



(12) 发明专利

(10) 授权公告号 CN 111079101 B

(45) 授权公告日 2020.10.23

(21) 申请号 201911326024.5

(22) 申请日 2019.12.20

(65) 同一申请的已公布的文献号
申请公布号 CN 111079101 A

(43) 申请公布日 2020.04.28

(73) 专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路
556号8层B段801-11

(72) 发明人 孙健康 林锋

(74) 专利代理机构 北京博思佳知识产权代理有
限公司 11415

代理人 周嗣勇

(51) Int. Cl.

G06F 21/16 (2013.01)

G06F 21/64 (2013.01)

(56) 对比文件

CN 108629038 A, 2018.10.09

CN 108959416 A, 2018.12.07

CN 110009336 A, 2019.07.12

CN 109102437 A, 2018.12.28

CN 110046994 A, 2019.07.23

US 2016212146 A1, 2016.07.21

审查员 岳孟果

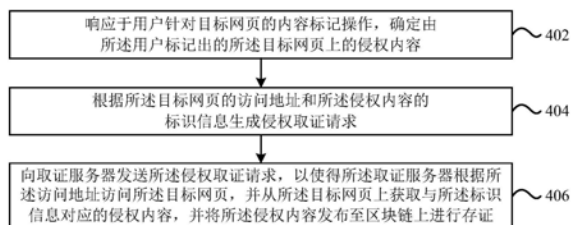
权利要求书2页 说明书12页 附图7页

(54) 发明名称

基于区块链的侵权取证方法及装置、电子设备、存储介质

(57) 摘要

本说明书一个或多个实施例提供一种基于区块链的侵权取证方法及装置、电子设备、存储介质;该方法应用于客户端,可以包括:响应于用户针对目标网页的内容标记操作,确定由所述用户标记出的所述目标网页上的侵权内容;根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请求;向取证服务器发送所述侵权取证请求,以使得所述取证服务器根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容,并将所述侵权内容发布至区块链上进行存证。



1. 一种基于区块链的侵权取证方法,应用于客户端,所述客户端为浏览器搭载的插件程序;所述方法包括:

接收用户针对所述插件程序的调用指令,并执行所述插件程序以检测用户针对目标网页的内容标记操作;

响应于用户针对目标网页的内容标记操作,确定由所述用户标记出的所述目标网页上的侵权内容;

根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请求;

向取证服务器发送所述侵权取证请求,以使得所述取证服务器根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容,并将所述侵权内容发布至区块链上进行存证。

2. 一种基于区块链的侵权取证方法,应用于取证服务器;所述方法包括:

接收客户端发送的侵权取证请求,所述侵权取证请求由所述客户端根据目标网页的访问地址和所述目标网页上的侵权内容的标识信息生成,所述侵权内容由所述客户端根据用户针对目标网页的内容标记操作得到,所述客户端为浏览器搭载的插件程序,所述内容标记操作通过响应于所述用户针对所述插件程序的调用指令,执行所述插件程序以检测得到;

响应于所述侵权取证请求,根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容;

将所述侵权内容发布至区块链上进行存证。

3. 根据权利要求2所述的方法,所述侵权取证请求中还包含针对所述目标网页的登录信息;所述从所述目标网页上获取与所述标识信息对应的侵权内容,包括:

根据所述侵权取证请求中包含的登录信息登录所述目标网页;

从登录成功后的所述目标网页上获取与所述标识信息对应的侵权内容。

4. 根据权利要求2所述的方法,

所述侵权取证请求中还包含所述侵权内容;所述方法还包括:在获取到与所述标识信息对应的侵权内容后,确定获取到的侵权内容与所述侵权取证请求中包含的侵权内容是否一致;当获取到的侵权内容与所述侵权取证请求中包含的侵权内容一致时,执行存证侵权内容的操作;或者,

所述侵权取证请求中还包含所述侵权内容的校验值;所述方法还包括:在获取到与所述标识信息对应的侵权内容后,确定获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值是否一致;当获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值一致时,执行存证侵权内容的操作。

5. 一种基于区块链的侵权取证装置,应用于客户端,所述客户端为浏览器搭载的插件程序;所述装置包括:

接收单元,接收用户针对所述插件程序的调用指令;

执行单元,执行所述插件程序以检测用户针对目标网页的内容标记操作;

确定单元,响应于用户针对目标网页的内容标记操作,确定由所述用户标记出的所述目标网页上的侵权内容;

生成单元,根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请

求；

发送单元，向取证服务器发送所述侵权取证请求，以使得所述取证服务器根据所述访问地址访问所述目标网页，并从所述目标网页上获取与所述标识信息对应的侵权内容，并将所述侵权内容发布至区块链上进行存证。

6. 一种基于区块链的侵权取证装置，应用于取证服务器；所述装置包括：

接收单元，接收客户端发送的侵权取证请求，所述侵权取证请求由所述客户端根据目标网页的访问地址和所述目标网页上的侵权内容的标识信息生成，所述侵权内容由所述客户端根据用户针对目标网页的内容标记操作得到，所述客户端为浏览器搭载的插件程序，所述内容标记操作通过响应于所述用户针对所述插件程序的调用指令，执行所述插件程序以检测得到；

获取单元，响应于所述侵权取证请求，根据所述访问地址访问所述目标网页，并从所述目标网页上获取与所述标识信息对应的侵权内容；

存证单元，将所述侵权内容发布至区块链上进行存证。

7. 根据权利要求6所述的装置，所述侵权取证请求中还包含针对所述目标网页的登录信息；所述获取单元具体用于：

根据所述侵权取证请求中包含的登录信息登录所述目标网页；

从登录成功后的所述目标网页上获取与所述标识信息对应的侵权内容。

8. 根据权利要求6所述的装置，

所述侵权取证请求中还包含所述侵权内容；所述装置还包括：第一校验单元，在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容与所述侵权取证请求中包含的侵权内容是否一致；当获取到的侵权内容与所述侵权取证请求中包含的侵权内容一致时，执行存证侵权内容的操作；或者，

所述侵权取证请求中还包含所述侵权内容的校验值；所述装置还包括：第二校验单元，在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值是否一致；当获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值一致时，执行存证侵权内容的操作。

9. 一种电子设备，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求1所述的方法。

10. 一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求1所述方法的步骤。

11. 一种电子设备，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求2-4中任一项所述的方法。

12. 一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求2-4中任一项所述方法的步骤。

基于区块链的侵权取证方法及装置、电子设备、存储介质

技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域,尤其涉及一种基于区块链的侵权取证方法及装置、电子设备、存储介质。

背景技术

[0002] 区块链技术,也被称之为分布式账本技术,是一种由若干台计算设备共同参与“记账”,共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性,使得区块链技术已在众多的领域中广泛的进行应用。

发明内容

[0003] 有鉴于此,本说明书一个或多个实施例提供一种基于区块链的侵权取证方法及装置、电子设备、存储介质。

[0004] 为实现上述目的,本说明书一个或多个实施例提供技术方案如下:

[0005] 根据本说明书一个或多个实施例的第一方面,提出了一种基于区块链的侵权取证方法,应用于客户端;所述方法包括:

[0006] 响应于用户针对目标网页的内容标记操作,确定由所述用户标记出的所述目标网页上的侵权内容;

[0007] 根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请求;

[0008] 向取证服务器发送所述侵权取证请求,以使得所述取证服务器根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容,并将所述侵权内容发布至区块链上进行存证。

[0009] 可选的,所述客户端为浏览器搭载的插件程序;所述方法还包括:

[0010] 接收用户针对所述插件程序的调用指令;

[0011] 执行所述插件程序以检测用户针对目标网页的内容标记操作。

[0012] 根据本说明书一个或多个实施例的第二方面,提出了一种基于区块链的侵权取证方法,应用于取证服务器;所述方法包括:

