



(21) 申请号 202210635675.8

(22) 申请日 2022.06.07

(65) 同一申请的已公布的文献号

申请公布号 CN 115118460 A

(43) 申请公布日 2022.09.27

(73) 专利权人 上海旋杰智能科技有限公司

地址 201700 上海市青浦区双联路158号2
层

(72) 发明人 余利华

(74) 专利代理机构 北京鼎云升知识产权代理事

务所(普通合伙) 11495

专利代理师 安静

(51) Int. Cl.

H04L 9/40 (2022.01)

H04L 43/0894 (2022.01)

(56) 对比文件

CN 104811450 A, 2015.07.29

CN 113553627 A, 2021.10.26

审查员 龚力

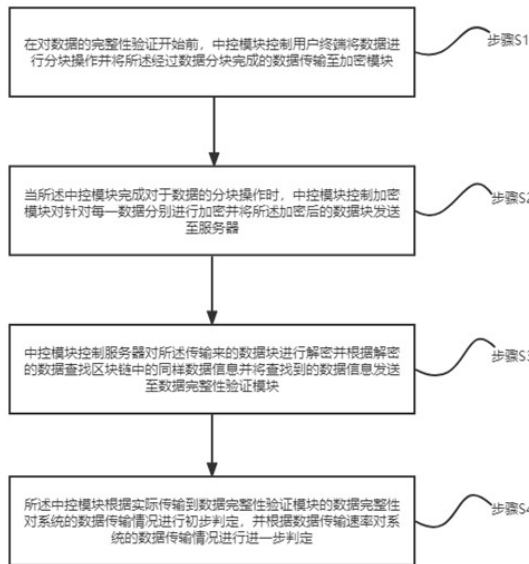
权利要求书3页 说明书8页 附图1页

(54) 发明名称

基于区块链的数据完整性验证方法及系统

(57) 摘要

本发明涉及技术领域,尤其涉及一种基于区块链的数据完整性验证方法与系统。包括:步骤S1,在对数据的完整性验证开始前,中控模块控制用户终端将数据进行分块操作并将所述经过数据分块完成的数据传输加密模块;步骤S2,对数据块进行加密并发送至服务器;步骤S3,中控模块控制服务器将数据信息发送至数据完整性验证模块,步骤S4,中控模块根据实际传输到数据完整性验证模块的数据完整性对系统的传输情况进行初步的判定,并根据数据传输速率检测装置检测到的数据传输速率对系统的数据传输情况进行进一步判定,系统包括:用户终端、加密模块、服务器以及数据完整性验证模块,本发明实现了对于数据完整性验证的准确度和验证效率的提高。



1. 基于区块链的数据完整性验证方法,其特征在于,包括:

步骤S1,在对数据的完整性验证开始前,中控模块控制用户终端对数据进行分块操作并将经过数据分块完成的各数据块传输至加密模块;

步骤S2,当所述加密模块完成对各所述数据块的接收时,中控模块控制加密模块分别针对每一数据块进行加密,并将所述加密后的数据块发送至服务器;

步骤S3,当所述服务器接收到所述加密模块传输的数据块时,中控模块控制服务器对各数据块进行解密操作并根据解密的数据查找区块链中是否存在与用户终端发送的数据信息同样的数据信息、将该数据信息发送至数据完整性验证模块并在将数据经用户终端传输至数据完整性验证模块的过程中检测数据的传输速率;

步骤S4,当中控模块判定对于数据信息的上传时间达到预定传输时间时,中控模块根据实际传输到数据完整性验证模块的数据的完整性对系统的传输情况进行初步判定,并根据数据传输速率检测装置检测到的数据传输速率对系统的数据传输情况进行进一步判定,当中控模块完成针对数据传输情况的判定时根据实际数据完整度与预设数据完整度的差值对延迟传输检测的时长进行调节,在延迟时间后,中控模块控制数据完整性验证模块对数据的完整性进行二次检测并对数据的传输情况进行进一步判定。

2. 根据权利要求1所述的基于区块链的数据完整性验证方法,其特征在于,在所述步骤S4中,当所述数据完整性验证模块接收到用户终端传输来的数据,所述中控模块根据数据完整性验证模块接收到的数据的实际完整度S对系统的数据传输情况进行判定,中控模块设有预设第一预设完整度S1、第二预设完整度S2和第三预设完整度S3,其中, $S1 < S2 < S3$,

若 $S \leq S1$,所述中控模块初步判定系统遭遇拦截并对拦截数据的设备进行反向追踪;

若 $S1 < S \leq S2$,所述中控模块初步判定数据传输不良并控制所述数据传输速率检测装置检测数据传输速率;

若 $S2 < S \leq S3$,所述中控模块初步判定数据传输未完成且需进行延迟检测,中控模块计算实际完整度与预设完整度的差值 ΔS 并根据 ΔS 确定延迟检测的时长;

若 $S > S3$,所述中控模块判定数据完整度合格且数据传输正常。

3. 根据权利要求2所述的基于区块链的数据完整性验证方法,其特征在于,所述中控模块在判定 $S \leq S1$ 时根据周期内数据传输速率是否产生突变对系统遭到的拦截的地址进行确定,中控模块设有预设第一数据传输速率突变值P1和预设第二数据传输速率突变值P2,其中 $P1 < P2$,

