

一种基于区块链存证的证据采集方法及系统

技术领域

[01] 本说明书实施例涉及信息技术领域，尤其涉及一种基于区块链存证的证据采集方法及系统。

5 背景技术

[02] 在司法实践中，对于有些以当事人的真实意思表示为必备要素的证据（如证人证言、遗嘱等），为了使得这些证据获得确定的法律效力，有时会由权威机构（如法院、公证处等）现场采集这些证据。

[03] 例如，对于证人证言，为了防止采集的证言在提交给法庭之前被篡改，通常需要证
10 人亲自出庭陈述证言。

[04] 又如，对于遗嘱，为了防止遗嘱人作出的遗嘱在提交给法庭之前被篡改，从而无法反映遗嘱人的真实意思，可以由公证人员现场对遗嘱人作出的遗嘱进行公证。

[05] 基于此，需要一种对当事人而言更为便利的证据采集方法。

发明内容

15 [06] 为了解决现有的证据采集方式对当事人而言不够便利的问题，本说明书实施例提供一种基于区块链存证的证据采集方法及系统，技术方案如下：

[07] 根据本说明书实施例的第 1 方面，提供一种基于区块链存证的证据采集方法，包括：

[08] 用户设备接收用户通过目标账号输入的证据采集指令；所述目标账号是在业务设备上预先注册的；

20 [09] 所述用户设备响应于所述证据采集指令，将所述用户的行为和/或语音录制成多媒体文件；

[10] 所述用户设备将所述多媒体文件发送给所述业务设备；所述业务设备为区块链网络中的任一节点；

[11] 所述业务设备基于所述多媒体文件，构建目标交易，并将所述目标交易广播至区块
25 链网络；

[12]所述区块链网络中的各节点基于共识机制，将所述目标交易发布至区块链。

[13]根据本说明书实施例的第2方面，一种基于区块链存证的证据采集系统，包括区块链网络 and 用户设备，所述区块链网络中的任一节点为业务设备；

5 [14]所述用户设备，接收用户通过目标账号输入的证据采集指令，所述目标账号是在业务设备上预先注册的；响应于所述证据采集指令，将所述用户的行为和/或语音录制成多媒体文件；将所述多媒体文件发送给所述业务设备；

[15]所述业务设备，基于所述多媒体文件，构建目标交易，并将所述目标交易广播至所述区块链网络；

[16]所述区块链网络中的各节点，基于共识机制，将所述目标交易发布至区块链。

10 [17]本说明书实施例所提供的技术方案，用户（当事人）可以操作用户设备，将自己的行为和/或语音录制成多媒体文件，随后，用户设备会将所述多媒体文件发送给业务设备，进而由业务设备基于所述多媒体文件构建目标交易，将目标交易广播至区块链网络，由区块链网络中的各节点基于共识机制，将目标交易发布至区块链。如此，就实现了所述多媒体文件的多方存证。通过本说明书实施例，当事人不必依赖权威机构（如法庭、公
15 证处），就可以随时随地通过对自己的行为和/或语音进行录制的方式采集证据（即多媒体文件），并且，采集的证据会被区块链网络存证，使得采集的证据难以被篡改，能够得到权威机构的认可，具有法律效力。

[18]应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本说明书实施例。

20 [19]此外，本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[20]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些
25 附图获得其他的附图。

[21]图1是本说明书实施例提供的一种基于区块链存证的证据采集方法的流程示意图；

[22]图2是本说明书实施例提供的一种基于区块链存证的证据采集系统的结构示意图；

[23]图 3 是本说明书实施例提供的一种基于区块链存证的证据采集装置的结构示意图；

[24]图 4 是本说明书实施例提供的另一种基于区块链存证的证据采集装置的结构示意图；

[25]图 5 是用于配置本说明书实施例方法的一种计算机设备的结构示意图。

具体实施方式

5 [26]为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[27]以下结合附图，详细说明本说明书各实施例提供的技术方案。

10 [28]图 1 是本说明书实施例提供的一种基于区块链存证的证据采集方法的流程示意图，包括以下步骤：

[29]S100：用户设备接收用户输入的证据采集指令。

[30]S102：所述用户设备响应于所述证据采集指令，将所述用户的行为和/或语音录制成多媒体文件。

15 [31]如背景技术所述，在司法实践中，对于有些以当事人的真实意思表示为必备要素的证据（如证人证言、遗嘱等），为了使得这些证据获得确定的法律效力，有时会由权威机构（如法院、公证处等）现场采集这些证据。