[0013] 接收客户端发送的侵权取证请求,所述侵权取证请求由所述客户端根据目标网页的访问地址和所述目标网页上的侵权内容的标识信息生成,所述侵权内容由所述客户端根据用户针对目标网页的内容标记操作得到;

[0014] 响应于所述侵权取证请求,根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容;

[0015] 将所述侵权内容发布至区块链上进行存证。

[0016] 可选的,所述侵权取证请求中还包含针对所述目标网页的登录信息;所述从所述目标网页上获取与所述标识信息对应的侵权内容,包括:

[0017] 根据所述侵权取证请求中包含的登录信息登录所述目标网页;

- [0018] 从登录成功后的所述目标网页上获取与所述标识信息对应的侵权内容。
- [0019] 可选的，
- [0020] 所述侵权取证请求中还包含所述侵权内容；所述方法还包括：在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容与所述侵权取证请求中包含的侵权内容是否一致；当获取到的侵权内容与所述侵权取证请求中包含的侵权内容一致时，执行存证侵权内容的操作；或者，
- [0021] 所述侵权取证请求中还包含所述侵权内容的校验值；所述方法还包括：在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值是否一致；当获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值一致时，执行存证侵权内容的操作。
- [0022] 根据本说明书一个或多个实施例的第三方面，提出了一种基于区块链的侵权取证装置，应用于客户端；所述装置包括：
- [0023] 确定单元，响应于用户针对目标网页的内容标记操作，确定由所述用户标记出的所述目标网页上的侵权内容；
- [0024] 生成单元，根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请求；
- [0025] 发送单元，向取证服务器发送所述侵权取证请求，以使得所述取证服务器根据所述访问地址访问所述目标网页，并从所述目标网页上获取与所述标识信息对应的侵权内容，并将所述侵权内容发布至区块链上进行存证。
- [0026] 可选的，所述客户端为浏览器搭载的插件程序；所述装置还包括：
- [0027] 接收单元，接收用户针对所述插件程序的调用指令；
- [0028] 执行单元，执行所述插件程序以检测用户针对目标网页的内容标记操作。
- [0029] 根据本说明书一个或多个实施例的第四方面，提出了一种基于区块链的侵权取证装置，应用于取证服务器；所述装置包括：
- [0030] 接收单元，接收客户端发送的侵权取证请求，所述侵权取证请求由所述客户端根据目标网页的访问地址和所述目标网页上的侵权内容的标识信息生成，所述侵权内容由所述客户端根据用户针对目标网页的内容标记操作得到；
- [0031] 获取单元，响应于所述侵权取证请求，根据所述访问地址访问所述目标网页，并从所述目标网页上获取与所述标识信息对应的侵权内容；
- [0032] 存证单元，将所述侵权内容发布至区块链上进行存证。
- [0033] 可选的，所述侵权取证请求中还包含针对所述目标网页的登录信息；所述获取单元具体用于：
- [0034] 根据所述侵权取证请求中包含的登录信息登录所述目标网页；
- [0035] 从登录成功后的所述目标网页上获取与所述标识信息对应的侵权内容。
- [0036] 可选的，
- [0037] 所述侵权取证请求中还包含所述侵权内容；所述装置还包括：第一校验单元，在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容与所述侵权取证请求中包含的侵权内容是否一致；当获取到的侵权内容与所述侵权取证请求中包含的侵权内容一致时，执行存证侵权内容的操作；或者，

[0038] 所述侵权取证请求中还包含所述侵权内容的校验值；所述装置还包括：第二校验单元，在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值是否一致；当获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值一致时，执行存证侵权内容的操作。

[0039] 根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，包括：

[0040] 处理器；

[0041] 用于存储处理器可执行指令的存储器；

[0042] 其中，所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

[0043] 根据本说明书一个或多个实施例的第六方面，提出了一种电子设备，包括：

[0044] 处理器；

[0045] 用于存储处理器可执行指令的存储器；

[0046] 其中，所述处理器通过运行所述可执行指令以实现如第二方面所述的方法。

[0047] 根据本说明书一个或多个实施例的第七方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面所述方法的步骤。

[0048] 根据本说明书一个或多个实施例的第八方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第二方面所述方法的步骤。

[0049] 由以上实施例可见，当用户发现所访问的网页侵权时，可由该用户对网页上存在侵权问题的内容进行标记以告知取证服务器，那么取证服务器可获取侵权内容，并将获取到的侵权内容作为被侵权方的侵权追溯证据发布至区块链上进行存证，从而完成侵权取证的过程。

[0050] 由于侵权内容被发布至区块链上进行存证，各个区块链节点中均记录有一份完整的侵权内容，那么即使某个节点出现数据损坏的问题，也不会影响整体的数据完整性；同时，充分利用了区块链存储数据的不可篡改性和可追溯性，从而防止不法分子恶意修改侵权内容，保证了所记录侵权内容的安全，并可进行溯源。

[0051] 进一步的，上述标记侵权内容的过程可由用户配合搭载于浏览器的插件程序来完成。具体而言，当用户通过浏览器访问网页时，若发现该网页存在侵权问题，则可直接利用浏览器搭载的插件程序来完成取证的过程，从而有效提升了取证效率。

附图说明

[0052] 图1是一示例性实施例提供的一种创建智能合约的示意图；

[0053] 图2是一示例性实施例提供的调用智能合约的示意图；

[0054] 图3是一示例性实施例提供的创建智能合约和调用智能合约的示意图；

[0055] 图4是一示例性实施例提供的一种基于客户端侧的侵权取证方法的流程图；

[0056] 图5是一示例性实施例提供的一种基于取证服务器侧的侵权取证方法的流程图；

[0057] 图6是一示例性实施例提供的一种基于区块链的侵权取证方法的交互图；

[0058] 图7是一示例性实施例提供的一种侵权标记插件的示意图；

[0059] 图8是一示例性实施例提供的一种设备的结构示意图；

[0060] 图9是一示例性实施例提供的一种基于区块链的侵权取证装置的框图；

[0061] 图10是一示例性实施例提供的另一种设备的结构示意图；

[0062] 图11是一示例性实施例提供的另一种基于区块链的侵权取证装置的框图。

具体实施方式

[0063] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本发明说明书一个或多个实施例相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本发明说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0064] 需要说明的是:在其他实施例中并不一定按照本发明说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中,其方法所包括的步骤可以比本发明说明书所描述的更多或更少。此外,本发明说明书中所描述的单个步骤,在其他实施例中可能被分解为多个步骤进行描述;而本发明说明书中所描述的多个步骤,在其他实施例中也可能被合并为单个步骤进行描述。

[0065] 区块链一般被划分为三种类型:公有链(Public Blockchain),私有链(Private Blockchain)和联盟链(Consortium Blockchain)。此外,还可以有上述多种类型的结合,比如私有链+联盟链、联盟链+公有链等。

[0066] 其中,去中心化程度最高的是公有链。公有链以比特币、以太坊为代表,加入公有链的参与者(也可称为区块链中的节点)可以读取链上的数据记录、参与交易、以及竞争新区块的记账权等。而且,各节点可自由加入或者退出网络,并进行相关操作。

[0067] 私有链则相反,该网络的写入权限由某个组织或者机构控制,数据读取权限受组织规定。简单来说,私有链可以为一个弱中心化系统,其对节点具有严格限制且节点数量较少。这种类型的区块链更适合于特定机构内部使用。

[0068] 联盟链则是介于公有链以及私有链之间的区块链,可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织;节点通过授权加入网络并组成利益相关联盟,共同维护区块链运行。

[0069] 基于区块链的基本特性,区块链通常是由若干个区块构成。在这些区块中分别记录有与该区块的创建时刻对应的时间戳,所有的区块严格按照区块中记录的时间戳,构成一条在时间上有序的数据链条。

[0070] 对于物理世界产生的真实数据,可以将其构建成区块链所支持的标准的交易(transaction)格式,然后发布至区块链,由区块链中的节点设备对收到的交易进行共识处理,并在达成共识后,由区块链中作为记账节点的节点设备,将这笔交易打包进区块,在区块链中进行持久化存证。

