# (19)中华人民共和国国家知识产权局

(12)发明专利申请



(10)申请公布号 CN xxxxxxxxx A

(43)申请公布日 xxxx.xx.xx

(21)申请号 xxxxxxxxxxxx .X

(22)申请日 xxxx .xx .xx

(71)申请人 xxx（北京）科技有限公司

地址 xxxx

(72)发明人 xxx

( 51 )Int .Cl .

|  |  |
| --- | --- |
| *H04L* | *29/06*( 2006 .01 ) |
| *H04L* | *9/32*( 2006 .01 ) |
| *G06F* | *21/62*( 2013 .01 ) |

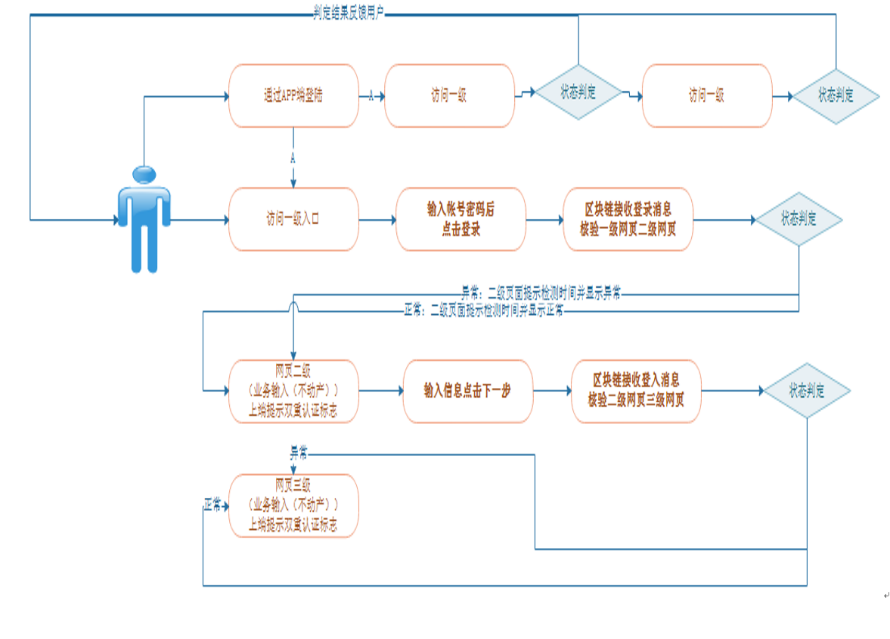


权利要求书2页 说明书5页 附图2页

(54)发明名称

基于区块链技术的网页双重验证防篡改方法

(57)摘要

本发明是一种基于区块链技术的网页双重验证防篡改方法，包括1）客户端程序文件预先打包，通过区块链上链，如果是客户端程序格式文件要上传区块链，先将客户端程序打包形成xxx格式文件，然后区块链将已经打包好xxx格式文件上链生成xxx-HASH加密标识数据，最后将此数据保存在区块链分布式系统中（原始客户端程序文件xxx-HASH加密标识）；2） 网页/信息系统入口等各级链接文件预先打包，成前端js格式文件，将前端js格式文件生成xxx-HASH加密标识，最后将此数据保存在区块链分布式系统中（原始各级链接xxx-HASH加密标识）；3）在使用上述区块链技术的上链过程中，数据经过哈希加密处理。本发明通过将用户在打开或者登入客户端、网页、或者信息系统入口时，通过自动生成客户端程序启动文件或链接文件打包的HASH和预先在区块链分布式系统中的客户端程序文件、网页、信息系统入口各级链接的原始哈希标识，进行核验，从根源上解决了现在出现的防钓鱼、网络攻击行为；数据核验过程中采用网页双重验证防篡改方法处理，保证了用户数据的安全性。

CN 107181765 A

# 权 利 要 求 书 1/2 页



CN xxxxxxxxx A

1 .一种基于区块链技术的网页双重验证防篡改方法，其特征在于，所述的方法包括：

1）用户打开客户端程序，系统自动打包生成a.xxx-HASH标识，区块链预先将客户端程序文件打包，通过区块链上链，如果是客户端程序格式文件要上传区块链，先将客户端程序打包形成xxx格式文件，然后区块链将已经打包好xxx格式文件上链生成b.xxx-HASH加密标识数据，最后将此数据保存在区块链分布式系统中（原始客户端程序文件xxx-HASH加密标识）；如果核验a与b不相等，发送请求给用户关闭客户端程序，客户端启动失败；