若 $P \leq P1$,所述中控模块判定实际数据传输速率突变值在允许范围内并不对该传输速率突变值对应的地址进行确定;

若 $P1 < P \leq P2$,所述中控模块判定实际数据传输速率突变值超出允许范围并计算实际数据传输速率突变值与预设第一数据传输速率突变值的差值 ΔP 并根据 ΔP 对是否存在拦截进行进一步确定,设定 $\Delta P = P - P1$;

若 $P > P2$,所述中控模块判定实际数据传输速率突变值超出允许范围、将该突变值对应的地址确定为系统遭到拦截的地址并将该地址发送至服务器进行存储。

4. 根据权利要求3所述的基于区块链的数据完整性验证方法,其特征在于,所述中控模块在判定 $P1 < P \leq P2$ 时根据实际数据传输速率突变值与预设数据传输速率突变值的差值 ΔP 对是否存在拦截进行进一步判定,中控模块设有预设第一数据传输速率突变值差值 $\Delta P1$

和预设第二数据传输速率突变差值 ΔP_2 ,其中 $\Delta P_1 < \Delta P_2$,

若 $\Delta P \leq \Delta P_1$,所述中控模块判定实际数据传输速率突变值与预设数据传输速率突变值的差值在允许范围内并判定不对该传输速率突变值对应的地址进行确定;

若 $\Delta P_1 < \Delta P \leq \Delta P_2$,所述中控模块判定实际数据传输速率突变值与预设数据传输速率突变值的差值在允许范围内并将该传输速率突变值对应的地址发送至服务器作为储备地址;

若 $\Delta P > \Delta P_2$,所述中控模块判定实际实际数据传输速率突变值与预设数据传输速率突变值的差值超出允许范围并将该突变值对应的地址确定为系统遭到拦截的地址并将该地址发送至服务器进行存储。

5. 根据权利要求4所述的基于区块链的数据完整性验证方法,其特征在于,所述中控模块在判定 $S_1 < S \leq S_2$ 时根据数据传输速率检测装置检测到的实际数据传输速率对数据传输情况进行进一步判定,中控模块设有预设第一传输速率 Q_1 和预设第二传输速率 Q_2 ,其中 $Q_1 < Q_2$,

若 $Q \leq Q_1$,所述中控模块判定网络环境拥堵并发出传输不良警报;

若 $Q_1 < Q \leq Q_2$,所述中控模块判定数据传输不良、检测服务器负载并根据负载判定是否推迟服务器负载中同时进行的任务;

若 $Q > Q_2$,所述中控模块判定数据传输速率合格且数据遭到拦截。

6. 根据权利要求5所述的基于区块链的数据完整性验证方法,其特征在于,所述中控模块在判定 $Q_1 < Q \leq Q_2$ 时控制负载检测装置检测服务器同时传输的负载量以判定是否推迟同时进行的传输任务,中控模块设有预设第一传输负载量 D_1 、预设第二传输负载量 D_2 ,其中 $D_1 < D_2$,

若 $D \leq D_1$,所述中控模块判定实际传输负载量低于允许范围并增加传输的数据块的数量;

若 $D_1 < D \leq D_2$,所述中控模块判定实际传输负载量在允许范围内并不对同时传输的数据传输任务进行推迟;

若 $D > D_2$,所述中控模块判定实际传输负载量超出允许范围并对同时传输的数据传输任务进行推迟操作。

7. 根据权利要求6所述的基于区块链的数据完整性验证方法,其特征在于,所述中控模块在判定 $S_2 < S \leq S_3$ 时根据所述数据完整性验证模块接收到的数据的实际完整度与预设完整度的差值 ΔS 对延迟时长进行确定,设定 $\Delta S = S_3 - S$,中控模块设有预设第一预设完整度差值 ΔS_1 、第二预设完整度差值 ΔS_2 ,第一预设延迟时长 t_1 和第二预设延迟时长 t_2 , $\Delta S_1 < \Delta S_2$, $t_1 < t_2$,

若 $0 < \Delta S \leq \Delta S_1$,所述中控模块判定验证模块对数据的接收延迟 t_1 时长检测;

若 $\Delta S_1 < \Delta S \leq \Delta S_2$,所述中控模块判定验证模块对数据的接收延迟 t_2 时长后再进行检测;

若 $\Delta S > \Delta S_2$,所述中控模块判定数据传输不良并对数据传输速率进行二次检测。

8. 根据权利要求7所述的基于区块链的数据完整性验证方法,其特征在于,当所述中控模块延迟 t_1 后,中控模块控制数据完整度检测程序重新检测数据完整度 S' ,

若 $S' > S_3$,所述中控模块判定数据未受到拦截并不对数据进行反向追踪;

若 $S' \leq S3$,所述中控模块判定数据数据受到拦截并进行反向追踪。

9.根据权利要求8所述的基于区块链的数据完整性验证方法,其特征在于,当所述中控模块延迟 $t2$ 后,中控模块控制数据完整度检测程序重新检测数据完整度 S' 并根据 S' 与 $S3$ 的差值对数据是否受到拦截进行进一步判定,

若 $S' > S3$,所述中控模块判定数据存在传输不良的情况并发出数据传输问题警报;

若 $S' \leq S3$,计算 $\Delta S'$,设定 $\Delta S' = S3 - S'$;