[0071] 其中,区块链中支持的共识算法可以包括:

[0072] 第一类共识算法,即节点设备需要争夺每一轮的记账周期的记账权的共识算法;例如,工作量证明(Proof of Work,POW)、股权证明(Proof of Stake,POS)、委任权益证明(Delegated Proof of Stake,DPOS)等共识算法;

[0073] 第二类共识算法,即预先为每一轮记账周期选举记账节点(不需要争夺记账权)的共识算法;例如,实用拜占庭容错(Practical Byzantine Fault Tolerance,PBFT)等共识算法。

[0074] 在采用第一类共识算法的区块链网络中,争夺记账权的节点设备,都可以在接收到交易后执行该笔交易。争夺记账权的节点设备中可能有一个节点设备在本轮争夺记账权的过程中胜出,成为记账节点。记账节点可以将收到的交易与其它交易一起打包以生成最新区块,并将生成的最新区块或者该最新区块的区块头发送至其它节点设备进行共识。

[0075] 在采用第二类共识算法的区块链网络中,具有记账权的节点设备在本轮记账前已经商定好。因此,节点设备在接收到交易后,如果自身不是本轮的记账节点,则可以将该交易发送至记账节点。对于本轮的记账节点,在将该交易与其它交易一起打包以生成最新区块的过程中或者之前,可以执行该交易。记账节点在生成最新区块后,可以将该最新区块或者该最新区块的区块头发送至其它节点设备进行共识。

[0076] 如上所述,无论区块链采用以上示出的哪种共识算法,本轮的记账节点都可以将接收到的交易打包以生成最新区块,并将生成的最新区块或者该最新区块的区块头发送至其它节点设备进行共识验证。如果其它节点设备接收到最新区块或者该最新区块的区块头后,经验证没有问题,可以将该最新区块追加到原有的区块链末尾,从而完成区块链的记账过程。其它节点验证记账节点发来的新的区块或区块头的过程中,也可以执行该区块中的包含的交易。

[0077] 在实际应用中,不论是公有链、私有链还是联盟链,都可能提供智能合约(Smart contract)的功能。区块链上的智能合约是在区块链上可以被交易触发执行的合约。智能合约可以通过代码的形式定义。

[0078] 以以太坊为例,支持用户在以太坊网络中创建并调用一些复杂的逻辑。以太坊作为一个可编程区块链,其核心是以太坊虚拟机(EVM),每个以太坊节点都可以运行EVM。EVM是一个图灵完备的虚拟机,通过它可以实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在EVM上运行的。实际上,EVM直接运行的是虚拟机代码(虚拟机字节码,下简称“字节码”),所以部署在区块链上的智能合约可以是字节码。

[0079] 如图1所示,Bob将一笔包含创建智能合约信息的交易(Transaction)发送到以太坊网络后,各节点均可以在EVM中执行这笔交易。其中,图中1中交易的From字段用于记录发起创建智能合约的账户的地址,交易的数据字段的字段值保存的合约代码可以是字节码,交易的To字段的字段值为一个null(空)的账户。当节点间通过共识机制达成一致后,这个智能合约成功创建,后续用户可以调用这个智能合约。

[0080] 智能合约创建后,区块链上出现一个与该智能合约对应的合约账户,并拥有一个特定的地址;比如,图1中各节点中的“0x68e12cf284...”就代表了创建的这个合约账户的地址;合约代码(Code)和账户存储(Storage)将保存在该合约账户的账户存储中。智能合约的行为由合约代码控制,而智能合约的账户存储则保存了合约的状态。换句话说,智能合约使得区块链上产生包含合约代码和账户存储的虚拟账户。

[0081] 前述提到,包含创建智能合约的交易的Data字段保存的可以是该智能合约的字节码。字节码由一连串的字节组成,每一字节可以标识一个操作。基于开发效率、可读性等多方面考虑,开发者可以不直接书写字节码,而是选择一门高级语言编写智能合约代码。例如,高级语言可以采用诸如Solidity、Serpent、LLL语言等。对于采用高级语言编写的智能合约代码,可以经过编译器编译,生成可以部署到区块链上的字节码。

[0082] 以Solidity语言为例,用其编写的合约代码与面向对象编程语言中的类(Class)

很相似,在一个合约中可以声明多种成员,包括状态变量、函数、函数修改器、事件等。状态变量是永久存储在智能合约的账户存储(Storage)字段中的值,用于保存合约的状态。

[0083] 如图2所示,仍以以太坊为例,Bob将一笔包含调用智能合约信息的交易发送到以太坊网络后,各节点均可以在EVM中执行这笔交易。其中,图2中交易的From字段用于记录发起调用智能合约的账户的地址,To字段用于记录被调用的智能合约的地址,交易的Data字段用于记录调用智能合约的方法和参数。调用智能合约后,合约账户的账户状态可能改变。后续,某个客户端可以通过接入的区块链节点(例如图2中的节点1)查看合约账户的账户状态。

[0084] 智能合约可以以规定的方式在区块链网络中每个节点独立的执行,所有执行记录和数据都保存在区块链上,所以当这样的交易执行完毕后,区块链上就保存了无法篡改、不会丢失的交易凭证。

[0085] 创建智能合约和调用智能合约的示意图如图3所示。以太坊中要创建一个智能合约,需要经过编写智能合约、变成字节码、部署到区块链等过程。以太坊中调用智能合约,是发起一笔指向智能合约地址的交易,各个节点的EVM可以分别执行该交易,将智能合约代码分布式的运行在以太坊网络中每个节点的虚拟机中。

[0086] 请参见图4,图4是一示例性实施例提供的一种基于区块链的侵权取证方法的流程图。如图4所示,该方法应用于客户端,可以包括以下步骤:

[0087] 步骤402,响应于用户针对目标网页的内容标记操作,确定由所述用户标记出的所述目标网页上的侵权内容。

[0088] 在一实施例中,用户在访问目标网页时,若发现该网页中的内容存在侵权问题,可对网页上存在侵权问题的内容(后文简称为侵权内容)进行标记,从而告知取证服务器所标记的内容存在侵权问题,进而由取证服务器获取目标网页的侵权内容,并发布至区块链上进行存证。

[0089] 针对用户标记侵权内容的过程,由于用户通常通过浏览器访问网页,可开发一搭载于浏览器的插件程序用于标记侵权内容。换言之,本实施例应用的客户端为浏览器搭载的插件程序。那么,当用户存在标记侵权内容的需求时,可直接调用浏览器中搭载的插件程序来标记侵权内容,而无需通过其他类似于拍照、截图等方式来进行取证,从而可有效提升取证效率。例如,用户可向浏览器下发针对插件程序的调用指令,那么浏览器在接收到该调用指令后,执行该插件程序以检测用户针对目标网页的内容标记操作。

[0090] 当然,对于上述用于标记侵权内容的插件程序,可采用各种编程语言进行开发,插件程序的具体类型也可依据实际需求灵活选取。例如,可采用*.ocx、*.dll、*.cab、*.exe等文件类型的插件程序,本说明书一个或多个实施例并不对此进行限制。

[0091] 步骤404,根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请求。

[0092] 步骤406,向取证服务器发送所述侵权取证请求,以使得所述取证服务器根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容,并将所述侵权内容发布至区块链上进行存证。

[0093] 相应的,请参见图5,图5是一示例性实施例提供的一种基于区块链的侵权取证方法的流程图。如图5所示,该方法应用于取证服务器,可以包括以下步骤:

[0094] 步骤502,接收客户端发送的侵权取证请求,所述侵权取证请求由所述客户端根据目标网页的访问地址和所述目标网页上的侵权内容的标识信息生成,所述侵权内容由所述客户端根据用户针对目标网页的内容标记操作得到。