2）用户访问网页/信息入口时，系统自动将各级链接文件打包生成a.xxx-HASH标识，区块链预先将网页/信息系统入口等各级链接文件预先打包，成前端js格式文件，采用区块链上链技术，将前端js格式文件生成b.xxx-HASH加密标识，最后将此数据保存在区块链分布式系统中（原始各级链接xxx-HASH加密标识）；如果核验a与b不相等，发送请求给用户，网页访问失败，请重新访问；

3）在使用上述区块链核验过程中，数据经过预先上链处理。

2.根据权利要求1所述的网页双重验证防篡改方法，其特征在于，所述的生成防篡改的JS文件处理方法如下：

1）选择网页中进行访问的url网址链接；

2）将网页中相关需求的url网址链接写入html静态页面（每个页面中有一个URL链接），然后将静态页面放入js文件中（此操作就是打包js文件）；

3）读取js文件，通过MD5加密算法，对js文件进行HASH加密，形成js文件的HASH加密码；

4）将形成js文件的HASH加密码通过区块链上链技术写入区块链，并保存在区块链分布式系统；

3.根据权利要求2所述的网页双重验证防篡改方法，其特征在于，所述JS文件防篡改应用处理方法如下：

1）用户预备选择相关网页；

2）用户点击网页触发JS文件xxx；

3）主机后台通过用户点击的相关js文件读取当前js文件；

4）web端将读取的js文件生成HASH码文件；

5）验证端读取原存档HASH文件；

6）验证端将web端读取的js文件生成的HASH码文件与原存档HASH文件两者的js的HASH进行比较；

①一致：页面处理正常信息返回给用户，进行下一步登录操作。

②不一致：页面处理异常信息返回给用户，进行异常处理重新加载页面或者关闭页面。

4 .根据权利要求2所述的网页双重验证防篡改方法，其特征在于，所述JS文件防篡改功能处理方法如下：

1）用户收到网页正常信息；

2）用户点击网页的服务或功能按钮触发；

3）web网页端将触发消息的当前页面网页的XX文件或信息系统的XXX文件，按XXX流程，生成当前HASH；

4）web端通过HTTP协议中request.setAttribute（‘HASH’,HASH）方法将当前生成HASH码存入request域对象；

5）web网页端通过发送触发消息请求到云后台；

6）云后台接收到功能触发消息；

7）云后台通过域对象request.getAttribute(“HASH”)方法获取HASH码；

8）云后台将获取的HASH码与原始区块链分布式系统中的HASH进行核验：

①一致：页面处理正常信息返回给用户，收到正常指令后，下一步按钮可以点击。

②不一致：页面处理异常信息返回给用户，提示系统风险，进行异常处理，提示检查环境重新加载页面或者关闭页面。

# 基于区块链的网页双重验证防篡改方法

技术领域

[0001] 本发明涉及计算机网络安全技术，尤其是涉及网页双重验证防篡改安全管理体系，完成对用户的登录、认证和传输等过程安全验证。

背景技术

[0002] 当我们使用一些网页或者客户端进行启动、访问或者登入的操作时，都需要经过各种网络身份登录、认证和传输等过程。现在我们的网络身份都已经基本实名制，其中包含了我们重要的基本信息。

[0003] 信息化服务通过网页、系统功能界面，实现与用户的交互。攻击者通过篡改、劫持网页或信息系统的登陆端，实现钓鱼攻击、链接劫持攻击，通过劫持，将用户的访问引导到攻击者的页面进行欺骗，达到窃取用户信息、盗窃材料资金等目标。

[0004] 双重验证：双重验证也称为区块链上链验证，是指在计算机及计算机网络系统中确认操作者启动客户端程序或者登入时的安全过程，通过区块链上链预先保存的原始数据HASH与用户访问、打开网页/客户端程序时自动生成的HASH标识数据两者进行核验，是否一致，从而确定该用户是否具有对某种资源在启动和访问过程中的安全性，进而使计算机和网络系统的访问策略能够可靠、有效地执行，防止钓鱼攻击者假冒合法用户获得资源信息，保证系统和数据的安全，以及保护用户的信息安全。

