(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114461623 B
(45)授权公告日 2024.08.27

(21)申请号 202210100479.0
(22)申请日 2022.01.27
(65)同一申请的已公布的文献号
申请公布号 CN 114461623 A
(43)申请公布日 2022.05.10
(73)专利权人 东南大学
地址 210000 江苏省南京市玄武区新街口街道四牌楼2号
(72)发明人 吴子晗 王良民 胡轶宁 许昱玮 费越 李春姣 何冉
(74)专利代理机构 南京华恒专利代理事务所(普通合伙) 32335
专利代理师 宋方园
(51)Int.Cl.
G06F 16/215(2019.01)
G06F 16/23(2019.01)
G06F 16/27(2019.01)
G06F 21/62(2013.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)
(56)对比文件
CN 111988290 A,2020.11.24
US 2021042744 A1,2021.02.11
审查员 倪赛华

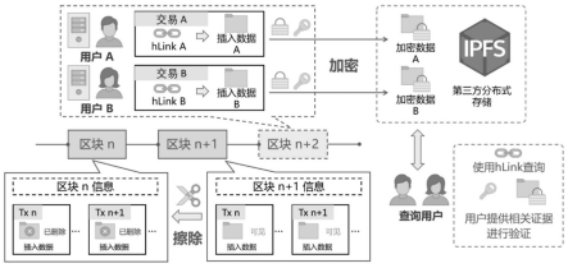
权利要求书3页 说明书7页 附图1页

(54)发明名称

一种许可链上授权的非交易有害数据完全擦除方法

(57)摘要

本发明公开许可链上授权的非交易有害数据完全擦除方法,包括异地多步擦除、擦除后的验证与示证、设置擦除周期可调节和新用户节点初始化,本发明可在授权后完全擦除链上有害数据,而非对相关数据的隐藏处理。所设计的一致性验证算法,能保证擦除操作不影响交易相关数据的完整性、一致性、有效性等永久写入特性,且提供基于密码学的用户示证;所涉及的擦除周期可调整方法,允许许可链系统在不扩大影响的情况下对突发性的非法数据插入进行及时处理。



CN 114461623 B

1.一种许可链上授权的非交易有害数据完全擦除方法,其特征在于:包括用户节点、授权节点、分布式客户端和非交易数据;所述用户节点使用分布式客户端与许可链网络进行交互;所述授权节点对加入许可链网络的分布式客户端进行认证,并对许可链网络中用户节点的擦除操作进行授权;所述分布式客户端保存许可链中的账本信息,并生成或验证区块中的交易;所述非交易数据为分布式客户端生成交易时,用户节点在交易的输入脚本和输出脚本插入的辅助交易执行的补充信息;具体非交易有害数据完全擦除方法包括以下步骤:

步骤S1、异地多步擦除

许可链的用户节点写入非交易数据时加入附加信息,数据上链后,若授权节点间共识判定非交易数据中包含有害数据,则授权分布式客户端执行该数据的本地擦除;

步骤S2、擦除后的验证与示证

许可链的用户节点使用非交易数据中的附加信息验证许可链全账本数据,擦除后插入相应数据的用户可提供基于密码学的示证;

步骤S3、调节设置擦除周期

授权节点设定特定区块段来用于执行即时的触发擦除,或设定全网络节点的周期擦除;

步骤S4、初始化新用户节点

许可链网络中新加入用户节点同步擦除部分与未擦除部分全账本数据。

2.根据权利要求1所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S1中异地多步擦除的具体步骤:

S1.1、新交易写入:用户节点通过分布式客户端对插入数据预处理存入第三方云存储并获得存储凭据,然后将插入数据与存储凭据等附加信息与写入非交易区域;

S1.2、有害数据判定及擦除授权:许可链网络中的用户节点选举出授权节点,若授权节点发现本地账本中存在有害数据,则定位相应有害数据并发起区块区间的擦除的授权;

S1.3、分布式客户端的本地擦除:分布式客户端接收到授权节点的擦除请求后,根据接受到的信息执行授权节点指定区段的数据擦除或执行周期擦除。

3.根据权利要求2所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S1.1中新交易写入的详细过程如下:

(1)、许可链中的用户节点首先随机生成加密密钥$dk \leftarrow \{0,1\}^{\lambda}$,然后使用对称加密写入信息明文$t_D$得到密文$t_C \leftarrow Enc(dk, t_D)$;