[0095] 在本实施例中,标记的过程可参考上述图4所示实施例中的标记过程,在此不再赘述。

[0096] 步骤504,响应于所述侵权取证请求,根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容。

[0097] 在本实施例中,一些网页的内容可能需要用户登录以后才能访问。因此,当用户发现访问的网页(登录成功以后)中的内容存在侵权问题时,可生成侵权取证请求以指示取证服务器进行取证。而在生成侵权取证请求时,除目标网页的访问地址和侵权内容的标识信息之外,还可在侵权取证请求中添加针对目标网页的登录信息。那么,取证服务器在接收到该侵权取证请求后,可先根据侵权取证请求中包含的登录信息登录目标网页,再从登录成功后的目标网页上获取与标识信息对应的侵权内容,从而避免因未登录成功导致无法获取侵权内容的问题。

[0098] 步骤506,将所述侵权内容发布至区块链上进行存证。

[0099] 在本实施例中,网页通常支持对网页上的内容进行修改的功能,在取证的过程中或者后续判定侵权的过程中,存在侵权方(即目标网页上侵权内容的发布方)修改侵权内容的可能。因此,可将用户标记的侵权内容或者该侵权内容的校验值添加至侵权取证请求中,从而确保取证服务器能够获取到用户实际标记的侵权内容。

[0100] 在一种情况下,侵权取证请求中包含侵权内容,那么取证服务器在获取到与标识信息对应的侵权内容后,可先确定获取到的侵权内容与侵权取证请求中包含的侵权内容是否一致,当获取到的侵权内容与侵权取证请求中包含的侵权内容一致时,再执行存证侵权内容的操作。

[0101] 在另一种情况下,侵权取证请求中包含侵权内容的校验值,那么取证服务器在获取到与标识信息对应的侵权内容后,可先计算获取到的侵权内容的校验值,再确定获取到的侵权内容的校验值与侵权取证请求中包含的校验值是否一致,并在获取到的侵权内容的校验值与侵权取证请求中包含的校验值一致时,执行存证侵权内容的操作。

[0102] 由以上实施例可见,当用户发现所访问的网页侵权时,可由该用户对网页上存在侵权问题的内容进行标记以告知取证服务器,那么取证服务器可获取侵权内容,并将获取到的侵权内容作为被侵权方的侵权追溯证据发布至区块链上进行存证,从而完成侵权取证的过程。

[0103] 由于侵权内容被发布至区块链上进行存证,各个区块链节点中均记录有一份完整的侵权内容,那么即使某个节点出现数据损坏的问题,也不会影响整体的数据完整性;同时,充分利用了区块链存储数据的不可篡改性和可追溯性,从而防止不法分子恶意修改侵权内容,保证了所记录侵权内容的安全,并可进行溯源。

[0104] 进一步的,上述标记侵权内容的过程可由用户配合搭载于浏览器的插件程序来完成。具体而言,当用户通过浏览器访问网页时,若发现该网页存在侵权问题,则可直接利用浏览器搭载的插件程序来完成取证的过程,从而有效提升了取证效率。

[0105] 为了便于理解,下面结合举例和附图6-7对本说明书的侵权取证方案进行详细说

明。

[0106] 如图6所示,由浏览器61与取证服务器62之间进行交互来完成取证过程,该取证过程可以包括以下步骤:

[0107] 步骤602,用户通过浏览器61访问目标网页A。

[0108] 在本实施例中,浏览器61中搭载有侵权标记插件,当用户发现当前访问的网页存在侵权问题时,可直接调用浏览器上的侵权标记插件,对目标网页A上的侵权内容进行标记。

[0109] 步骤604,侵权标记插件检测用户针对目标网页A的内容标记操作。

[0110] 如图7所示,浏览器61上安装有侵权标记插件,可通过图中的“侵权取证标记”按钮来触发启动该插件。例如,用户可通过鼠标点击“侵权取证标记”按钮来调用侵权标记插件,当浏览器61检测到针对该按钮的点击操作时,执行侵权标记插件。而当触发执行侵权标记插件时,目标网页A上的各个页面区域更换为可选择状态以供用户选取进行标记。比如,目标网页A上包含页面区域A1~A6,用户可以通过鼠标勾选包含侵权内容的页面区域来完成对侵权内容的标记。

[0111] 步骤606,侵权标记插件生成侵权取证请求。

[0112] 在本实施例中,一些网页的内容可能需要用户登录以后才能访问。因此,可在侵权取证请求中添加目标网页的访问地址、针对目标网页的登录信息和侵权内容的标识信息,以使得取证服务器可先根据访问地址访问目标网页,再根据该登录信息登录目标网页,从而成功获取与标识信息对应的侵权内容(即用户标记的侵权内容)。举例而言,访问地址可以是目标网页的网页地址,登录信息可以是用于登录目标网页的cookie,标识信息可以是用户选取的页面区域的标识符。

[0113] 除此之外,网页通常支持对网页上的内容进行修改的功能,在取证的过程中或者后续判定侵权的过程中,存在侵权方(即目标网页上侵权内容的发布方)修改侵权内容的可能。因此,还可将用户标记的侵权内容或者该侵权内容的校验值添加至侵权取证请求中,从而确保取证服务器能够获取到用户实际标记的侵权内容。以添加检验值为例,可采用MD5(Message-Digest Algorithm,信息摘要算法)、CRC(Cyclic Redundancy Check,循环冗余校验)、LRC(Longitudinal Redundancy Check,纵向冗余校验)、哈希计算(hash)等算法对侵权内容进行计算进而得到校验值,当然,本说明书一个或多个实施例并不对采用的算法进行限制。

[0114] 步骤608,侵权标记插件向取证服务器62发送侵权取证请求。

[0115] 步骤610,取证服务器62访问目标网页A,获取侵权内容。

[0116] 承接于上述举例,取证服务器62根据侵权取证请求中包含的网址访问目标网页A,并根据侵权取证请求中包含的cookie登录目标网页A,从而再根据标识符获取相应的页面内容,即侵权内容。

[0117] 步骤612,取证服务器62校验侵权内容。

[0118] 承接于上述举例,假定侵权标记插件采用hsah算法计算得到第一校验值并添加至侵权取证请求中,那么取证服务器62在获取到侵权内容后,采用同一hash算法对获取到的侵权内容进行hsah计算得到第二校验值。若第一校验值与第二校验值一致,则执行步骤614;否则,向侵权标记插件返回相应的提示消息。例如,提示消息可以为“标记内容与网页

实际内容不符”，或者“网页侵权内容已修改”等。

[0119] 步骤614，取证服务器62将侵权内容发布至区块链B上进行存证。

[0120] 在本实施例中，取证服务器62作为区块链的客户端与区块链节点对接，当校验结果为一致时，取证服务器62打包一笔用于存证侵权内容的交易，并向区块链节点提交该交易，以使得区块链节点在共识通过后将侵权内容发布至区块链上进行存证。

[0121] 由以上实施例可见，基于浏览器插件的取证形式，交由线下大量的访问网页的用户来进行网页侵权举报，并通过取证服务器将侵权内容上链来固化侵权证据，从而完成对线上网页普遍存在的侵权行为进行有效记录，有利于提高取证效率。

[0122] 需要说明的是，本说明书中的侵权取证方案还可进一步将与侵权内容对应的被侵权方，以及相应的被侵权内容发送至取证服务器。作为一示例性实施例，可同样采用与上述对侵权内容进行取证的方式，指示取证服务器获取被侵权网页中的被侵权内容，并将被侵权内容发布至区块链上与侵权内容关联存证。例如，被侵权内容同样由用户进行标记，可在上述侵权取证请求中记录目标网页（即侵权网页）的访问地址、目标网页的登录信息、侵权内容的标识信息，以及被侵权网页的访问地址、侵权网页的登录信息、被侵权内容的标识信息等数据，那么取证服务器可根据上述数据获取到侵权内容和被侵权内容，从而将侵权内容和被侵权内容（两者共同作为侵权证据）关联存证以用于侵权判定。

