭证信息,第七标识对应的凭证信息用于验证卡商或终端厂商对应的设备和/或用于验证第七标识对应的属性。第九信息用于指示终端的第八标识和第八标识对应的凭证信息,第八标识对应的凭证信息用于验证终端和/或第八标识对应的属性。第八标识和第八标识对应的凭证信息是由卡商或终端厂商对应的设备生成的即第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的。收发模块 1102,用于向存储节点发送第八信息和第九信息。

45 一种可能的实现方式中,收发模块 1102,还用于向终端发送第九信息。

可选地,收发模块 1102 可以包括接收模块和发送模块(图 11 中未示出)。其中,收发模块

1102 用于实现通信装置 1100 的发送功能和接收功能。

可选地，通信装置 1100 还可以包括存储模块（图 11 中未示出），该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时，使得通信装置 1100 可以执行 10 所示出的通信方法中存储节点的功能。

5 应理解，通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块 1102 可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1100 可以是终端或网络设备，也可以是可设置于终端或网络设备中的芯片（系统）、或其他部件或组件或者软件模块，还可以是包含终端或网络设备的装置，本申请对此不做限定。

10 此外，通信装置 1100 的技术效果可以参考图 10 中任一项所示出的通信方法的技术效果，此处不再赘述。

一些实施例中，通信装置 1100 可适用于图 1 中所示出的通信系统中，执行图 10 中所示出的通信方法中存储节点的功能。

15 收发模块 1102，用于接收第八信息和第九信息。其中，第八信息包括用于指示卡商或终端厂商对应的设备的第七标识，以及第七标识对应的凭证信息，第七标识对应的凭证信息用于验证卡商或终端厂商对应的设备和/或用于验证第七标识对应的属性。第九信息用于指示终端的第八标识和第八标识对应的凭证信息，第八标识对应的凭证信息用于验证终端和/或第八标识对应的属性。第八标识和第八标识对应的凭证信息是由卡商或终端厂商对应的设备生成的，即第八标识对应的凭证信息是由卡商或终端厂商对应的设备的私钥签名的。处理模块 1101，用于存储第八信息和第九信息。

一种可能的实现方式中，收发模块 1102，还用于接收来自卡商或终端厂商对应的设备的第八信息和第九信息。

25 一种可能的实现方式中，收发模块 1102，还用于接收来自卡商或终端厂商对应的设备的第八信息，以及接收来自终端的第九信息。

可选地，收发模块 1102 可以包括接收模块和发送模块（图 11 中未示出）。其中，收发模块 1102 用于实现通信装置 1100 的发送功能和接收功能。

30 可选地，通信装置 1100 还可以包括存储模块（图 11 中未示出），该存储模块存储有程序或指令。当处理模块 1101 执行该程序或指令时，使得通信装置 1100 可以执行 10 所示出的通信方法中存储节点的功能。

应理解，通信装置 1100 中涉及的处理模块 1101 可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块 1102 可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

35 需要说明的是，通信装置 1100 可以是终端或网络设备，也可以是可设置于终端或网络设备中的芯片（系统）、或其他部件或组件或者软件模块，还可以是包含终端或网络设备的装置，本申请对此不做限定。

此外，通信装置 1100 的技术效果可以参考图 10 中任一项所示出的通信方法的技术效果，此处不再赘述。

40 其中，示例性地，图 12 为本申请实施例提供的通信装置的结构示意图。该通信装置可以是终端或网络设备，也可以是可设置于终端或网络设备的芯片（系统）、或其他部件或组件或者软件模块。如图 12 所示，通信装置 1200 可以包括处理器 1201。可选地，通信装置 1200 还可以包括存储器 1202 和/或收发器 1203。其中，处理器 1201 与存储器 1202 和收发器 1203 耦合，如可以通过通信总线连接。

下面结合图 12 对通信装置 1200 的各个构成部件进行具体的介绍：

45 其中，处理器 1201 是通信装置 1200 的控制中心，可以是一个处理器，也可以是多个处理元件的统称。例如，处理器 1201 是一个或多个中央处理器（central processing unit, CPU），也可以是特定集成电路（application specific integrated circuit, ASIC），或者是被配置成实施本申请实施