若 $0 < \Delta S \leq \Delta S1$,所述中控模块判定再延迟 $t1$ 时长并检测数据传输速率 Q 以判定是否存在数据传输不良的情况;

若 $\Delta S1 < \Delta S \leq \Delta S2$,所述中控模块判定数据受到拦截并发出数据被拦截警报;

若 $\Delta S > \Delta S2$,所述中控模块判定数据传输受阻并发出数据传输问题警报。

10.一种使用权利要求1-9任一权利要求所述方法的基于区块链的数据完整性验证方法的系统,其特征在于,包括:

用户终端,用于将数据进行分块操作和数据加密操作并将经数据分块和加密后的数据发送至服务器;

加密模块,其与所述用户终端相连,用于对用户终端传输来的数据块进行加密操作;

服务器,其与所述加密模块相连,用于接收所述加密模块传输来的数据加密信息并将所述数据加密信息解密,在完成信息的解密后根据解密的数据查找区块链中是否存在与用户终端发送的数据信息同样的数据信息并将该数据信息发送至数据完整性验证模块;

数据完整性验证模块,其与所述服务器相连,用于根据服务器接收到数据信息对经用户终端传输来的数据的完整性进行验证。

基于区块链的数据完整性验证方法及系统

技术领域

[0001] 本发明涉及区块链技术领域,尤其涉及一种基于区块链的数据完整性验证方法及系统。

背景技术

[0002] 区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式结构,并以密码学方式保证的不可篡改和不可伪造的分布式账本。区块链的节点信息由所有区块链的参与者共同维护,因此区块链上的所有信息都是公开透明的,且信息一经发布就永久保留,无法篡改。区块链所拥有的公开验证、不可篡改的特性使其可以作为可信的第三方解决云计算环境下用户的顾虑,一切结果都可以发布到区块链中,由区块链的所有用户进行认证和维护。因此将区块链结合到云计算领域,利用区块链的优势解决云计算环境的弊端,可以更加有效地为用户的数据安全性提供保障。

[0003] 中国专利公开号:CN113553627A。公开了一种基于区块链的数据完整性验证方法、系统、设备及介质,该方法包括:接收用户端发送的实时完整性信息,所述实时完整性信息由云存储数据基于预设数据处理规则生成;查找区块链网络中是否存在与所述实时完整性信息一致的原始完整性信息,以获得查找结果。通过将原始数据的完整性信息存储到区块链网络中,并在区块链网络中进行数据完整性验证,从而保证原始数据完整性信息不被篡改和删除,提高数据完整性验证的可靠性。由此可见,所述一种基于区块链的数据完整性验证方法、系统、设备及介质存在以下问题:数据完整性验证的准确度和验证效率较低。

发明内容

[0004] 为此,本发明提供一种基于区块链的数据完整性验证方法及系统,用以克服现有技术中的数据完整性验证的准确度和验证效率较低的问题。

[0005] 为实现上述目的,本发明提供一种基于区块链的数据完整性验证方法,包括:

[0006] 步骤S1,在对数据的完整性验证开始前,中控模块控制用户终端对数据进行分块操作并将经过数据分块完成的各数据块传输至加密模块;步骤S2,当所述加密模块完成对各所述数据块的接收时,中控模块控制加密模块分别针对每一数据块进行加密,并将所述加密后的数据块发送至服务器;步骤S3,当所述服务器接收到所述加密模块传输的数据块时,中控模块控制服务器对各数据块进行解密操作并根据解密的数据查找区块链中是否存在与用户终端发送的数据信息同样的数据信息、将该数据信息发送至数据完整性验证模块并在将数据经用户终端传输至数据完整性验证模块的过程中检测数据的传输速率;步骤S4,当中控模块判定对于数据信息的上传时间达到预定传输时间时,中控模块根据实际传输到数据完整性验证模块的数据的完整性对系统的传输情况进行初步判定,并根据数据传输速率检测装置检测到的数据传输速率对系统的数据传输情况进行进一步判定,当中控模块完成针对数据传输情况的判定时根据实际数据完整度与预设数完整度的差值对延迟传输检测的时长进行调节,在延迟时间后,中控模块控制验证模块对数据的完整性进行二次

检测并对数据的传输情况进行进一步判定。

[0007] 进一步地,在所述步骤S4中,当所述数据完整性验证模块接收到用户终端传输来的数据,所述中控模块根据数据完整性验证模块接收到的数据的实际完整度S对系统的数据传输情况进行判定,中控模块设有预设第一预设完整度S1、第二预设完整度S2和第三预设完整度S3,其中, $S1 < S2 < S3$,

[0008] 若 $S \leq S1$,所述中控模块初步判定系统遭遇拦截并对拦截数据的设备进行反向追踪;

[0009] 若 $S1 < S \leq S2$,所述中控模块初步判定数据传输不良并控制所述数据传输速率检测装置检测数据传输速率;

[0010] 若 $S2 < S \leq S3$,所述中控模块初步判定数据传输未完成且需进行延迟检测,中控模块计算实际完整度与预设完整度的差值 ΔS 并根据 ΔS 确定延迟检测的时长;

[0011] 若 $S > S3$,所述中控模块判定数据完整度合格且数据传输正常。

[0012] 进一步地,所述中控模块在判定 $S \leq S1$ 时根据周期内数据传输速率是否产生突变对系统遭到的拦截的地址进行确定,中控模块设有预设第一数据传输速率突变值P1和预设第二数据传输速率突变值P2,其中 $P1 < P2$,