[0005] 区块链是指以去中心化和去信任的方式集体维护一个可靠数据库的技术方案，其交易过程如下：

第一步：所有者a利用她的私钥对前一次交易和下一位所有者b签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单；

第二步：a将交易单广播至全网，比特币就发送给了b，每个节点都将收到的交易信息纳入一个区块；

第三步：每个节点通过解一道数学题，从而去获得创建新区块的权利，并争取得到比特币的奖励（新的比特币会在此过程中产生）；

第四步：当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易，并对全网其他节点核对；

第五步：全网其他节点核对该区块记账的正确性，没有错误后他们将该合法区域之后竞争下一个区块，这样就形成了一个合法记账的区块链。

[0006] 如何建立一种基于区块链上链双重验证的数据平台，从根源上解决了防钓鱼、网络诈骗行为，保证数据的安全性是当务之急。

发明内容

[0007] 本发明的目的是提出一种基于区块链技术的网页双重验证防篡改方法，给不同应用提供数据存储认证等服务，其融合了区块链上链，有效保证了信息的安全性。可用于客户端程序或者网页、信息系统入口等用户访问时安全保证。

[0008] 为了实现本发明的目的，采用以下技术方案：

一种基于区块链技术的网页双重验证防篡改方法，其特征在于，所述的方法包括：

1）用户打开客户端程序，系统自动打包生成a.xxx-HASH标识，区块链预先将客户端程序文件打包，采用区块链上链技术，如果是客户端程序格式文件要上传区块链，先将客户端程序打包形成xxx格式文件，然后区块链将已经打包好xxx格式文件上链生成b.xxx-HASH加密标识数据，最后将此数据保存在区块链分布式系统中（原始客户端程序文件xxx-HASH加密标识）；如果核验a与b不相等，发送请求给用户关闭客户端程序，客户端启动失败；

2）用户访问网页/信息入口时，系统自动将各级链接文件打包生成a.xxx-HASH标识，区块链预先将网页/信息系统入口等各级链接文件预先打包，成前端js格式文件，采用区块链上链技术，将前端js格式文件生成b.xxx-HASH加密标识，最后将此数据保存在区块链分布式系统中（原始各级链接xxx-HASH加密标识）；如果核验a与b不相等，发送请求给用户，网页访问失败，请重新访问；

3）客户端正常后，用户可通过客户端提供的链接访问目标网页。在用户点击网页的服务或功能触发按钮后，通过网页端发送触发消息给云后台，云后台接收到消息后：将网页或系统的当前页面网页的XX文件或信息系统的XXX文件，按XXX流程，生成当前HASH，并将该HASH传送到云后台，云后台进行HASH核验：