例的一个或多个集成电路，例如：一个或多个数字信号处理器（digital signal processor, DSP），或，一个或者多个现场可编程门阵列（field programmable gate array, FPGA）。

可选地，处理器 1201 可以通过运行或执行存储在存储器 1202 内的软件程序，以及调用存储在存储器 1202 内的数据，执行通信装置 1200 的各种功能。

5 在具体的实现中，作为一种实施例，处理器 1201 可以包括一个或多个 CPU，例如图 12 中所示出的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，通信装置 1200 也可以包括多个处理器，例如图 12 中所示的处理器 1201 和处理器 1204。这些处理器中的每一个可以是一个单核处理器（single-CPU），也可以是一个多核处理器（multi-CPU）。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

其中，所述存储器 1202 用于存储执行本申请方案的软件程序，并由处理器 1201 来控制执行，具体实现方式可以参考上述方法实施例，此处不再赘述。

10 可选地，存储器 1202 可以是只读存储器（read-only memory, ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory, RAM）或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only memory, EEPROM）、只读光盘（compact disc read-only memory, CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器 1202 可以和处理器 1201 集成在一起，也可以独立存在，并通过通信装置 1200 的接口电路（图 12 中未示出）与处理器 1201 耦合，本申请实施例对此不作具体限定。

收发器 1203，用于与其他通信装置之间的通信。例如，通信装置 1200 为终端，收发器 1203 可以用于与网络设备通信，或者与另一个终端通信。又例如，通信装置 1200 为网络设备，收发器 1203 可以用于与终端通信，或者与另一个网络设备通信。

25 可选地，收发器 1203 可以包括接收器和发送器（图 12 中未单独示出）。其中，接收器用于实现接收功能，发送器用于实现发送功能。

可选地，收发器 1203 可以和处理器 1201 集成在一起，也可以独立存在，并通过通信装置 1200 的接口电路（图 12 中未示出）与处理器 1201 耦合，本申请实施例对此不作具体限定。

需要说明的是，图 12 中示出的通信装置 1200 的结构并不构成对该通信装置的限定，实际的通信装置可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

此外，通信装置 1200 的技术效果可以参考上述方法实施例所述的通信方法的技术效果，此处不再赘述。

本申请实施例提供一种通信系统。该通信系统包括上述一个或多个终端，以及一个或多个网络设备。

35 应理解，在本申请实施例中的处理器可以是 CPU，该处理器还可以是其他通用处理器、DSP、ASIC、FPGA 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

还应理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是 ROM、可编程只读存储器（programmable ROM, PROM）、可擦除可编程只读存储器（erasable PROM, EPROM）、EEPROM 或闪存。易失性存储器可以是 RAM，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（static RAM, SRAM）、动态随机存取存储器（DRAM）、同步动态随机存取存储器（synchronous DRAM, SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM, DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM, ESDRAM）、同步连接动态随机存取存储器（synchlink DRAM, SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM, DR RAM）。

上述实施例，可以全部或部分地通过软件、硬件（如电路）、固件或其他任意组合来实现。

当使用软件实现时，上述实施例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或计算机程序。在计算机上加载或执行所述计算机指令或计算机程序时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以为通用计算机、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（例如红外、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。所述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合的服务器、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。半导体介质可以是固态硬盘。

应理解，本文中术语“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，其中 A、B 可以是单数或者复数。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系，但也可表示的是一种“和/或”的关系，具体可参考前后文进行理解。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a、b、或 c 中的至少一项(个)，可以表示：a、b、c、a-b、a-c、b-c，或 a-b-c，其中 a、b、c 可以是单个，也可以是多个。