[0123] 进一步的，可在区块链上部署智能合约，该智能合约用于判定区块链上关联存证的侵权内容与被侵权内容实际上是否构成侵权行为。举例而言，可开发一侵权判定合约，该侵权判定合约中声明有侵权判定逻辑，用于校验侵权证据（侵权内容和相应的被侵权内容）是否符合侵权条件。其中，侵权条件可根据实际需求灵活设定，本说明书一个或多个实施例并不对此进行限制。

[0124] 基于上述对侵权判定合约的部署，侵权标记插件可监听区块链上存证的数据，当监听到区块链上存证有针对目标网页的侵权证据时，创建针对目标网页的侵权判定交易（侵权判定交易的to字段内容为侵权判定合约的合约地址，即交易用于调用侵权判定合约），并向区块链节点提交该侵权判定交易，以使得区块链节点调用侵权判定合约，根据侵权判定合约中声明的侵权判定逻辑校验对应于目标网页的侵权证据是否符合侵权条件，以及根据校验结果生成针对目标网页的侵权判定结果。由此可见，通过本说明书的取证方式和侵权判定方式，可由用户在浏览网页并发现侵权行为时及时进行取证举报，并将侵权内容上链来固化侵权证据，以及通过智能合约来完成侵权判定，从而可简化用户操作，有利于提高取证效率和侵权判定的效率。

[0125] 与上述方法实施例相对应，本说明书还提供了一种应用于客户端的基于区块链的侵权取证装置的实施例。

[0126] 本说明书的基于区块链的侵权取证装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。

[0127] 从硬件层面而言，请参考图8，图8是一示例性实施例提供的一种设备的示意结构图。如图8所示，在硬件层面，该设备包括处理器802、内部总线804、网络接口806、内存808以及非易失性存储器810，当然还可能包括其他业务所需要的硬件。处理器802从非易失性存

存储器810中读取对应的计算机程序到内存808中然后运行,在逻辑层面上形成基于区块链的侵权取证装置。当然,除了软件实现方式之外,本说明书一个或多个实施例并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[0128] 请参考图9,在软件实施方式中,该基于区块链的侵权取证装置应用于客户端,可以包括:

[0129] 确定单元91,响应于用户针对目标网页的内容标记操作,确定由所述用户标记出的所述目标网页上的侵权内容;

[0130] 生成单元92,根据所述目标网页的访问地址和所述侵权内容的标识信息生成侵权取证请求;

[0131] 发送单元93,向取证服务器发送所述侵权取证请求,以使得所述取证服务器根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容,并将所述侵权内容发布至区块链上进行存证。

[0132] 可选的,所述客户端为浏览器搭载的插件程序;所述装置还包括:

[0133] 接收单元94,接收用户针对所述插件程序的调用指令;

[0134] 执行单元95,执行所述插件程序以检测用户针对目标网页的内容标记操作。

[0135] 与上述方法实施例相对应,本说明书还提供了一种应用于取证服务器的基于区块链的侵权取证装置的实施例。

[0136] 本说明书的基于区块链的侵权取证装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为一个逻辑意义上的装置,是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。

[0137] 从硬件层面而言,请参考图10,图10是一示例性实施例提供的一种设备的示意结构图。如图10所示,在硬件层面,该设备包括处理器1002、内部总线1004、网络接口1006、内存1010以及非易失性存储器1010,当然还可能包括其他业务所需要的硬件。处理器1002从非易失性存储器1010中读取对应的计算机程序到内存1010中然后运行,在逻辑层面上形成基于区块链的侵权取证装置。当然,除了软件实现方式之外,本说明书一个或多个实施例并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[0138] 请参考图11,在软件实施方式中,该基于区块链的侵权取证装置应用于取证服务器,可以包括:

[0139] 接收单元1101,接收客户端发送的侵权取证请求,所述侵权取证请求由所述客户端根据目标网页的访问地址和所述目标网页上的侵权内容的标识信息生成,所述侵权内容由所述客户端根据用户针对目标网页的内容标记操作得到;

[0140] 获取单元1102,响应于所述侵权取证请求,根据所述访问地址访问所述目标网页,并从所述目标网页上获取与所述标识信息对应的侵权内容;

[0141] 存证单元1103,将所述侵权内容发布至区块链上进行存证。

[0142] 可选的,所述侵权取证请求中还包含针对所述目标网页的登录信息;所述获取单元1102具体用于:

[0143] 根据所述侵权取证请求中包含的登录信息登录所述目标网页；

[0144] 从登录成功后的所述目标网页上获取与所述标识信息对应的侵权内容。

[0145] 可选的，

[0146] 所述侵权取证请求中还包含所述侵权内容；所述装置还包括：第一校验单元1104，在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容与所述侵权取证请求中包含的侵权内容是否一致；当获取到的侵权内容与所述侵权取证请求中包含的侵权内容一致时，执行存证侵权内容的操作；或者，

[0147] 所述侵权取证请求中还包含所述侵权内容的校验值；所述装置还包括：第二校验单元1105，在获取到与所述标识信息对应的侵权内容后，确定获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值是否一致；当获取到的侵权内容的校验值与所述侵权取证请求中包含的校验值一致时，执行存证侵权内容的操作。

[0148] 上述实施例阐明的系统、装置、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。

[0149] 在一个典型的配置中，计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[0150] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存 (flash RAM)。内存是计算机可读介质的示例。

[0151] 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、磁盘存储、量子存储器、基于石墨烯的存储介质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脑可读媒体 (transitory media)，如调制的数据信号和载波。

[0152] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0153] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可

以的或者可能是有利的。

[0154] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0155] 应当理解,尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本说明书一个或多个实施例范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0156] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已,并不用以限制本说明书一个或多个实施例,凡在本说明书一个或多个实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本说明书一个或多个实施例保护的范围之内。