(2)、用户节点将加密后的密文t_C存储到第三方分布式云存储,得到数据存储凭证$hLink_{t_C}$;

(3)、为验证擦除后交易数据,用户节点计算擦除后的交易哈希值hash(Tx′)和插入数据明文t_D的哈希值$hash(t_D)$,组合得到非交易数据$t_{D'} = \{hLink_{t_C}, hash(t_D), hash(Tx'), t_D\}$,并将其写入所生成交易。

4.根据权利要求2所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S1.2中有害数据判定及擦除授权的详细过程如下:

(1)、用户节点通过心跳机制选举出授权节点,当许可链网络中不存在授权节点时,许

可链网络用户节点首先切换到候选状态并进行投票,收到大多数投票认可的用户节点则成为新的授权节点,授权节点周期性的发送心跳信息给所有用户节点来维持其主导地位,若用户节点一段时间没有接收到心跳信息,许可链中则因为没有授权节点重新选出新的授权节点,此时所有用户节点均切换到候选状态并进入新的任期,投票选出新的授权节点;

(2)、许可链授权节点检索全账本区块数据$\mathcal{C}_p$,若检测到区块链中存在有害数据或收到涉及用户隐私的敏感数据的擦除请求,则根据数据内容定位区块区间[q_s,q_e],其中q_s和q_e分别表示区块高度s和e的区块,生成擦除授权交易。

5.根据权利要求2所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S1.3中异地分布式客户端进行本地擦除的详细过程如下:

(1)、分布式客户端DApp查询当前许可链数据$\mathcal{C}_p$当前区块高度n,确定需要进行擦除的区块区间[q_s,q_e],得到需要擦除的链上区块集合${}^{[q_s,q_e]}\mathcal{C}_p$;

(2)、分布式客户端DApp对交易数据$Tx_{i,j} \in B_i \in {}^{[q_s,q_e]}\mathcal{C}_p$执行判断$\langle Tx_{i,j};t_{D'}\rangle \mapsto \{true,false\}$,若结果为true,则该数据为非交易数据并选定,若结果为false则忽略该数据内容,其中B_i表示特定区块高度i的区块数据,$T_{x_{i,j}}$表示第i个区块数据中的第j个交易数据;

(3)、分布式客户端$DApp_i$执行非交易数据擦除算法txPrune擦除选定的非交易数据,其中输入为许可链数据$\mathcal{C}_p$和擦除区块区间[q_s,q_e],输出为擦除后的许可链数据$\{{}^{[0,q_{s-1}]}\mathcal{C}_p,{}^{[q_s,q_e]}\mathcal{C}_p',{}^{[q_{e+1},q_n]}\mathcal{C}_p\}$,其中$\mathcal{C}_p'$为执行擦除操作后的$\mathcal{C}_p$数据,擦除后的非交易数据变为:$t_{D'}^{'}=\left\{hLink_{t_C},hash\left(t_D\right),hash(Tx')\right\}$;

其中擦除算法txPrune的方法如下:

(A)、分布式客户端DApp读取需要擦除的许可链数据$\mathcal{C}_p=\left(B_1,B_2,\cdots,B_n\right)$和擦除区块区间[$q_s$,$q_e$],$B_n$为当前区块高度为n的区块,定位得到目标区块数据${}^{[q_s,q_e]}\mathcal{C}_p$;

(B)、分布式客户端DApp提取出$Tx_{i,j}$,对于每一个交易数据$Tx_{i,j} \in B_i \in {}^{[q_s,q_e]}\mathcal{C}_p$,若区块$B_i$未执行擦除操作P:$\langle Tx_{i,j};t_D\rangle$=ture,则分布式客户端DApp擦除$t_{D'}:=\left\{hLink_{t_C},hash\left(t_D\right),hash(Tx'),t_D\right\}$中的$t_D$得到$t_{D'}^{'}=\left\{hLink_{t_C},hash\left(t_D\right),hash(Tx')\right\}$;

(C)、分布式客户端DApp返回擦除后的许可链数据$\{{}^{[0,q_{s-1}]}\mathcal{C},{}^{[q_s,q_e]}\mathcal{C}_p',{}^{[q_{e+1},q_n]}\mathcal{C}_p\}$。