应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

- 1.一种通信方法，其特征在于，应用于第一节点，所述方法包括：
获取第一信息；其中，所述第一信息用于指示第一标识和所述第一标识对应的服务信息；
5 向存储节点发送所述第一信息。
- 2.根据权利要求1所述的方法，其特征在于，所述第一节点可以包括一项或多项：
卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信
机构对应的设备、或空中写卡服务器。
- 3.根据权利要求2所述的方法，其特征在于，若所述第一节点为所述卡商或终端厂商对应的
10 设备，则所述方法还包括：
获取第二信息；所述第二信息用于指示终端的第二标识和所述第二标识对应的凭证信息，所
述第二标识对应的凭证信息用于验证所述终端和/或所述第二标识对应的属性；所述第二标识和所
述第二标识对应的凭证信息是由所述第一节点生成的；
向存储节点发送所述第二信息和/或所述第二信息的哈希值。
- 15 4.根据权利要求3所述的方法，其特征在于，所述第二标识对应的凭证信息包括所述第二标
识对应的认证信息和/或所述第二标识对应的证明信息，所述第二标识对应的认证信息用于验证所
述终端；所述第二标识对应的证明信息用于验证所述第二标识对应的属性。
- 5.根据权利要求3或4所述的方法，其特征在于，所述第二信息包括所述第二标识，和如下
一项或多项：
20 所述第二标识对应的凭证信息，所述第二标识对应的服务信息、用于指示所述终端的类型的
信息、所述第二标识的签发者的信息、或用于指示所述第二标识对应的凭证信息的公开条件的信
息。
- 6.根据权利要求5所述的方法，其特征在于，所述第二标识和所述第二标识对应的凭证信息
携带在所述第二标识对应的标识信息中；或者，所述第二标识携带在所述第二标识对应的标识信
25 息中，所述第二标识对应的凭证信息、所述第二标识对应的服务信息、所述用于指示终端的类
型的信息、所述第二标识的签发者的信息、或用于指示所述第二标识对应的凭证信息的公开条件
的信息中的一项或多项携带在第二标识对应的文件信息中。
- 7.根据权利要求6所述的方法，其特征在于，所述第二标识对应的标识信息包括第一字段和
如下一项或多项：第二字段或第三字段，其中，所述第一字段承载的信息用于指示所述第二标
30 识，所述第二字段承载的信息用于指示所述第二标识的标识类型，所述第三字段承载的信息用于校
验所述第二标识对应的标识信息中除所述第三字段之外的字段承载的信息。
- 8.根据权利要求3-7中任一项所述的方法，其特征在于，所述方法还包括：
向终端发送第三信息；所述第三信息用于指示所述第二信息，或者，所述第三信息用于指示
第二信息和所述第二信息在存储系统中的存储位置。
- 35 9.根据权利要求2所述的方法，其特征在于，若所述第一节点为终端，则所述方法还包括：
接收来自卡商或终端厂商对应的设备的第四信息；其中，所述第四信息用于指示所述第一标
识和所述第一标识对应的凭证信息；或者，所述第四信息用于指示所述第一标识、所述第一标识
对应的凭证信息、所述第一标识和所述第一标识对应的凭证信息在存储节点中的存储位置。
- 10.根据权利要求1、或2、或9所述的方法，其特征在于，所述方法还包括：
40 向存储节点发送第五信息和/或第五信息的哈希值；其中，所述第五信息用于指示所述第一节
点的第三标识和所述第三标识对应的凭证信息；所述第三标识与所述第一标识不同。
- 11.根据权利要求2所述的方法，其特征在于，若所述第一节点为所述终端，则所述方法还包
括：
45 向所述卡商或终端厂商对应的设备发送证明请求信息；其中，所述证明请求信息用于请求所
述第一节点对应的证明信息，所述第一节点对应的证明信息用于验证所述第一节点或所述第一节
点的标识对应的属性；
接收所述第一节点对应的证明信息，所述第一节点对应的证明信息是所述卡商或终端厂商对