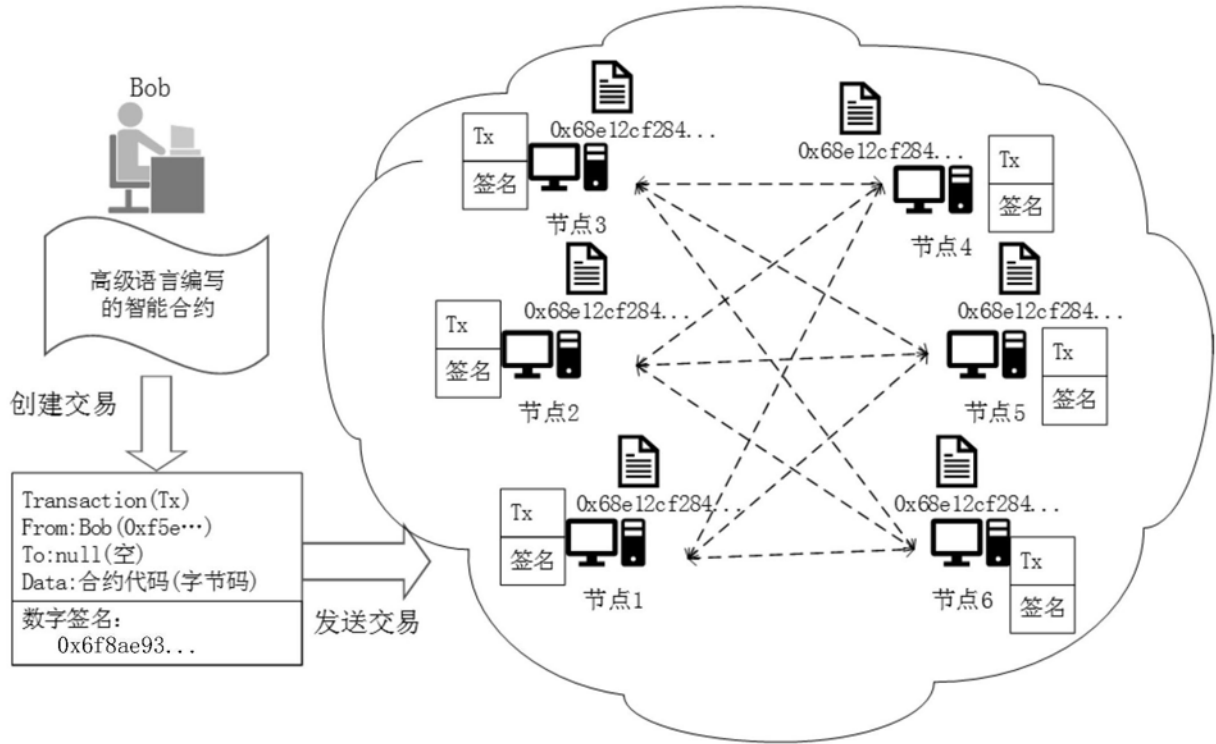


图1

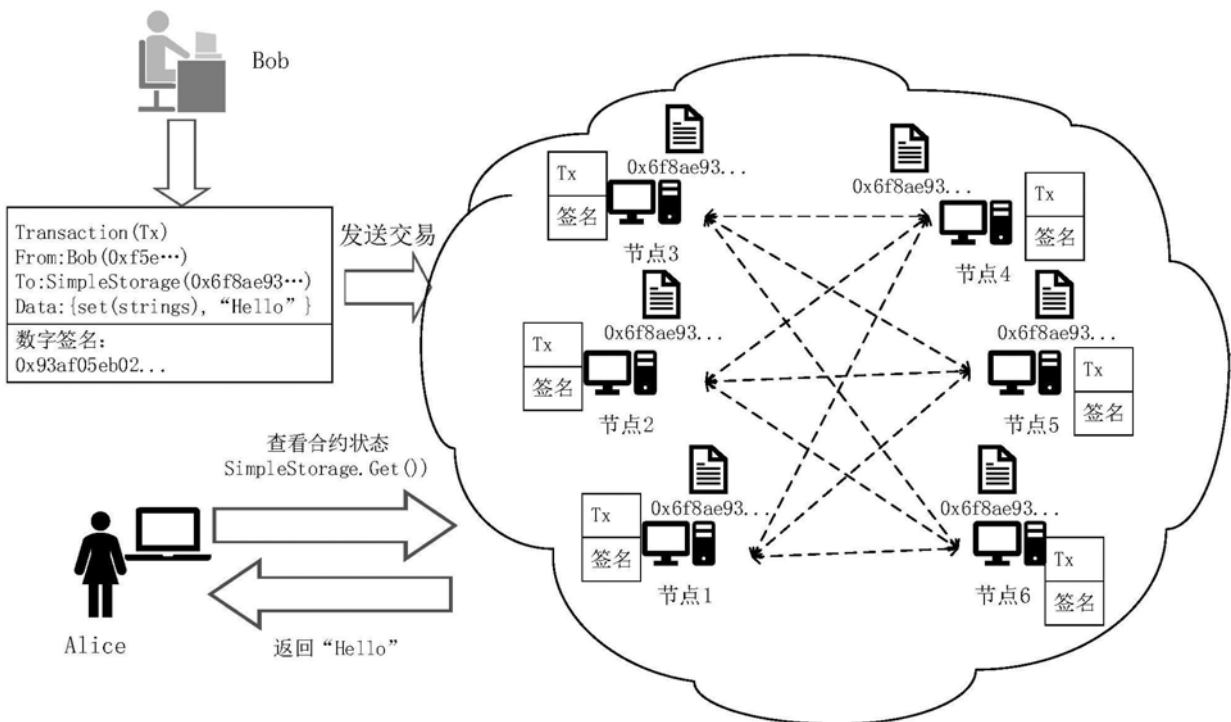


图2

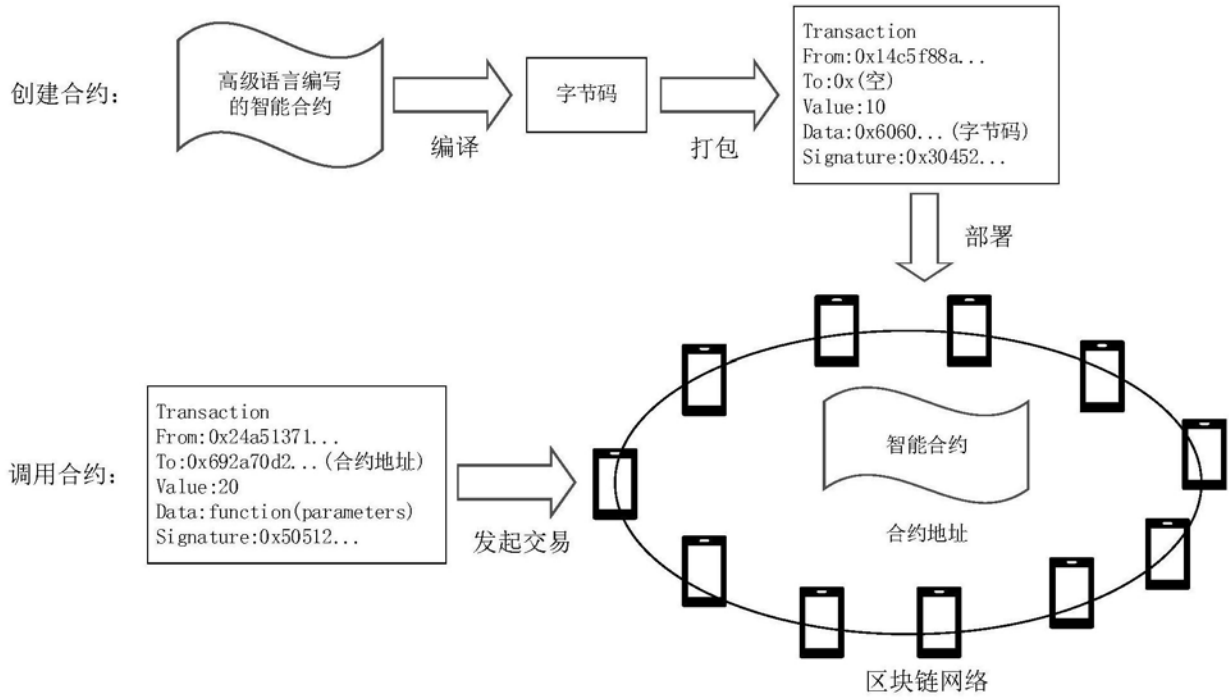


图3

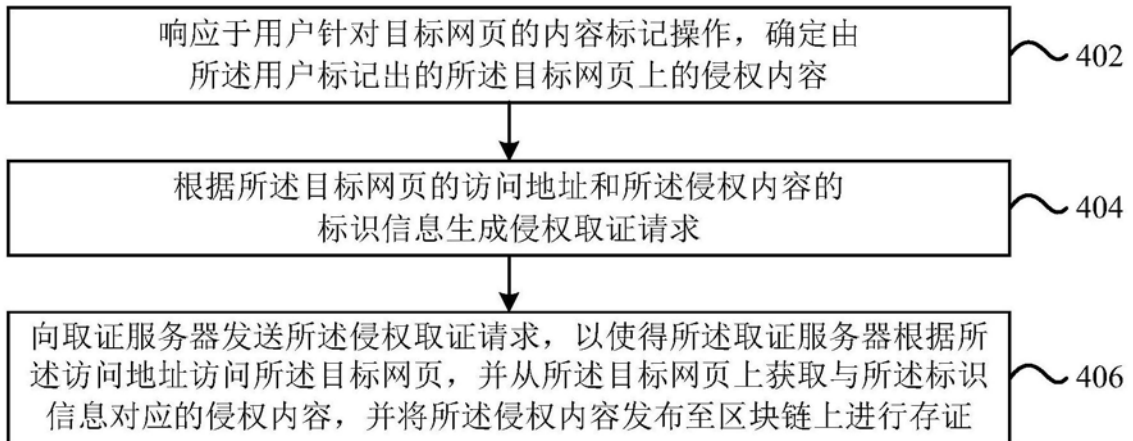