①核验正常：则向客户发送正常

客户端收到正常指令后，下一步按钮可以点击。

②核验异常：则向客户发送异常

客户端收到异常指令后，提示系统风险，提示检查环境重新下载后，自动关闭客户端。

4）在使用上述双重验证过程中，数据经过预先上链处理。

[0009] 所述的生成防篡改的JS文件具体处理方法如下：

1）选择网页中进行访问的url网址链接；

2）将网页中相关需求的url网址链接写入html静态页面（每个页面中有一个URL链接），然后将静态页面放入js文件中（此操作就是打包js文件）；

3）读取js文件，通过MD5加密算法，对js文件进行HASH加密，形成js文件的HASH加密码；

4）将形成js文件的HASH加密码通过区块链上链技术写入区块链，并保存在区块链分布式系统；

[0010] 所述JS文件防篡改应用处理方法如下：

1）用户预备选择相关网页；

2）用户点击网页触发JS文件xxx；

3）主机后台通过用户点击的相关js文件读取当前js文件；

4）web端将读取的js文件生成HASH码文件；

5）验证端读取原存档HASH文件；

6）验证端将web端读取的js文件生成的HASH码文件与原存档HASH文件两者的js的HASH进行比较；

①一致：页面处理正常信息返回给用户，进行下一步登录操作。

②不一致：页面处理异常信息返回给用户，进行异常处理重新加载页面或者关闭页面。

[0011] 所述JS文件防篡改功能处理方法如下：

1）用户收到网页正常信息；

2）用户点击网页的服务或功能按钮触发；

3）web网页端将触发消息的当前页面网页的XX文件或信息系统的XXX文件，按XXX流程，生成当前HASH；

4）web端通过HTTP协议中request.setAttribute（‘HASH’,HASH）方法将当前生成HASH码存入request域对象；

5）web网页端通过发送触发消息请求到云后台；

6）云后台接收到功能触发消息；

7）云后台通过域对象request.getAttribute(“HASH”)方法获取HASH码；

8）云后台将获取的HASH码与原始区块链分布式系统中的HASH进行核验：

①一致：页面处理正常信息返回给用户，收到正常指令后，下一步按钮可以点击。

②不一致：页面处理异常信息返回给用户，提示系统风险，进行异常处理，提示检查环境重新加载页面或者关闭页面。

[0012] 本发明的双重验证防篡改通过将用户个人数据存储在区块链而不是服务器，在没有个人授权的前提下，任何机构或个人不能获取本人的数据，从根源上解决了现在出现的黑客攻击、防钓鱼信息泄露、网络诈骗行为，保证了数据的安全性；

用户使用过程中采用双重验证防篡改处理，使用户在启动网页和触发功能时不被篡改，看不见原数据，起到了用户在上网过程中的保护作用。

附图说明

[0013] 图1是基于区块链技术的网页双重验证防篡改体系架构；

图2是本发明的生成防篡改的JS文件流程；

图3是本发明的JS文件防篡改应用；

具体实施方式

[0014] 为使本发明的目的、技术方案和优点更加清楚明白，以下结合附图和具体实施例， 对本发明进一步详细说明。

[0015] 图1是基于区块链技术的网页双重验证防篡改体系架构，如图所示。基于区块链技术的网页双重验证防篡改体系主要是用户在通过APP端登陆，访问一级域名，状态判定是否正常，如果状态判定异常，判定结果反馈用户，重新访问；访问一级域名，如果判定状态正常，判定结果反馈用户，可以进入下一步操作，去登入页面。用户在访问一级入口，登陆页面，输入账号密码后点击登录按钮，区块链接收登录触发消息并核验一级网页二级网页，判定状态，如果判定状态异常，二级页面提示检测时间并显示异常；如果判定状态正常，二级页面提示检测时间并显示正常并在二级页面上端提示双重认证标志，进入输入信息点击下一步，触发传递消息至区块链，区块链接收登陆消息核验二级页面三级页面，判定状态，如果判定状态异常，三级页面提示检测时间并显示异常；如果判定状态正常，三级页面提示检测时间并显示正常并在三级页面上端提示双重认证标志，进入下一步业务操作。

[0016] 图2是本发明的生成防篡改的JS文件流程，如图所示。本发明的生成防篡改的JS文件流程主要是预先将网页链接打包成js文件，读取js文件，通过MD5算法对js文件进行HASH加密，并生成HASH码js文件，将此js文件写入区块链：

1）选择网页中进行访问的url网址链接；

2）将网页中相关需求的url网址链接写入html静态页面（每个页面中有一个URL链接），然后将静态页面放入js文件中（此操作就是打包js文件）；

3）读取js文件，通过MD5加密算法，对js文件进行HASH加密，形成js文件的HASH加密码；

4）将形成js文件的HASH加密码通过区块链上链技术写入区块链，并保存在区块链分布式系统；

[0017] 图3是本发明的JS文件防篡改应用，如图所示。本发明的JS文件防篡改应用主要是用户通过点击网页触发js文件xxx，后台读取当前js文件，并生成HASH码，服务器读取原存档HASH文件，并将两个JS的HASH进行比较，判定状态，如果状态不一致，页面异常处理，并将异常信息发送给用户；如果状态一致，进入页面处理正常，并将正常信息传递用户，进入下一步操作。

[0018]以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步的详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明， 凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