应的设备生成的。

12.根据权利要求 2 所述的方法，其特征在于，若所述第一节点为所述卡商或终端厂商对应的设备，则所述方法还包括：

5 接收来自所述终端的证明请求信息；其中，所述证明请求信息用于请求所述终端对应的证明信息，所述终端对应的证明信息用于验证所述终端或所述终端的标识对应的属性；

向存储节点发送所述终端对应的证明信息；

向所述终端发送所述终端对应的证明信息。

13.一种通信方法，其特征在于，应用于存储节点，所述方法包括：

10 存储节点接收来自第一节点的第一信息；其中，所述第一信息包括第一标识和第一标识对应的服务信息；

所述存储节点存储所述第一信息。

14.根据权利要求 13 所述的方法，其特征在于，所述第一节点可以包括一项或多项：

卡商或终端厂商对应的设备、终端、运营商对应的设备、权威机构对应的设备、第三方可信机构对应的设备、或空中写卡服务器。

15.根据权利要求 14 所述的方法，其特征在于，若所述第一节点包括所述卡商或终端厂商对应的设备，则所述方法还包括：

所述存储节点接收来自所述第一节点的第二信息；所述第二信息用于指示终端的第二标识和所述第二标识对应的凭证信息，所述第二标识对应的凭证信息用于验证所述终端和/或所述第二标识对应的属性；所述第二标识和所述第二标识对应的凭证信息是由所述第一节点生成的；

20 所述存储节点存储所述第二信息。

16.根据权利要求 15 所述的方法，其特征在于，所述第二标识对应的凭证信息包括所述第二标识对应的认证信息和/或所述第二标识对应的证明信息，所述第二标识对应的认证信息用于验证所述终端；所述第二标识对应的证明信息用于验证所述第二标识对应的属性。

25 17.根据权利要求 15 或 16 所述的方法，其特征在于，所述第二信息包括所述第二标识，和如下项或多项：

所述第二标识对应的凭证信息，所述第二标识对应的服务信息、用于指示所述终端的类型的信息、所述第二标识的签发者的信息、或用于指示所述第二标识对应的凭证信息的公开条件的信息。

30 18.根据权利要求 17 所述的方法，其特征在于，所述第二标识和所述第二标识对应的凭证信息携带在所述第二标识对应的标识信息中；或者，所述第二标识携带在所述第二标识对应的标识信息中，所述第二标识对应的凭证信息、所述第二标识对应的服务信息、用于指示终端的类型的信息、所述第二标识的签发者的信息、或用于指示所述第二标识对应的凭证信息的公开条件的信息中的一项或多项携带在所述第二标识对应的文件信息中。

35 19.根据权利要求 18 所述的方法，其特征在于，所述第二标识对应的标识信息包括第一字段和如下项或多项：第二字段或第三字段，其中，所述第一字段承载的信息用于指示所述第二标识，所述第二字段承载的信息用于指示所述第二标识的标识类型，所述第三字段承载的信息用于校验所述第二标识对应的标识信息中除所述第三字段之外的字段承载的信息。

20.根据权利要求 13 或 14 所述的方法，其特征在于，所述方法还包括：

40 所述存储节点接收来自所述第一节点的第五信息；其中，所述第五信息用于指示所述第一节点的第三标识和所述第三标识对应的凭证信息。

21.根据权利要求 14 所述的方法，其特征在于，若所述第一节点包括卡商或终端厂商对应的设备，则所述方法还包括：

接收来自所述第一节点的终端对应的证明信息；其中，所述终端对应的证明信息用于验证终端或终端的标识对应的属性。

45 22.根据权利要求 13 所述的方法，其特征在于，所述方法还包括：

所述存储节点接收来自第二节点的第六信息；其中，所述第六信息用于指示所述第二节点的第四标识和所述第四标识对应的凭证信息，所述第四标识对应的凭证信息用于验证所述第二节点

和/或所述第四标识对应的属性；所述第四标识和所述第四标识对应的凭证信息是由第一节点生成的；

所述存储节点存储所述第六信息。

23.根据权利要求 22 所述的方法，其特征在于，所述第四标识对应的凭证信息包括第四标识对应的认证信息和/或第四标识对应的证明信息，所述第四标识对应的认证信息用于验证所述第二节点，所述第四标识对应的证明信息用于验证所述第四标识对应的属性。