[0013] 若 $P \leq P1$,所述中控模块判定实际数据传输速率突变值在允许范围内并不对该传输速率突变值对应的地址进行确定;

[0014] 若 $P1 < P \leq P2$,所述中控模块判定实际数据传输速率突变值超出允许范围并计算实际数据传输速率突变值与预设第一数据传输速率突变值的差值 ΔP 并根据 ΔP 对是否存在拦截进行进一步确定,设定 $\Delta P = P - P1$;

[0015] 若 $P > P2$,所述中控模块判定实际数据传输速率突变值超出允许范围、将该突变值对应的地址确定为系统遭到拦截的地址并将该地址发送至服务器进行存储。

[0016] 进一步地,所述中控模块在判定 $P1 < P \leq P2$ 时根据实际数据传输速率突变值与预设数据传输速率突变值的差值 ΔP 对是否存在拦截进行进一步判定,中控模块设有预设第一数据传输速率突变值差值 $\Delta P1$ 和预设第二数据传输速率突变差值 $\Delta P2$,其中 $\Delta P1 < \Delta P2$,

[0017] 若 $\Delta P \leq \Delta P1$,所述中控模块判定实际数据传输速率突变值与预设数据传输速率突变值的差值在允许范围内并判定不对该传输速率突变值对应的地址进行确定;

[0018] 若 $\Delta P1 < \Delta P \leq \Delta P2$,所述中控模块判定实际数据传输速率突变值与预设数据传输速率突变值的差值在允许范围内并将该传输速率突变值对应的地址发送至服务器作为储备地址;

[0019] 若 $\Delta P > \Delta P2$,所述中控模块判定实际实际数据传输速率突变值与预设数据传输速率突变值的差值超出允许范围并将该突变值对应的地址确定为系统遭到拦截的地址并将该地址发送至服务器进行存储。

[0020] 进一步地,所述中控模块在判定 $S1 < S \leq S2$ 时根据实际传输速率检测装置检测到的实际数据传输速率对数据传输情况进行进一步判定,中控模块设有预设第一传输速率Q1和预设第二传输速率Q2,其中 $Q1 < Q2$,

[0021] 若 $Q \leq Q1$,所述中控模块判定网络环境拥堵并发出传输不良警报;

[0022] 若 $Q1 < Q \leq Q2$,所述中控模块判定数据传输不良、检测服务器负载并根据负载判定

是否推迟服务器负载中同时进行的任务；

[0023] 若 $Q > Q_2$,所述中控模块判定数据传输速率合格且数据遭到拦截。

[0024] 进一步地,所述中控模块在判定 $Q_1 < Q \leq Q_2$ 时控制所述负载检测装置检测到服务器同时传输的负载量是否推迟同时进行的数据传输任务进行判定,中控模块设有预设第一传输负载量 D_1 、预设第二传输负载量 D_2 ,其中 $D_1 < D_2$,

[0025] 若 $D \leq D_1$,所述中控模块判定实际传输负载量低于允许范围并增加传输的数据块的数量；

[0026] 若 $D_1 < D \leq D_2$,所述中控模块判定实际传输负载量在允许范围内并不对同时传输的数据传输任务进行推迟；

[0027] 若 $D > D_2$,所述中控模块判定实际传输负载量超出允许范围并对同时传输的数据传输任务进行推迟操作。

[0028] 进一步地,所述中控模块在判定 $S_2 < S \leq S_3$ 时根据所述数据完整性验证模块接收到的数据的实际完整度与预设完整度的差值 ΔS 对延迟时长进行确定,设定 $\Delta S = S_3 - S$,中控模块设有预设第一预设完整度差值 ΔS_1 、第二预设完整度差值 ΔS_2 ,第一预设延迟时长 t_1 和第二预设延迟时长 t_2 , $\Delta S_1 < \Delta S_2$, $t_1 < t_2$,

[0029] 若 $0 < \Delta S \leq \Delta S_1$,所述中控模块判定验证模块对数据的接收延迟 t_1 时长检测；

[0030] 若 $\Delta S_1 < \Delta S \leq \Delta S_2$,所述中控模块判定验证模块对数据的接收延迟 t_2 时长后再进行检测；

[0031] 若 $\Delta S > \Delta S_2$,所述中控模块判定数据传输不良并对数据传输速率进行二次检测。

[0032] 进一步地,当所述中控模块延迟 t_1 后,中控模块控制数据完整度检测程序重新检测数据完整度 S' ,

[0033] 若 $S' > S_3$,所述中控模块判定数据未受到拦截并不对数据进行反向追踪；

[0034] 若 $S' \leq S_3$,所述中控模块判定数据数据受到拦截并进行反向追踪。

[0035] 进一步地,当所述中控模块延迟 t_2 后,中控模块控制数据完整度检测程序重新检测数据完整度 S' 并根据 S' 与 S_3 的差值对数据是否受到拦截进行进一步判定,

[0036] 若 $S' > S_3$,所述中控模块判定数据存在传输不良的情况并发出数据传输问题警报；

[0037] 若 $S' \leq S_3$,计算 $\Delta S'$,设定 $\Delta S' = S_3 - S'$ ；

[0038] 若 $0 < \Delta S \leq \Delta S_1$,所述中控模块判定再延迟 t_1 时长并检测数据传输速率 Q 以判定是否存在数据传输不良的情况；