图4

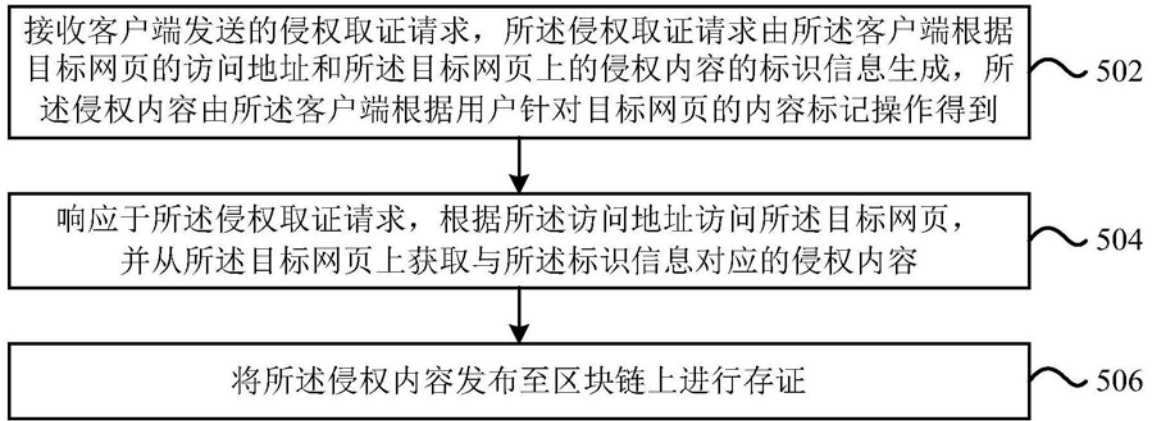


图5

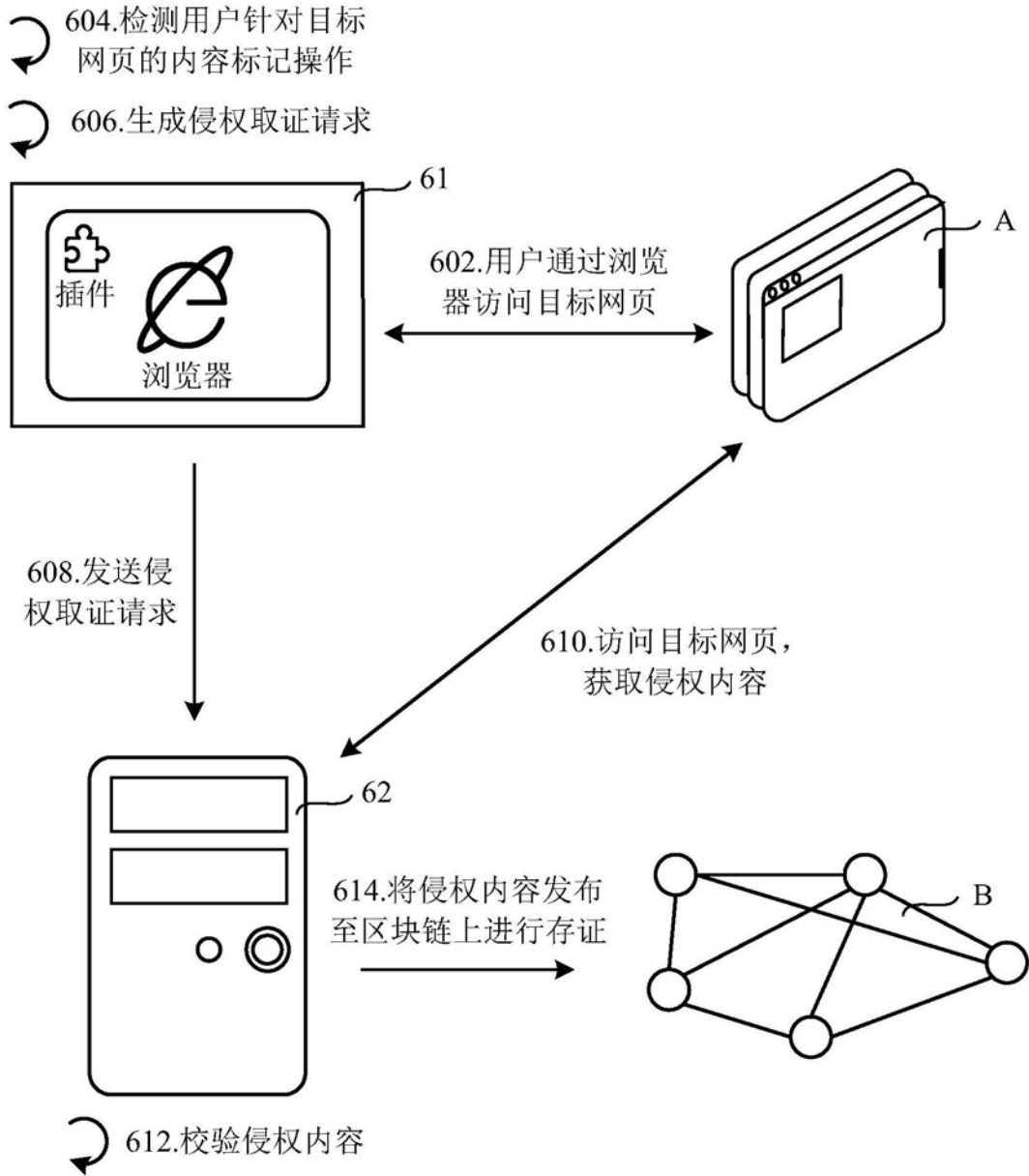


图6

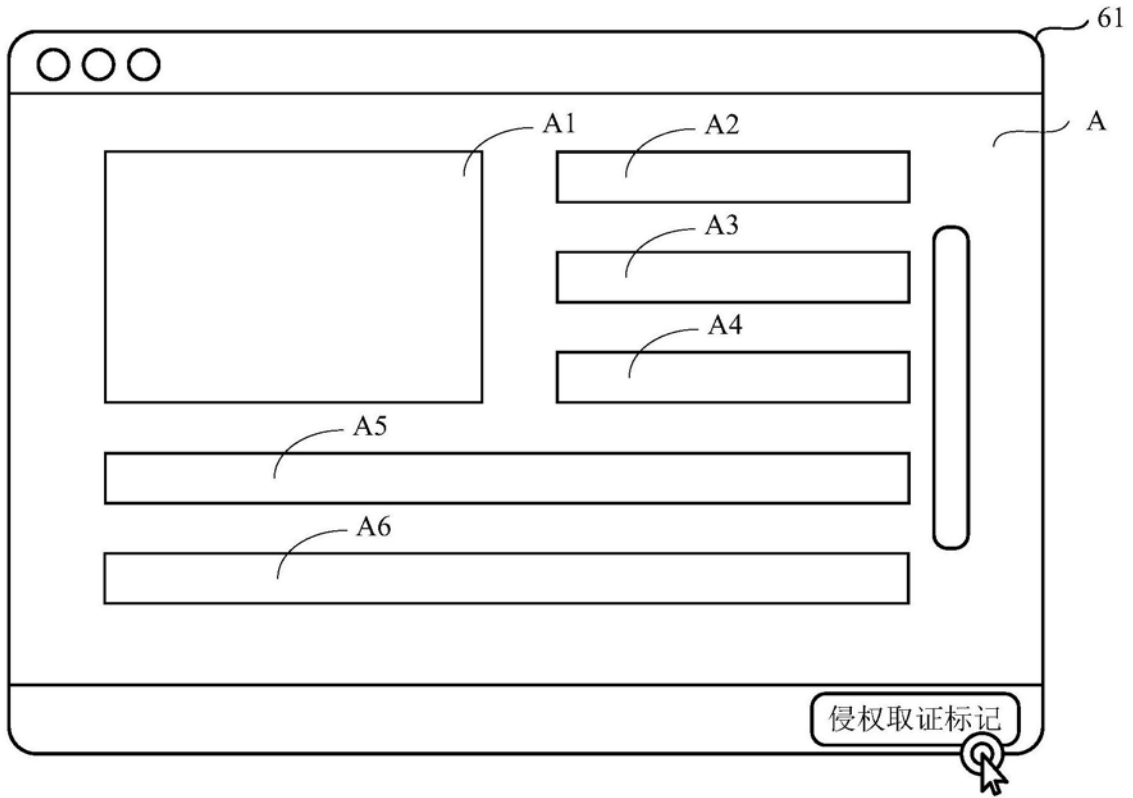


图7