24.根据权利要求 22 或 23 所述的方法，其特征在于，所述第六信息包括所述第四标识和如下一项或多项：

所述第四标识对应的凭证信息，所述第四标识对应的服务信息、用于指示所述第二节点的类型的信息、所述第四标识的签发者的信息、或用于指示所述第四标识对应的凭证信息的公开条件的信息。

25.根据权利要求 24 所述的方法，其特征在于，所述第四标识和所述第四标识对应的凭证信息携带在所述第四标识对应的标识信息中；或者，所述第四标识携带在第四标识对应的标识信息中，第四标识对应的凭证信息、第四标识对应的服务信息、用于指示第二节点的类型的信息、第四标识的签发者的信息、或用于指示第四标识对应的凭证信息的公开条件的信息中的一项或多项携带在第四标识对应的文件信息中。

26.根据权利要求 25 所述的方法，其特征在于，第四标识对应的标识信息包括第四字段和如下一项或多项：第五字段或第六字段，其中，所述第四字段承载的信息用于指示所述第四标识，所述第五字段承载的信息用于指示所述第四标识的标识类型，所述第六字段承载的信息用于校验所述第四标识对应的标识信息中除所述第六字段之外的字段承载的信息。

27.根据权利要求 1-26 中任一项所述的方法，其特征在于，

所述第一标识对应的服务信息用于生成第三节点的证明信息和/或所述第三节点的认证信息；和/或，

所述第一标识对应的服务信息用于验证所述第三节点的证明信息和/或所述第三节点的认证信息；和/或，

所述第一标识对应的服务信息用于为所述第三节点提供如下一项或多项服务：签约服务、网络接入服务、或数据共享服务；

其中，所述第三节点与所述第一节点不同，所述第三节点的凭证信息用于验证所述第三节点，所述第三节点的证明信息用于验证所述第三节点的标识对应的属性。

28.根据权利要求 1-27 中任一项所述的方法，其特征在于，所述第一信息还用于指示所述第一标识对应的凭证信息，所述第一标识对应的凭证信息用于验证所述第一节点和/或用于验证所述第一标识对应的属性。

29.根据权利要求 28 所述的方法，其特征在于，所述第一标识对应的凭证信息包括所述第一标识对应的认证信息和/或所述第一标识对应的证明信息，所述第一标识对应的认证信息用于验证所述第一节点，所述第一标识对应的证明信息用于验证所述第一节点对应的属性。

30.根据权利要求 29 所述的方法，其特征在于，所述第一标识和所述第一标识对应的凭证信息携带在所述第一标识对应的标识信息中；或者，所述第一标识携带在第一标识对应的标识信息中，所述第一标识对应的凭证信息、所述第一标识对应的服务信息、用于指示终端的类型的信息、所述第一标识的签发者的信息、或用于指示所述第一标识对应的凭证信息的公开条件的信息中的一项或多项携带在所述第一标识对应的文件信息中。

31.根据权利要求 29 或 30 所述的方法，其特征在于，所述第一标识对应的证明信息是由第四节点根据所述第四节点对应的服务信息生成的，所述第一标识对应的证明信息由所述第四节点对应的私钥签名；所述第四节点与所述第一节点不同。

32.根据权利要求 31 所述的方法，其特征在于，所述第四节点对应的服务信息用于生成服务结果信息，所述服务结果信息包括第五节点的凭证信息；所述第五节点与所述第四节点不同；所述第五节点的凭证信息用于验证所述第五节点和/或用于验证所述第五节点的标识对应的属性。

33.根据权利要求 30 所述的方法，其特征在于，所述第一标识对应的标识信息是经过卡商或

终端厂商生成的所述第一节点的标识对应的私钥签名的信息。

34.根据权利要求 1-33 中任一项所述的方法,其特征在于,所述第一信息还包括如下一项或多项:用于指示所述第一节点的类型的信息、所述第一标识的签发者的信息、或用于指示所述第一标识对应的凭证信息的公开条件的信息。

5 35.根据权利要求 1-34 中任一项所述的方法,其特征在于,所述存储节点为如下一项或多项:区块链节点、分布式存储节点、或通信设备;所述通信设备与所述第一节点不同。

36.一种通信方法,其特征在于,应用于第二节点,所述方法包括:

10 获取第六信息;其中,所述第六信息用于指示所述第二节点的第四标识和所述第四标识对应的凭证信息,所述第四标识对应的凭证信息用于验证所述第二节点和/或所述第四标识对应的属性;所述第四标识和所述第四标识对应的凭证信息是由第一节点生成的;

向存储节点发送所述第六信息和/或所述第六信息的哈希值。

37.根据权利要求 36 所述的方法,其特征在于,所述第四标识对应的凭证信息包括所述第四标识对应的认证信息和/或所述第四标识对应的证明信息,所述第四标识对应的认证信息用于验证所述第二节点,所述第四标识对应的证明信息用于验证所述第四标识对应的属性。

15 38.根据权利要求 36 或 37 所述的方法,其特征在于,所述第六信息包括第四标识和如下一项或多项:所述第四标识对应的凭证信息,所述第四标识对应的服务信息、用于指示所述第二节点的类型的信息、所述第四标识的签发者的信息、或用于指示所述第四标识对应的凭证信息的公开条件的信息。

20 39.根据权利要求 36-38 中任一项所述的方法,其特征在于,所述第四标识和所述第四标识对应的凭证信息携带在所述第四标识对应的标识信息中;或者,所述第四标识携带在第四标识对应的标识信息中,所述第四标识对应的凭证信息、所述第四标识对应的服务信息、用于指示所述第二节点的类型的信息、所述第四标识的签发者的信息、或用于指示所述第四标识对应的凭证信息的公开条件的信息中的一项或多项携带在所述第四标识对应的文件信息中。

25 40.根据权利要求 39 所述的方法,其特征在于,所述第四标识对应的标识信息包括所述第四字段和如下一项或多项:第五字段或第六字段,其中,所述第四字段承载的信息用于指示所述第四标识,所述第五字段承载的信息用于指示所述第四标识的标识类型,所述第六字段承载的信息用于校验所述第四标识对应的标识信息中除所述第六字段之外的字段承载的信息。

41.根据权利要求 36-40 中任一项所述的方法,其特征在于,存储节点为如下一项或多项:区块链节点、分布式存储节点、或通信设备,所述通信设备与所述第一节点不同。

30 42.一种通信方法,其特征在于,应用于运营商对应的设备,所述方法包括:

获取第七信息;其中,所述第七信息用于指示终端的第五标识和第五标识对应的凭证信息,所述第五标识对应的凭证信息用于验证终端和/或所述第五标识对应的属性,所述第五标识与所述运营商对应的设备中终端的用户永久标识不同,且所述第五标识与所述终端的用户永久标识对应,所述用户永久标识用于所述运营商对应的设备与所述终端之间的通信;

35 向所述终端发送所述第七信息。

43.一种通信方法,其特征在于,应用于终端,所述方法包括:

40 接收来自运营商对应的设备的第七信息;其中,所述第七信息用于指示所述终端的第五标识和第五标识对应的凭证信息,所述第五标识对应的凭证信息用于验证所述终端和/或所述第五标识对应的属性,所述第五标识与所述终端的用户永久标识不同,且所述第五标识与所述终端的用户永久标识对应,所述用户永久标识用于所述运营商对应的设备与所述终端之间的通信;

存储所述第七信息。

44.根据权利要求 42 或 43 所述的方法,其特征在于,所述第五标识对应的凭证信息包括所述第五标识对应的认证信息和/或所述第五标识对应的证明信息,所述第五标识对应的认证信息用于验证所述终端,所述第五标识对应的证明信息用于验证所述终端对应的属性。

45 45.根据权利要求 42-44 中任一项所述的方法,其特征在于,所述第七信息包括所述第五标识,和如下一项或多项:

所述第五标识对应的凭证信息、第五标识对应的证明信息、用于指示所述终端的类型的信息、

所述第五标识的签发者的信息、用于指示所述第五标识对应的凭证信息的公开条件的信息。

46.根据权利要求 45 所述的方法，其特征在于，所述第五标识和所述第五标识对应的凭证信息携带在所述第五标识对应的标识信息中；或者，所述第五标识携带在第五标识对应的标识信息中，所述第五标识对应的凭证信息、所述第五标识对应的服务信息、用于指示终端的类型的信息、
5 所述第五标识的签发者的信息、用于指示所述第五标识对应的凭证信息的公开条件的信息中的一项或多项携带在所述第五标识对应的文件信息中。

47.根据权利要求 46 所述的方法，其特征在于，所述第五标识对应的标识信息包括第七字段和如下一项或多项：第八字段或第九字段，其中，所述第七字段承载的信息用于指示所述第五标识，所述第八字段承载的信息用于指示所述第五标识的标识类型，所述第九字段承载的信息用于
10 校验第所述五标识对应的标识信息中除所述第九字段之外的字段承载的信息。

48.一种通信方法，其特征在于，应用于卡商或终端厂商对应的设备，所述方法包括：
获取第八信息和第九信息；其中，所述第八信息包括用于指示所述卡商或终端厂商对应的设备的第七标识，以及所述第七标识对应的凭证信息，所述第七标识对应的凭证信息用于验证卡商或终端厂商对应的设备和/或用于验证所述第七标识对应的属性；所述第九信息用于指示终端的第八标识和所述第八标识对应的凭证信息，所述第八标识对应的凭证信息用于验证终端和/或所述第八标识对应的属性；所述第八标识和所述第八标识对应的凭证信息是由所述卡商或终端厂商对应的设备生成的；
15 向存储节点发送所述第八信息和所述第九信息。

49.根据权利要求 48 所述的方法，其特征在于，所述方法还包括：
20 向终端发送所述第九信息。

50.一种通信方法，其特征在于，应用于存储节点，所述方法包括：
接收第八信息和第九信息；其中，所述第八信息包括用于指示卡商或终端厂商对应的设备的第七标识，以及所述第七标识对应的凭证信息，所述第七标识对应的凭证信息用于验证所述卡商或终端厂商对应的设备和/或用于验证所述第七标识对应的属性；所述第九信息用于指示终端的第八标识和第八标识对应的凭证信息，所述第八标识对应的凭证信息用于验证终端和/或所述第八标识对应的属性；所述第八标识和所述第八标识对应的凭证信息是由所述卡商或终端厂商对应的设备生成的；
25 存储所述第八信息和所述第九信息。

51.根据权利要求 50 所述的方法，其特征在于，所述接收第八信息和第九信息，包括：
30 接收来自所述卡商或终端厂商对应的设备的所述第八信息和所述第九信息。

52.根据权利要求 50 所述的方法，其特征在于，接收第八信息和第九信息，包括：
接收来自所述卡商或终端厂商对应的设备的第八信息，以及接收来自终端的所述第九信息。

53.一种通信装置，其特征在于，所述通信装置用于执行如权利要求 1-52 中任一项所述的通信方法。

54.一种通信装置，其特征在于，包括处理器，所述处理器用于执行如权利要求 1-52 中任一项所述的通信方法。

55.一种通信装置，其特征在于，包括：处理器，所述处理器与存储器耦合；
所述处理器，用于执行所述存储器中存储的计算机程序，以使得所述通信装置执行如权利要求 1-52 中任一项所述的通信方法。

56.一种通信装置，其特征在于，包括：处理器和接口电路；其中，
40 所述接口电路，用于接收代码指令并传输至所述处理器；
所述处理器用于运行所述代码指令以执行如权利要求 1-52 中任一项所述的方法。

57.一种通信装置，其特征在于，所述通信装置包括处理器和收发器，所述收发器用于所述通信装置和其他通信装置之间进行信息交互，所述处理器执行程序指令，用以执行如权利要求 1-52 中任一项所述的通信方法。

58.一种通信系统，其特征在于，所述通信系统包括一个或多个终端设备以及一个或多个网络设备。

59.一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包括计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机执行如权利要求 1-52 中任一项所述的通信方法。

5 60.一种计算机程序产品，其特征在于，所述计算机程序产品包括：计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机执行如权利要求 1-52 中任一项所述的通信方法。