6.根据权利要求1所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S2的详细过程为:

S2.1、分布式客户端DApp读取未执行区块擦除操作的许可链区块数据$\{{}^{[0,q_{s-1}]}\mathcal{C}_p,{}^{[q_{e+1},q_n]}\mathcal{C}_p\}$,读取其中区块高度为i的区块数据$B_i \in \{{}^{[0,q_{s-1}]}\mathcal{C}_p,{}^{[q_{e+1},q_n]}\mathcal{C}_p\}$,首先检查区块$B_i$中所保存的前一区块$B_{i-1}$的哈希值PrevBlockHash是否正确,然后检查区块生成数据是否符合许可链网络设置,最后计算区块中所打包的交易$T_{x_{i,j}}$的MerkleRoot值,对于每个交易$T_{x_{i,j}}$,检查其输出脚本output是否与输入脚本input的值是否对应,并检查交易锁定时间

lockTime的有效性,若检验均通过,则未擦除部分区块链数据有效;

S2.2、分布式客户端DApp读取已经执行区块链擦除的许可链区块数据$^{[q_s,q_e]}\mathcal{C}_p'$,读取其中区块高度为i的区块数据$B_i \in^{[q_s,q_e]} \mathcal{C}_p'$,计算擦除后的交易哈希值f(Tx$_i$,*)=g(Tx$_i$,1)·g(Tx$_i$,2)·…g(Tx$_i$,u),其中u为区块B$_i$中保存的交易个数,其中擦除部分交易使用插入数据中的hash(Tx′)校验,若计算结果f(Tx$_i$,*)能验证许可链擦除部分$^{[q_s,q_e]}\mathcal{C}_p'$的完整性和一致性,则验证通过,该部分区块内容有效,否则擦除部分未通过验证,擦除操作无效;

S2.3、擦除后插入相应数据的用户可使用第三方分布式云存储中的加密副本结合区块交易中的数据存储凭证进行示证,需要对已擦除的链上擦除数据进行示证的用户提供相应数据的加密密钥dk,示证方通过擦除部分交易的$t_{D'}^{'}=\left\{hLink_{t_C},hash(t_D),hash(Tx')\right\}$得到$hLink_{t_C}$和hash(t$_D$);

S2.4、示证方通过下载第三方分布式存储中的加密数据t$_C$并使用dk解密得到t$_D$,计算hash(t'$_D$),若hash(t'$_D$)=hash(t$_D$),则被擦除的数据得到验证。

7.根据权利要求1所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S3的详细过程如下:

S3.1、许可链中的授权节点基于共识确认擦除操作,生成擦除授权交易,其中交易转账金额为0,擦除相关信息设置为{p,q$_s$,q$_e$},其中p为擦除周期,编码后设置为转入账户地址,将擦除授权写入账本数据;

S3.2、许可链网络中的分布式客户端DApp接收到新的区块后,若区块中存在由授权节点发起的转账金额为0的交易,则解码转入账户地址,提取出擦除设置{p,q$_s$,q$_e$},然后进行擦除设置判断,开始调整节点的本地擦除设置;

若擦除周期p≠0,则分布式客户端DApp忽略心跳数据包中的其余信息,在本地账本中的区块数据达到指定高度时,周期性执行擦除擦除区间[q$_n$-p,q$_n$]中的区块数据$^{[q_n-p,q_n]}\mathcal{C}_p$,其中q$_n$为当前最新区块;

若擦除周期p=0,则分布式客户端DApp执行即时的擦除,擦除本地区块账本数据中指定区间的区块数据$^{[q_s,q_e]}\mathcal{C}_p$。

8.根据权利要求1所述的许可链上授权的非交易有害数据完全擦除方法,其特征在于:所述步骤S4的详细过程如下:

S4.1、新用户节点加入许可链网络后,接收节点同步信息确认当前任期中的授权节点,并从许可链中的用户节点同步当前网络中的全账本数据;

S4.2、若当前许可链网络中正在执行周期擦除,新用户节点同步到未完成周期擦除的全账本数据后,检索全账本数据$\mathcal{C}_p$,逆序检索擦除周期设置的相关区块中的交易,从其中提取擦除周期{p,q$_s$,q$_e$},重新对最近一个周期执行擦除操作,得到与其他节点一致的全账本数据;