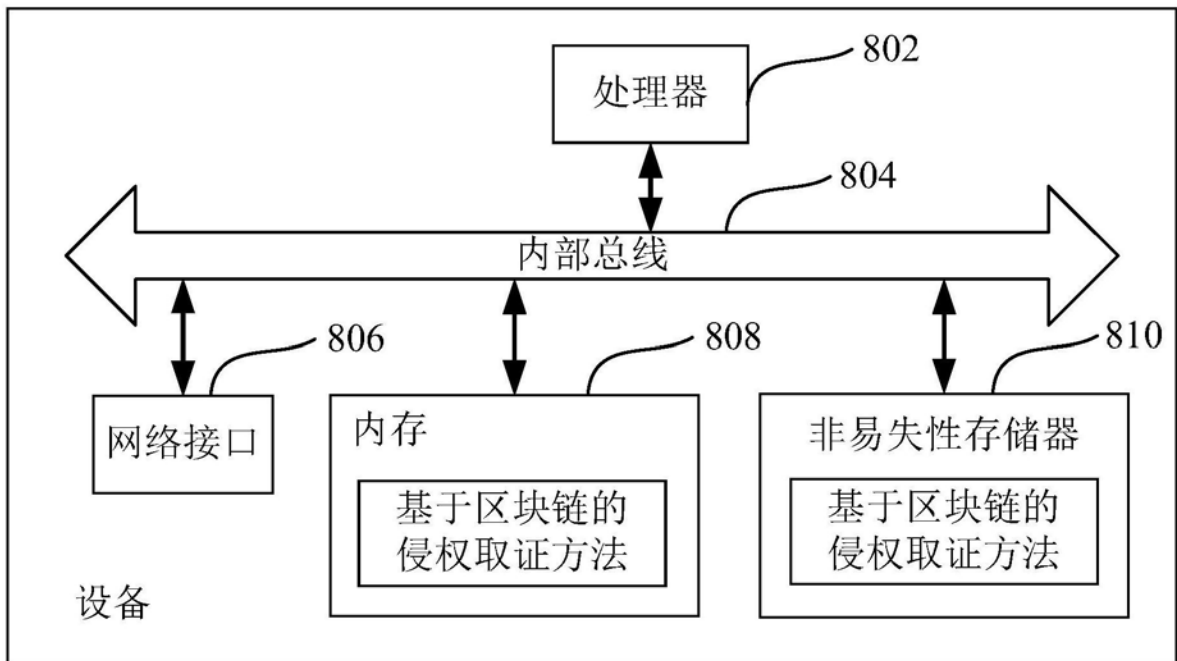


图8

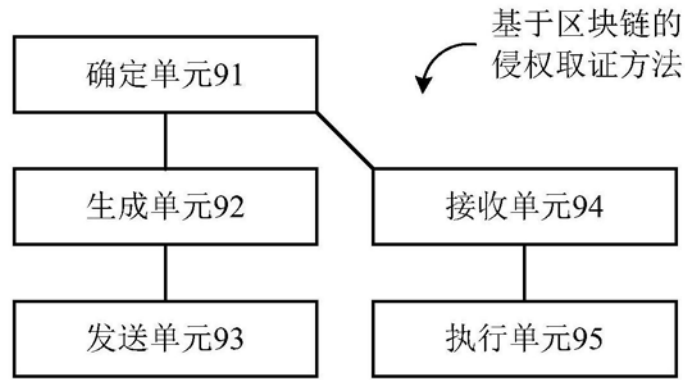


图9

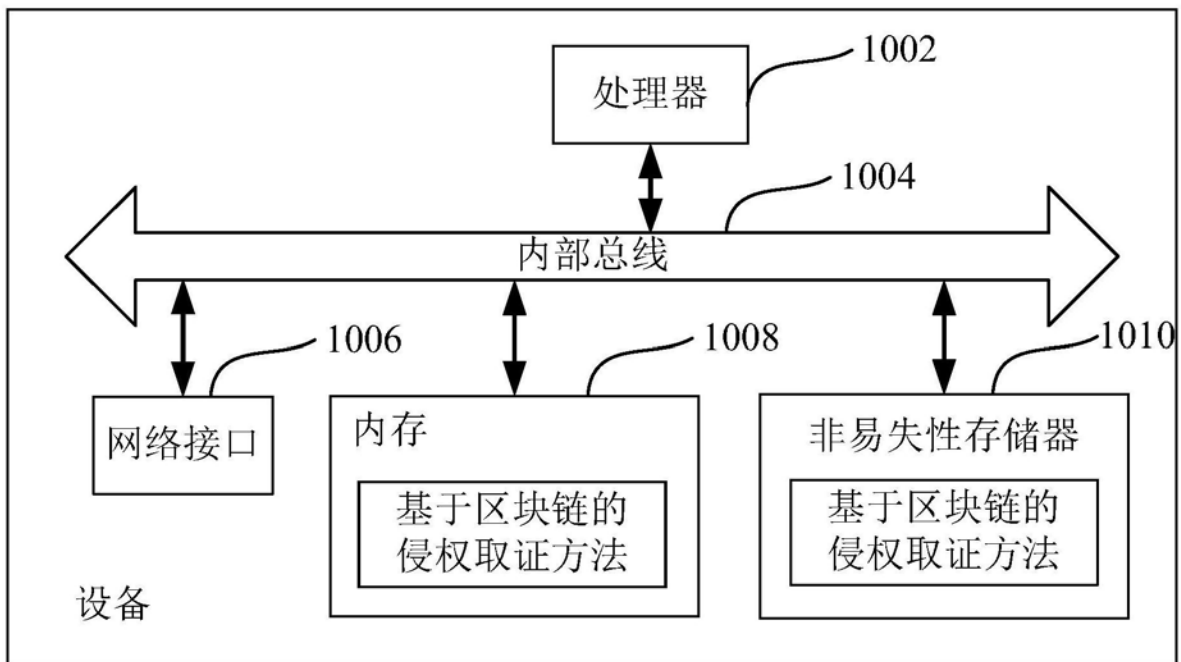


图10

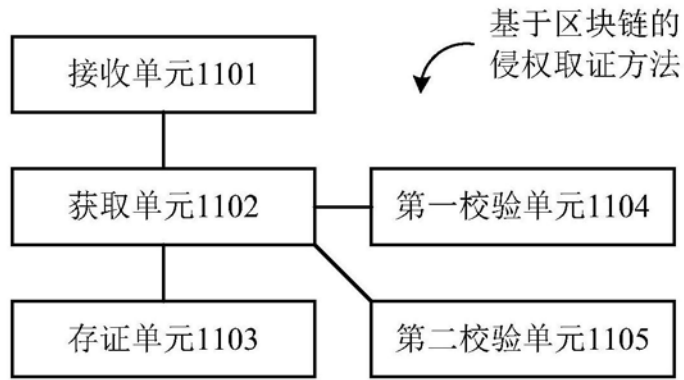


图11