[0039] 若 $\Delta S_1 < \Delta S \leq \Delta S_2$,所述中控模块判定数据受到拦截并发出数据被拦截警报；

[0040] 若 $\Delta S > \Delta S_2$,所述中控模块判定数据传输受阻并发出数据传输问题警报。

[0041] 一种基于区块链的数据完整性验证系统,包括：

[0042] 用户终端,用于将数据进行分块操作和数据加密操作并将经数据分块和加密后的数据发送至服务器；

[0043] 加密模块,其与所述用户终端相连,用于对用户终端传输来的数据块进行加密操作；

[0044] 服务器,其与所述加密模块相连,用于接收所述加密模块传输来的数据加密信息并将所述数据加密信息解密,在完成信息的解密后根据解密的数据查找区块链中是否存在

与用户终端发送的数据信息同样的数据信息并将该数据信息发送至数据完整性验证模块；
[0045] 数据完整性验证模块，其与所述服务器相连，用于根据服务器接收到数据信息对经用户终端传输来的数据的完整性进行验证。

[0046] 与现有技术相比，本发明的有益效果在于，本发明通过设置预设数据完整度、预设数据传输速率突变值以及预设完整度差值，可以根据实际数据完整度对系统的传输情况进行初步的判定，并根据数据传输速率检测装置检测到的数据传输速率对系统的数据传输情况进行进一步判定，可以根据实际数据完整度与预设数据完整度的差值对延迟传输检测的时长进行调节，提高了对于数据完整性验证的准确性、数据完整性验证的数据传输速率的精准监测以及数据完整性验证的效率，实现了对于数据完整性验证的准确度和验证效率的提高。

[0047] 进一步地，本发明所述方法通过设置预设第一预设完整度、第二预设完整度和第三预设完整度，可以根据实际完整度对系统的数据传输情况进行判定，提高了数据完整性验证的精准判别，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0048] 进一步地，本发明所述方法通过设置预设第一数据传输速率突变值和预设第二数据传输速率突变值，可以根据周期内数据传输速率是否产生突变对系统遭到的拦截的地址进行确定，提高了对于数据传输过程的监管能力，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0049] 进一步地，本发明所述方法通过设置预设第一数据传输速率突变值差值和预设第二数据传输速率突变差值，可以根据实际数据传输速率突变值与预设数据传输速率突变值的差值 ΔP 对是否存在拦截进行进一步判定，提高了数据传输过程是否存在拦截情况的精准识别能力，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0050] 进一步地，本发明所述方法通过设置预设第一传输速率和预设第二传输速率，可以根据实际传输速率检测装置检测到的实际数据传输速率对数据传输情况进行进一步判定，提高了对于数据传输的精准判定能力，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0051] 进一步地，本发明所述方法通过设置预设第一传输负载量和预设第二传输负载量，可以根据检测到的同时传输的负载量是否推迟同时进行的数据传输任务进行判定，提高了对于数据传输任务的精准调节能力，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0052] 进一步地，本发明所述方法通过设置预设第一预设完整度差值、第二预设完整度差值、第一预设延迟时长 t_1 以及第二预设延迟时长，可以根据实际完整度与预设完整度的差值对延迟时长进行确定，实现了对于延迟时长的精准确定，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0053] 进一步地，本发明所述方法通过在延迟时长后对于数据完整度进行重新检测，可以对数据完整度进行进一步判定，提高了对于影响数据完整性的传输过程的深层确认能力，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0054] 进一步地，本发明所述方法通过控制数据完整度检测程序重新检测数据完整度并对数据是否受到拦截进行进一步判定，实现了数据完整性涉及的数据传输过程情况的进一步精准确定，进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0055] 本发明所述系统通过设置用户终端、服务器以及数据完整性验证模块,可以对数据完整性进行验证,提高了数据完整性验证的准确度,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

附图说明

[0056] 图1为本发明实施例基于区块链的数据完整性验证方法的流程图;

[0057] 图2为本发明实施例基于区块链的数据完整性验证系统的系统框图。

具体实施方式

[0058] 为了使本发明的目的和优点更加清楚明白,下面结合实施例对本发明作进一步描述;应当理解,此处所描述的具体实施例仅仅用于解释本发明,并不用于限定本发明。

[0059] 下面参照附图来描述本发明的优选实施方式。本领域技术人员应当理解的是,这些实施方式仅仅用于解释本发明的技术原理,并非在限制本发明的保护范围。

[0060] 请参阅图1所示,一种基于区块链的数据完整性验证方法,包括:

[0061] 步骤S1,在对数据的完整性验证开始前,中控模块控制用户终端对数据进行分块操作并将经过数据分块完成的各数据块传输至加密模块;

[0062] 步骤S2,当所述加密模块完成对各所述数据块的接收时,中控模块控制加密模块分别针对每一数据块进行加密,并将所述加密后的数据块发送至服务器;

[0063] 步骤S3,当所述服务器接收到所述加密模块传输的数据块时,中控模块控制服务器对各数据块进行解密操作并根据解密的数据查找区块链中是否存在与用户终端发送的数据信息同样的数据信息、将该数据信息发送至数据完整性验证模块并在将数据经用户终端传输至数据完整性验证模块的过程中检测数据的传输速率;