S4.3、若当前许可链网络中正在执行即时擦除,新用户节点同步到未完成擦除的全账本数据后,从接收到的区块中提取擦除设置{p,q$_s$,q$_e$},本地重新执行即时擦除,保证网络中全账本数据的一致。

一种许可链上授权的非交易有害数据完全擦除方法

技术领域

[0001] 本发明涉及区块链监管技术,具体涉及一种许可链上授权的非交易有害数据完全擦除方法。

背景技术

[0002] 区块链可以被用于实现时间戳服务、在安全多方计算中实现公平性和正确性,以及建立智能合约,区块链还能为用户提供发布信息的能力,由于传统区块链不可篡改的特性,这些信息不能被审查或编辑,只要目标区块链网络持续存在,就会永久存在与链上。

[0003] 然而,任意数据的插入已经引起了一些严重的问题。非法数据内容的写入对于执法部门一直是一个巨大的挑战。当前的普遍观点认为,区块链网络中的全节点(存储区块链中的完整账本数据)中的数据内容是不可改变,无法被编辑的。在这一前提下,用户节点可能会无意中存储和传播非法内容,恶意用户可能会利用这一缺陷。此外,政府监管的应用需求可能与目前区块链协议中不可篡改的设定存在冲突。另一个需要关注的问题是用户隐私保护。

[0004] 欧盟的GDPR(通用数据保护条例)表明:每个数据主体都有被遗忘的权利,即有权从数据控制者那里获得关于他或她的个人数据的擦除,且不会存在不当的延迟,作为一种快速发展的应用系统,区块链需要包含实现隐私保护的机制来保障用户主体的安全需求。除了法律和隐私保护之外,不断增长的区块链规模也是值得关注的问题。虽然某些轻节点可以在没有区块链完整数据的情况下正常运行,但是新节点加入时还是需要同步完整数据来进行验证,这使得处理现有全账本数据的需求增大。

[0005] 为了解决有害数据任意插入区块链的问题,现有方案主要集中与事前监管与事后监管两个方面。事前监管生效于数据写入区块链前,主要方案是提高交易费用和内容监管,但是在数据写入阶段加入数据过滤或交易费用计算操作会降低交易速度,且基于机器学习方案的内容监管需要高算力服务器,由于高算力服务器通常集中在少数人手里,这一类中心化节点的加入会破坏区块链的去中心性。事后监管方案需要处理已经上链的数据,需要通过全网络的共识来执行修改或擦除操作,这一行为需要执行多方安全计算,对于规模较大的网络会消耗大量的负载,且耗时较长,而且投票行为可能某种意义上促进了被擦除对象(非法数据等)的扩散,造成更严重的影响。

[0006] 不同于传统区块链,许可链作为一种分布式账本技术,参与到许可链系统中的每个节点都是经过许可的,这降低了数据处理方案的设计难度。现有许可链中针对有害数据的监管仅仅是针对分布式账本中键值的隐藏,没有做到数据的完全清除。

发明内容

[0007] 发明目的:本发明的目的在于解决现有技术中存在的不足,提供一种许可链上授权的非交易有害数据完全擦除方法。

[0008] 技术方案:本发明一种许可链上授权的非交易有害数据完全擦除方法,包括用户

节点、授权节点、分布式客户端和非交易数据;所述用户节点使用分布式客户端与许可链网络进行交互;所述授权节点对加入许可链网络的分布式客户端进行认证,并对许可链网络中用户节点的擦除操作进行授权;所述分布式客户端保存许可链中的账本信息,并生成或验证区块中的交易;所述非交易数据为分布式客户端生成交易时,用户节点在交易的输入脚本和输出脚本插入的辅助交易执行的补充信息;具体非交易有害数据完全擦除方法包括以下步骤:

[0009] 步骤S1、异地多步擦除

[0010] 许可链的用户节点写入非交易数据时加入附加信息,数据上链后,若授权节点间共识判定非交易数据中包含有害数据,则授权分布式客户端执行该数据的本地擦除;

[0011] 步骤S2、擦除后的验证与示证

[0012] 许可链的用户节点使用非交易数据中的附加信息验证许可链全账本数据,擦除后插入相应数据的用户可提供基于密码学的示证;包括区块数据完整性验证、一致性验证、有效性验证和证据提供等;