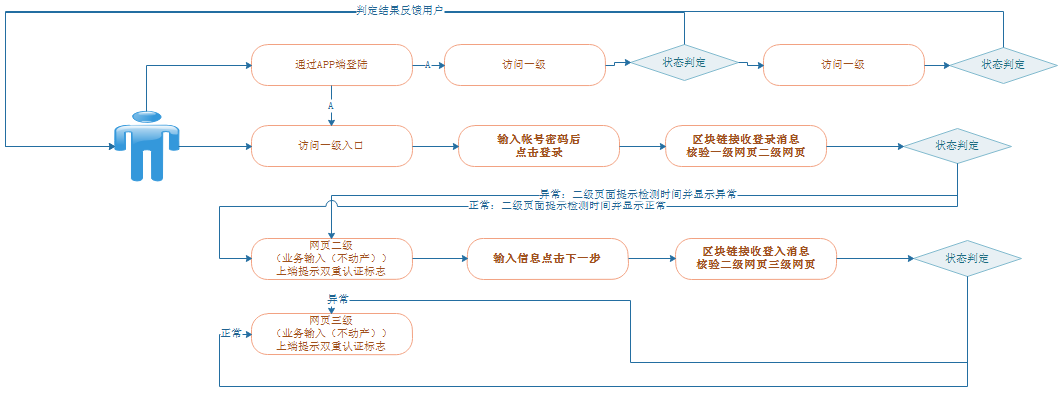


图1

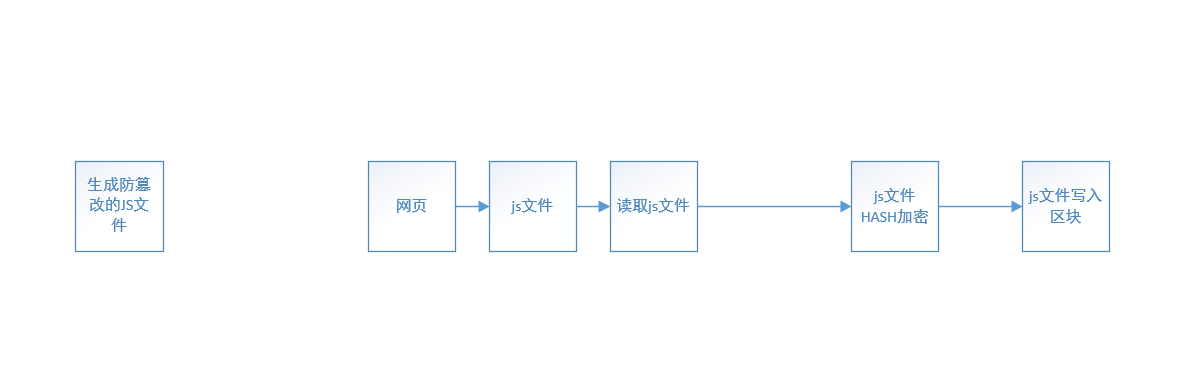
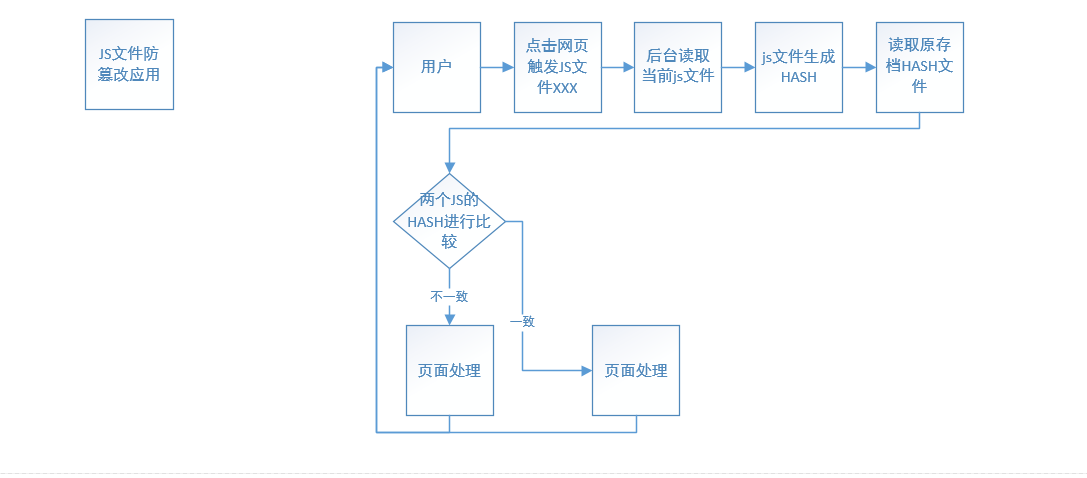


图2

图3