[0064] 步骤S4,当中控模块判定对于数据信息的上传时间达到预定传输时间时,中控模块根据实际传输到数据完整性验证模块的数据的完整性对系统的传输情况进行初步判定,并根据数据传输速率检测装置检测到的数据传输速率对系统的数据传输情况进行进一步判定,当中控模块完成针对数据传输情况的判定时根据实际数据完整度与预设数完整度的差值对延迟传输检测的时长进行调节,在延迟时间后,中控模块控制验证模块对数据的完整性进行二次检测并对数据的传输情况进行进一步判定。

[0065] 本发明通过设置预设数据完整度、预设数据传输速率突变值以及预设完整度差值,可以根据实际数据完整度对系统的传输情况进行初步的判定,并根据数据传输速率检测装置检测到的数据传输速率对系统的数据传输情况进行进一步判定,可以根据实际数据完整度与预设数完整度的差值对延迟传输检测的时长进行调节,提高了对于数据完整性验证的准确性、数据完整性验证的数据传输速率的精准监测以及数据完整性验证的效率,实现了对于数据完整性验证的准确度和验证效率的提高。

[0066] 具体而言,在所述步骤S4中,当所述数据完整性验证模块接收到用户终端传输来的数据,所述中控模块根据数据完整性验证模块接收到的数据的实际完整度S对系统的数据传输情况进行判定,中控模块设有预设第一预设完整度S1、第二预设完整度S2和第三预设完整度S3,其中, $S1 < S2 < S3$,

[0067] 若 $S \leq S1$,所述中控模块初步判定系统遭遇拦截并对拦截数据的设备进行反向追

踪;

[0068] 若 $S_1 < S \leq S_2$,所述中控模块初步判定数据传输不良并控制所述数据传输速率检测装置检测数据传输速率;

[0069] 若 $S_2 < S \leq S_3$,所述中控模块初步判定数据传输未完成且需进行延迟检测,中控模块计算实际完整度与预设完整度的差值 ΔS 并根据 ΔS 确定延迟检测的时长;

[0070] 若 $S > S_3$,所述中控模块判定数据完整度合格且数据传输正常。

[0071] 本发明所述方法通过设置预设第一预设完整度、第二预设完整度和第三预设完整度,可以根据实际完整度对系统的数据传输情况进行判定,提高了数据完整性验证的精准判别,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0072] 具体而言,所述中控模块在判定 $S \leq S_1$ 时根据周期内数据传输速率是否产生突变对系统遭到的拦截的地址进行确定,中控模块设有预设第一数据传输速率突变值 P_1 和预设第二数据传输速率突变值 P_2 ,其中 $P_1 < P_2$,

[0073] 若 $P \leq P_1$,所述中控模块判定实际数据传输速率突变值在允许范围内并不对该传输速率突变值对应的地址进行确定;

[0074] 若 $P_1 < P \leq P_2$,所述中控模块判定实际数据传输速率突变值超出允许范围并计算实际数据传输速率突变值与预设第一数据传输速率突变值的差值 ΔP 并根据 ΔP 对是否存在拦截进行进一步确定,设定 $\Delta P = P - P_1$;

[0075] 若 $P > P_2$,所述中控模块判定实际数据传输速率突变值超出允许范围、将该突变值对应的地址确定为系统遭到拦截的地址并将该地址发送至服务器进行存储。

[0076] 本发明所述方法通过设置预设第一数据传输速率突变值和预设第二数据传输速率突变值,可以根据周期内数据传输速率是否产生突变对系统遭到的拦截的地址进行确定,提高了对于数据传输过程的监管能力,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0077] 具体而言,所述中控模块在判定 $P_1 < P \leq P_2$ 时根据实际数据传输速率突变值与预设数据传输速率突变值的差值 ΔP 对是否存在拦截进行进一步判定,中控模块设有预设第一数据传输速率突变值差值 ΔP_1 和预设第二数据传输速率突变差值 ΔP_2 ,其中 $\Delta P_1 < \Delta P_2$,

[0078] 若 $\Delta P \leq \Delta P_1$,所述中控模块判定实际数据传输速率突变值与预设数据传输速率突变值的差值在允许范围内并判定不对该传输速率突变值对应的地址进行确定;

[0079] 若 $\Delta P_1 < \Delta P \leq \Delta P_2$,所述中控模块判定实际数据传输速率突变值与预设数据传输速率突变值的差值在允许范围内并将该传输速率突变值对应的地址发送至服务器作为储备地址;

[0080] 若 $\Delta P > \Delta P_2$,所述中控模块判定实际实际数据传输速率突变值与预设数据传输速率突变值的差值超出允许范围并将该突变值对应的地址确定为系统遭到拦截的地址并将该地址发送至服务器进行存储。

[0081] 本发明所述方法通过设置预设第一数据传输速率突变值差值和预设第二数据传输速率突变差值,可以根据实际数据传输速率突变值与预设数据传输速率突变值的差值 ΔP 对是否存在拦截进行进一步判定,提高了数据传输过程是否存在拦截情况的精准识别能力,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0082] 具体而言,所述中控模块在判定 $S_1 < S \leq S_2$ 时根据实际传输速率检测装置检测到的实际数据传输速率对数据传输情况进行进一步判定,中控模块设有预设第一传输速率 Q_1 和预设第二传输速率 Q_2 ,其中 $Q_1 < Q_2$,