[32]在本说明书实施例中，用户是指上述的当事人。用户可以通过本说明书实施例提供的方法，进行真实意思表示，形成证据（即多媒体文件），并且，形成的证据会被区块

20 链存证，具有不可篡改性。

[33]所述用户设备是所述用户的设备，具体可以是手机、电脑或其他设备。需要说明的是，所述用户设备一般具有数据处理功能、通信功能以及多媒体信息采集功能的设备。其中，用户设备多媒体信息采集功能体现为用户设备具有摄像头、录音器等元件。

[34]在本说明书实施例中，用户当需要进行真实意思表示时，可以向用户设备输入证据

25 采集指令，以触发用户设备进行证据采集。

[35]进一步地，用户设备可以接收用户通过目标账号输入的证据采集指令。其中，所述目标账号是在业务设备上预先注册的。

[36]此处需要说明的是，所述目标账号不一定是所述用户预先在业务设备上注册的，也就是说，所述用户不一定是所述目标账号的拥有者。基于此，在步骤 S102 中，所述用户设备可以根据所述目标账号对应的身份验证信息，对所述用户进行身份验证并验证通过后，将所述用户的行为和/或语音录制成多媒体文件。

- 5 [37]其中，所述身份验证信息可以是所述目标账号的拥有者预先设置的密码、预先提供的人脸特征、声纹特征等。

[38]在本说明书实施例中，所述多媒体文件具体可以是音频文件、视频文件、文本文件、图像文件（如图片、动态图片 GIF 等）中的任一种。

- [39]例如，所述用户设备可以直接将所述用户的语音信息录制成音频文件。又如，所述
10 用户设备可以先采集所述用户的语音信息，再将所述语音信息转换成文本文件。

[40]此外，在步骤 S102 中，所述用户设备还可以在录制之前，先对录制现场进行检测，得到录制现场参数。其中，所述录制现场参数包括现场位置信息、现场环境信息、所述用户的语音特征、所述用户的表情特征中的至少一种。

- [41]需要说明的是，所述现场位置信息可以是所述用户进行意思表示的现场的位置坐标，
15 所述现场环境信息可以是现场的亮度、现场的空间大小等信息，所述用户的语音特征可以是用户的语调、语速、声音分贝等特征，所述用户的表情特征可以是对用户的表情进行拍摄得到的图像。

- [42]随后，所述用户设备可以将所述录制现场参数发送给所述业务设备，由所述业务设备对所述录制现场参数进行分析，进而根据分析结果，得到用于表征所述用户处于被胁迫状态的可能性的胁迫性表征值。其中，所述胁迫性表征值与所述用户处于被胁迫状态的可能性正相关。
20

[43]对本领域技术人员而言，很容易想到多种方式，根据所述录制现场参数，分析出所述用户被胁迫的可能性。以下试举几例。

- [44]例如，所述业务设备可以将所述目标账号日常登录的设备的位置信息与录制现场的位置信息进行比较，如果不一致，则说明所述目标账号当前登录的位置异常，所述用户
25 可能被胁迫至陌生地点，或者，所述目标账号不是被拥有者本人登录的。

[45]例如，所述业务设备可以根据录制现场的亮度、空间大小，分析出录制现场是居室、地下室或仓库，如果不是居室，则说明所述用户可能被胁迫。

[46]例如，所述业务设备可以根据所述用户的语调、语速、声音的分贝等特征，分析出所述用户的声音是否稳定。如果用户被胁迫，其声音通常是不稳定的。

[47]例如，所述业务设备可以根据所述用户的图像，分析所述用户的表情，判断所述用户情绪是否紧张。如果所述用户情绪紧张，则可能被胁迫，不能做出真实意思表示。

- 5 [48]总之，所述业务设备在得到所述胁迫性表征值之后，可以判断所述胁迫性表征值是否小于指定阈值（即判断所述胁迫性表征值是否较低），如果是，就说明所述用户被胁迫的可能性不大，可以在这种情况下对作出真实意思表示。于是，所述业务设备此时可以通知所述用户设备将所述用户的行为和/或语音录制成多媒体文件。

[49]S104：所述用户设备将所述多媒体文件发送给所述业务设备。

- 10 [50]S106：所述业务设备基于所述多媒体文件，构建目标交易，并将所述目标交易广播至区块链网络。

[51]所述用户设备在得到所述多媒体文件之后，也就采集到了以所述用户的真实意思表示为必备要素的证据，可以将所述多媒体文件发送给业务设备。

- [52]由于所述业务设备同时也是区块链网络中的一个节点，因此，所述业务设备可以基于所述多媒体文件，构建目标交易，将目标交易广播至区块链网络，使得所述区块链网络中的各节点基于共识机制，将所述目标交易发布至区块链。至此，所述多媒体文件就被区块链存证了，也就难以被篡改。
- 15