[0083] 若 $Q \leq Q_1$,所述中控模块判定网络环境拥堵并发出传输不良警报;

[0084] 若 $Q_1 < Q \leq Q_2$,所述中控模块判定数据传输不良、检测服务器负载并根据负载判定是否推迟服务器负载中同时进行的任务;

[0085] 若 $Q > Q_2$,所述中控模块判定数据传输速率合格且数据遭到拦截。

[0086] 本发明所述方法通过设置预设第一传输速率和预设第二传输速率,可以根据实际传输速率检测装置检测到的实际数据传输速率对数据传输情况进行进一步判定,提高了对于数据传输的精准判定能力,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0087] 具体而言,所述中控模块在判定 $Q_1 < Q \leq Q_2$ 时控制所述负载检测装置检测到服务器同时传输的负载量是否推迟同时进行的数据传输任务进行判定,中控模块设有预设第一传输负载量 D_1 、预设第二传输负载量 D_2 ,其中 $D_1 < D_2$,

[0088] 若 $D \leq D_1$,所述中控模块判定实际传输负载量低于允许范围并增加传输的数据块的数量;

[0089] 若 $D_1 < D \leq D_2$,所述中控模块判定实际传输负载量在允许范围内并不对同时传输的数据传输任务进行推迟;

[0090] 若 $D > D_2$,所述中控模块判定实际传输负载量超出允许范围并对同时传输的数据传输任务进行推迟操作。

[0091] 本发明所述方法通过设置预设第一传输负载量和预设第二传输负载量,可以根据检测到的同时传输的负载量是否推迟同时进行的数据传输任务进行判定,提高了对于数据传输任务的精准调节能力,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0092] 具体而言,所述中控模块在判定 $S_2 < S \leq S_3$ 时根据所述数据完整性验证模块接收到的数据的实际完整度与预设完整度的差值 ΔS 对延迟时长进行确定,设定 $\Delta S = S_3 - S$,中控模块设有预设第一预设完整度差值 ΔS_1 、第二预设完整度差值 ΔS_2 ,第一预设延迟时长 t_1 和第二预设延迟时长 t_2 , $\Delta S_1 < \Delta S_2$, $t_1 < t_2$,

[0093] 若 $0 < \Delta S \leq \Delta S_1$,所述中控模块判定验证模块对数据的接收延迟 t_1 时长检测;

[0094] 若 $\Delta S_1 < \Delta S \leq \Delta S_2$,所述中控模块判定验证模块对数据的接收延迟 t_2 时长后再进行检测;

[0095] 若 $\Delta S > \Delta S_2$,所述中控模块判定数据传输不良并对数据传输速率进行二次检测。

[0096] 本发明所述方法通过设置预设第一预设完整度差值、第二预设完整度差值、第一预设延迟时长 t_1 以及第二预设延迟时长,可以根据实际完整度与预设完整度的差值对延迟时长进行确定,实现了对于延迟时长的精确定,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0097] 具体而言,当所述中控模块延迟 t_1 后,中控模块控制数据完整度检测程序重新检测数据完整度 S' ,

[0098] 若 $S' > S_3$,所述中控模块判定数据未受到拦截并不对数据进行反向追踪;

[0099] 若 $S' \leq S3$,所述中控模块判定数据数据受到拦截并进行反向追踪。

[0100] 本发明所述方法通过在延迟时长后对于数据完整度进行重新检测,可以对数据完整度进行进一步判定,提高了对于影响数据完整性的传输过程的深层确认能力,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0101] 具体而言,当所述中控模块延迟 $t2$ 后,中控模块控制数据完整度检测程序重新检测数据完整度 S' 并根据 S' 与 $S3$ 的差值对数据是否受到拦截进行进一步判定,

[0102] 若 $S' > S3$,所述中控模块判定数据存在传输不良的情况并发出数据传输问题警报;

[0103] 若 $S' \leq S3$,计算 $\Delta S'$,设定 $\Delta S' = S3 - S'$;

[0104] 若 $0 < \Delta S \leq \Delta S1$,所述中控模块判定再延迟 $t1$ 时长并检测数据传输速率 Q 以判定是否存在数据传输不良的情况;

[0105] 若 $\Delta S1 < \Delta S \leq \Delta S2$,所述中控模块判定数据受到拦截并发出数据被拦截警报;

[0106] 若 $\Delta S > \Delta S2$,所述中控模块判定数据传输受阻并发出数据传输问题警报。

[0107] 本发明所述方法通过控制数据完整度检测程序重新检测数据完整度并对数据是否受到拦截进行进一步判定,实现了数据完整性涉及的数据传输过程情况的进一步精准确定,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0108] 请参阅图2所示,一种基于区块链的数据完整性验证系统,包括:

[0109] 用户终端,用于将数据进行分块操作和数据加密操作并将经数据分块和加密后的数据发送至服务器;

[0110] 加密模块,其与所述用户终端相连,用于对用户终端传输来的数据块进行加密操作;

[0111] 服务器,其与所述加密模块相连,用于接收所述加密模块传输来的数据加密信息并将所述数据加密信息解密,在完成信息的解密后根据解密的数据查找区块链中是否存在与用户终端发送的数据信息同样的数据信息并将该数据信息发送至数据完整性验证模块;