[53]需要说明的是，在本说明书中所描述的交易（transfer），是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。

- 20 [54]其中，区块链中的交易，存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，租房业务、车辆调度业务、保
- 25 险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[55]在本说明书实施例中，所述业务设备基于所述多媒体文件构建目标交易的方式可以是，构建包含所述多媒体文件的目标交易。这种情况下，所述多媒体文件本身会被存入区块链，这对区块链网络中的节点的存储能力较高要求。

- [56]此外，所述业务设备基于所述多媒体文件构建目标交易的方式也可以是，一方面，所述业务设备存储所述多媒体文件，具体可以是将所述多媒体文件存入本地或存入云端；另一方面，所述业务设备可以根据所述多媒体文件，采用哈希算法，确定所述多媒体文件对应的目标哈希，再构建包含所述目标哈希的目标交易。目标哈希实际上是一段字符串，所占的存储空间很小，将所述目标哈希存入区块链，对区块链网络中的节点的存储能力要求不高。并且，由于所述多媒体文件是否被修改可以通过所述目标哈希检测出来，因此，将所述目标哈希存入区块链，也相当于实现了所述多媒体文件的多方存证。
- [57]进一步地，所述业务设备可以直接采用哈希算法，计算所述多媒体文件的哈希值，作为所述目标哈希。所述业务设备也可以以所述多媒体文件和所述多媒体文件的存储位置信息为哈希算法的输入，采用哈希算法计算得到所述多媒体文件对应的目标哈希。
- [58]通过图 1 所示的方法，用户（当事人）可以操作用户设备，将自己的行为和/或语音录制成多媒体文件，随后，用户设备会将所述多媒体文件发送给业务设备，进而由业务设备基于所述多媒体文件构建目标交易，将目标交易广播至区块链网络，由区块链网络中的各节点基于共识机制，将目标交易发布至区块链。如此，就实现了所述多媒体文件的多方存证。通过本说明书实施例，当事人不必依赖权威机构（如法庭、公证处），就可以随时随地通过对自己的行为和/或语音进行录制的方式采集证据（即多媒体文件），并且，采集的证据会被区块链网络存证，使得采集的证据难以被篡改，能够得到权威机构的认可，具有法律效力。
- [59]此外，实践中，所述用户可能不是所述目标账号的拥有者，因此，所述用户通过所述目标账户作出的意思表示，并不能代表所述目标账号的拥有者的意志。
- [60]为此，在本说明书实施例中，可以对所述多媒体文件记录的行为和/或语音的产生者进行识别，以判断这个人是否为所述目标账号的拥有者本人。
- [61]具体地，所述业务设备可以预先获取所述目标账号的拥有者的面部特征（可以是人脸特征、虹膜特征等）和声纹特征，作为所述目标账号对应的可信面部特征和可信声纹特征。在所述业务设备将所述目标交易广播至区块链网络之前，当所述多媒体文件为音频文件时，所述业务设备从所述多媒体文件中提取所述用户的声纹特征，将提取的声纹特征与所述可信声纹特征进行比对，若一致，则将一致结果写入所述目标交易，若不一致，则将不一致结果写入所述目标交易；当所述多媒体文件为视频文件或图像文件时，所述业务设备从所述多媒体文件中提取所述用户的面部特征，将提取的面部特征与所述可信面部特征进行比对，若一致，则将一致结果写入所述目标交易，若不一致，则将不

一致结果写入所述目标交易；当所述多媒体文件为音视频文件时，所述业务设备从所述多媒体文件中提取所述用户的声纹特征与面部特征，将提取的声纹特征与所述可信声纹特征进行比对，将提取的面部特征与所述可信面部特征进行比对，若提取的声纹特征与所述可信声纹特征一致，且提取的面部特征与所述可信面部特征一致，则将一致结果写入所述目标交易，若提取的声纹特征与所述可信声纹特征不一致，或提取的面部特征与所述可信面部特征不一致，则将不一致结果写入所述目标交易。

[62]也就是说，从所述多媒体文件中提取的面部特征和/或声纹特征如果与所述目标账号的拥有者的面部特征和/或声纹特征不一致，就说明所述多媒体文件并不代表所述目标账号的拥有者本人的意志。哪怕所述多媒体文件被区块链存证，也不能说明所述多媒体文件是以所述目标账号的拥有者的意思表示为必备要素的证据。基于此，将所述多媒体文件是否代表所述目标账号的拥有者的意志的信息（一致结果或不一致结果）也写入所述目标交易，进而存入区块链进行公示。

[63]进一步地，所述业务设备若将不一致结果写入所述目标交易，则可以根据提取的所述用户的声纹特征和/或面部特征，查询得到所述用户的身份信息，然后再将所述用户的身份信息写入所述目标交易。这意味着，若所述多媒体文件不是所述目标账号的拥有者本人产生的，则意味着所述多媒体文件这一证据是伪造的，而证据的伪造者的身份信息也会被存入区块链进行公示。

[64]更进一步地，证据的伪造者的信用评价也会受到不良影响。例如，假设存在一个基于区块链技术对每个用户进行信用评价的系统，每个用户对应的信用分都会被公示于区块链。那么，可以对证据的伪造者的信用分进行扣减，扣减记录可以存入区块链进行公示。

[65]此外，在本说明实施例中，在所述业务设备将所述目标交易广播至区块链网络之前，所述业务设备可以将当前时间的时间戳写入所述目标交易。如此，多媒体文件被区块链存证的时间也难以被篡改，在有些场景下，比如遗嘱场景，遗嘱人可能在临终前作出过多份遗嘱，相应的产生了多个多媒体文件，都通过图 1 所示的方法，由区块链进行了存证。那么，按照继承法规定，遗嘱人作出的最后一个遗嘱才是有效的，因此，可以查询区块链，确定遗嘱人产生的每个多媒体文件对应的时间戳，将时间最新的多媒体文件确定为遗嘱人最新作出的遗嘱，即有效遗嘱。

[66]图 2 是本说明书实施例提供的一种基于区块链存证的证据采集系统，包括区块链网络和用户设备，所述区块链网络中的任一节点为业务设备；

[67]所述用户设备，接收用户输入的证据采集指令；响应于所述证据采集指令，将所述用户的行为和/或语音录制成多媒体文件；将所述多媒体文件发送给所述业务设备；

[68]所述业务设备，基于所述多媒体文件，构建目标交易，并将所述目标交易广播至所述区块链网络；

5 [69]所述区块链网络中的各节点，基于共识机制，将所述目标交易发布至区块链。

[70]如图 2 所示，实心点是所述业务设备，其是区块链网络中的一个节点。空心点是所述区块链网络中除所述业务设备之外的其他节点。

[71]基于图 1 所示的基于区块链存证的证据采集方法，本说明书实施例还对应提供了一种基于区块链存证的采集装置，如图 3 所示，业务设备为区块链网络中的任一节点，所
10 述装置包括：

[72]接收模块 301，接收用户输入的证据采集指令；

[73]录制模块 302，响应于所述证据采集指令，将所述用户的行为和/或语音录制成多媒体文件；

[74]发送模块 303，将所述多媒体文件发送给所述业务设备，以使所述业务设备基于所述多媒体文件，构建目标交易，并将所述目标交易广播至区块链网络，进而使所述区块链网络中的各节点基于共识机制，将所述目标交易发布至区块链。
15

[75]基于图 1 所示的基于区块链存证的证据采集方法，本说明书实施例还对应提供了一种基于区块链存证的采集装置，如图 4 所示，所述装置为区块链网络中的任一节点，所述装置包括：

20 [76]接收模块 401，接收用户设备发送的多媒体文件；所述多媒体文件，是所述用户设备接收用户输入的证据采集指令后，响应于所述证据采集指令，对所述用户的行为和/或语音进行录制得到的；

[77]处理模块 402，基于所述多媒体文件，构建目标交易，并将所述目标交易广播至区块链网络，以使所述区块链网络中的各节点基于共识机制，将所述目标交易发布至区块链。
25

[78]本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现上述用户设备或上述业务设备的功能。

[79]图 5 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和总线 1050。其中处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

5 [80]处理器 1010 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[81]存储器 1020 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备、动态存储设备等形式实现。存储器 1020
10 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1020 中，并由处理器 1010 来调用执行。

[82]输入/输出接口 1030 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包
15 括显示器、扬声器、振动器、指示灯等。

[83]通信接口 1040 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[84]总线 1050 包括一通路，在设备的各个组件（例如处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040）之间传输信息。
20

[85]需要说明的是，尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

25 [86]本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述用户设备或上述业务设备的功能。

[87]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器

(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带、磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电

5 可读媒体(transitory media),如调制的数据信号和载波。

[88]通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,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)执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

10

[89]上述实施例阐明的系统、方法、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机,计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

15

[90]本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于装置和设备实施例而言,由于其基本相似于方法实施例,所以描述得比较简单,相关之处参见方法实施例的部分说明即可。以上所描述的方法实施例仅仅是示意性的,其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的,在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

20

25

[91]以上所述仅是本说明书实施例的具体实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本说明书实施例原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本说明书实施例的保护范围。