[0112] 数据完整性验证模块,其与所述服务器相连,用于根据服务器接收到数据信息对经用户终端传输来的数据的完整性进行验证。

[0113] 本发明所述系统通过设置用户终端、服务器以及数据完整性验证模块,可以对数据完整性进行验证,提高了数据完整性验证的准确度,进一步实现了对于数据完整性验证的准确度和验证效率的提高。

[0114] 至此,已经结合附图所示的优选实施方式描述了本发明的技术方案,但是,本领域技术人员容易理解的是,本发明的保护范围显然不局限于这些具体实施方式。在不偏离本发明的原理的前提下,本领域技术人员可以对相关技术特征做出等同的更改或替换,这些更改或替换之后的技术方案都将落入本发明的保护范围之内。

[0115] 以上所述仅为本发明的优选实施例,并不用于限制本发明;对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

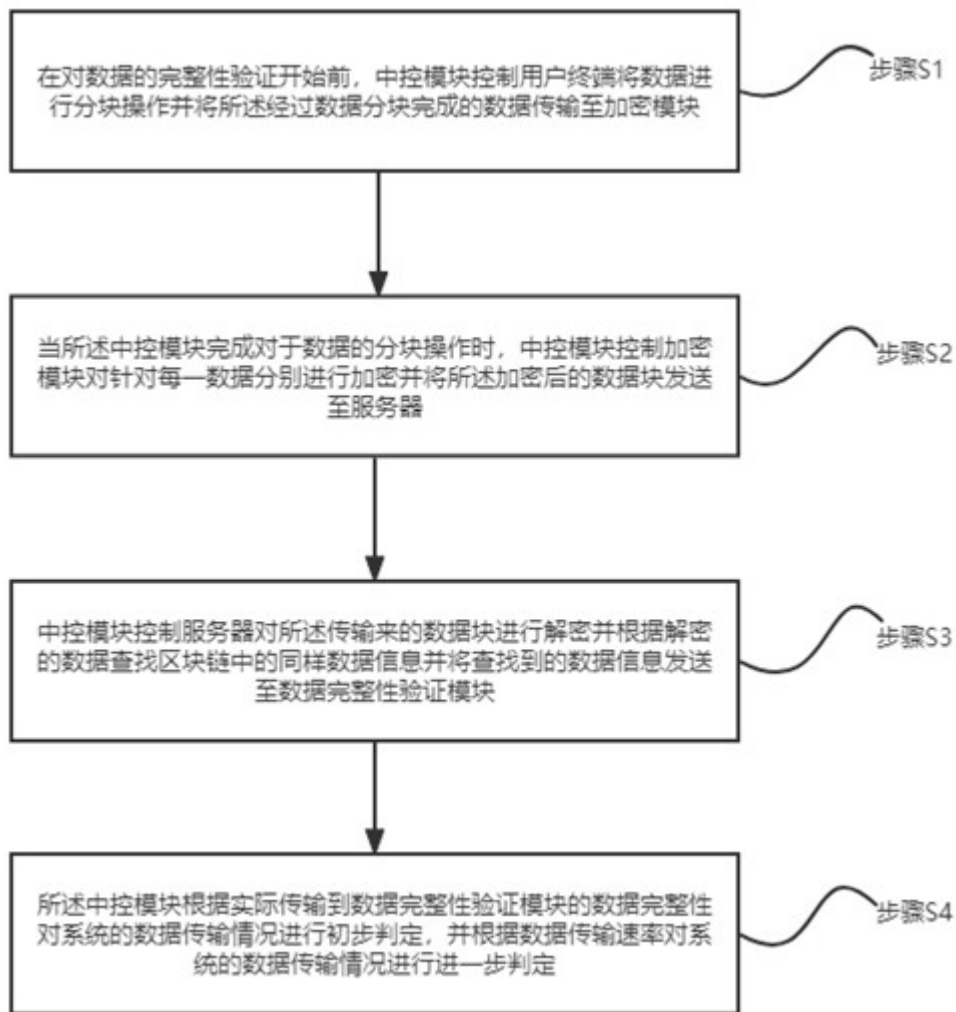


图1

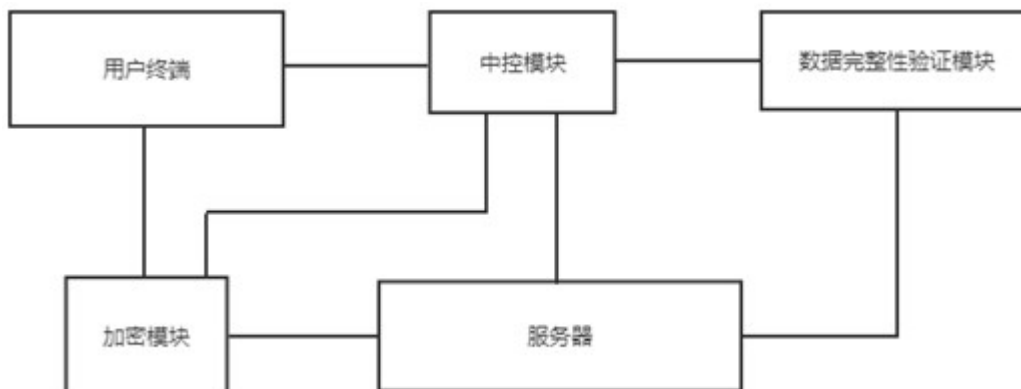


图2