[0013] 步骤S3、调节设置擦除周期可

[0014] 授权节点设定特定区块段来用于执行即时的触发擦除,或设定全网络节点的周期擦除;

[0015] 步骤S4、初始化新用户节点

[0016] 许可链网络中新加入用户节点同步擦除部分与未擦除部分全账本数据。

[0017] 进一步地,所述步骤S1中异地多步擦除的具体步骤:

[0018] S1.1、新交易写入:用户节点通过分布式客户端对插入数据预处理存入第三方云存储并获得存储凭据,然后将插入数据与存储凭据等附加信息与写入非交易区域;

[0019] S1.2、有害数据判定及擦除授权:许可链网络中的用户节点选举出授权节点,若授权节点发现本地账本中存在有害数据,则定位相应有害数据并发起该区块区间的擦除的授权;

[0020] S1.3、异地分布式客户端的本地擦除:分布式客户端接收到授权节点的擦除请求后,根据接受到的信息执行授权节点指定区段的数据擦除或执行周期擦除。

[0021] 进一步地,所述步骤S1.1中新交易写入的详细过程如下:

[0022] (1)、许可链中的用户节点首先随机生成加密密钥$dk \leftarrow \{0,1\}^{\lambda}$,然后使用对称加密写入信息明文$t_D$得到密文$t_C \leftarrow Enc(dk, t_D)$;

[0023] (2)、用户节点将加密后的密文t_C存储到第三方分布式云存储,得到数据存储凭证$hLink_{t_C}$;

[0024] (3)、为验证擦除后交易数据,用户节点计算擦除后的交易哈希值hash(Tx′)和插入数据明文t_D的哈希值$hash(t_D)$,组合得到非交易数据$t_{D'} = \{hLink_{t_C}, hash(t_D), hash(Tx'), t_D\}$,并将其写入所生成交易。

[0025] 进一步地,所述步骤S1.2中有害数据判定及擦除授权的详细过程如下:

[0026] (1)、用户节点通过心跳机制选举出授权节点,当许可链网络中不存在授权节点时,许可链网络用户节点首先切换到候选状态并进行投票,收到大多数投票认可的用户节点则成为新的授权节点,授权节点周期性的发送心跳信息给所有用户节点来维持其主导地

位,若用户节点一段时间没有接收到心跳信息,许可链中则因为没有授权节点重新选出新的授权节点,此时所有用户节点均切换到候选状态并进入新的任期,投票选出新的授权节点;

[0027] (2)、许可链授权节点检索全账本区块数据$\mathcal{C}_p$,若检测到区块链中存在有害数据或收到涉及用户隐私的敏感数据的擦除请求,则根据数据内容定位区块区间[q_s,q_e],其中q_s和q_e分别表示区块高度s和e的区块,生成擦除授权交易。

[0028] 进一步地,所述步骤S1.3中异地分布式客户端进行本地擦除的详细过程如下:

[0029] (1)、分布式客户端DApp查询当前许可链数据$\mathcal{C}_p$当前区块高度n,确定需要进行擦除的区块区间[q_s,q_e],得到需要擦除的链上区块集合$^{[q_s,q_e]}\mathcal{C}_p$;

[0030] (2)、分布式客户端DApp对交易数据$Tx_{i,j} \in B_i \in^{[q_s,q_e]} \mathcal{C}_p$执行判断$\langle Tx_{i,j};t_{D'}\rangle \mapsto \{true,false\}$,若结果为true,则该部分数据为非交易数据并选定,若结果为false则忽略该部分数据内容,其中B_i表示特定区块高度i的区块数据,$T_{x_{i,j}}$表示第i个区块数据中的第j个交易数据;

[0031] (3)、分布式客户端$DApp_i$执行非交易数据擦除算法txPrune擦除选定的非交易数据,其中输入为许可链数据C_p和擦除区块区间[q_s,q_e],输出为擦除后的许可链数据$\{^{[0,q_{s-1}]}\mathcal{C}_p,^{[q_s,q_e]}\mathcal{C}_p',^{[q_{e+1},q_n]}\mathcal{C}_p\}$,其中$\mathcal{C}_p'$为执行擦除操作后的$\mathcal{C}_p$数据,擦除后的非交易数据变为:$t_{D'}^{'}=\{hLink_{t_C},hash(t_D),hash(Tx')\}$;

[0032] 其中擦除算法txPrune的方法如下:

[0033] (A)、分布式客户端DApp读取需要擦除的许可链数据$\mathcal{C}_p=(B_1,B_2,\cdots,B_n)$和擦除区块区间[$q_s$,$q_e$],$B_n$为当前区块高度为n的区块,定位得到目标区块数据$^{[q_s,q_e]}\mathcal{C}_p$;

[0034] (B)、分布式客户端DApp提取出$Tx_{i,j}$,对于每一个交易数据$Tx_{i,j} \in B_i \in^{[q_s,q_e]} \mathcal{C}_p$,若该区块Bi未执行擦除操作P.$\langle Tx_{i,j};t_D\rangle$=ture,则分布式客户端DApp擦除$t_{D'}:=\{hLink_{t_C},hash(t_D),hash(Tx'),t_D\}$中的$t_D$得到$t_{D'}^{'}=\{hLink_{t_C},hash(t_D),hash(Tx')\}$;

[0035] (C)、分布式客户端DApp返回擦除后的许可链数据$\{^{[0,q_{s-1}]}\mathcal{C},^{[q_s,q_e]}\mathcal{C}_p',^{[q_{e+1},q_n]}\mathcal{C}_p\}$。

[0036] 进一步地,所述步骤S2的详细过程为:

[0037] S2.1、分布式客户端DApp读取未执行区块擦除操作的许可链区块数据$\{^{[0,q_{s-1}]}\mathcal{C}_p,^{[q_{e+1},q_n]}\mathcal{C}_p\}$,读取其中区块高度为i的区块数据$B_i \in \{^{[0,q_{s-1}]}\mathcal{C}_p,^{[q_{e+1},q_n]}\mathcal{C}_p\}$,首先检查区块$B_i$中所保存的前一区块$B_{i-1}$的哈希值PrevBlockHash是否正确,然后检查区块生成数据是否符合许可链网络设置,最后计算区块中所打包的交易$T_{x_{i,j}}$的MerkleRoot值,对于每个交易$T_{x_{i,j}}$,检查其输出脚本output是否与输入脚本input的值是否对应,并检查交易锁定时间lockTime的有效性,若上述检验均通过,则未擦除部分区块链数据有效;

[0038] S2.2、分布式客户端DApp读取已经执行区块链擦除的许可链区块数据$^{[q_s,q_e]}\mathcal{C}_p'$,读取其中区块高度为i的区块数据$B_i \in^{[q_s,q_e]} \mathcal{C}_p'$,计算擦除后的交易哈希值f($Tx_i$,*)=g($Tx_i$,1)·g($Tx_i$,2)·...g($Tx_i$,u),其中u为区块$B_i$中保存的交易个数,其中擦除部分交易使用插入数据中的hash(Tx′)校验,若计算结果f(Tx_i,*)能验证许可链擦除部分$^{[q_s,q_e]}\mathcal{C}_p'$的完整性

和一致性,则验证通过,该部分区块内容有效,否则擦除部分未通过验证,擦除操作无效;

[0039] S2.3、擦除后插入相应数据的用户可使用第三方分布式云存储中的加密副本结合区块交易中的数据存储凭证进行示证,需要对已擦除的链上擦除数据进行示证的用户提供相应数据的加密密钥dk,示证方通过擦除部分交易的$t'_{D'}=\{hLink_{t_C},hash(t_D),hash(Tx')\}$得到$hLink_{t_C}$和hash($t_D$);

[0040] S2.4、示证方通过下载第三方分布式存储中的加密数据t_C并使用dk解密得到t_D,计算hash(t'_D),若hash(t'_D)=hash(t_D),则被擦除的数据得到验证。

[0041] 进一步地,所述步骤S3的详细过程如下:

[0042] S3.1、许可链中的授权节点基于共识确认擦除操作,生成擦除授权交易,其中交易转账金额为0,擦除相关信息设置为{p,q_s,q_e},其中p为擦除周期,编码后设置为转入账户地址,将擦除授权写入账本数据;

[0043] S3.2、许可链网络中的分布式客户端DApp接收到新的区块后,若区块中存在由授权节点发起的转账金额为0的交易,则解码转入账户地址,提取出擦除设置{p,q_s,q_e},然后进行擦除设置判断,开始调整节点的本地擦除设置;

[0044] S3.3、若擦除周期p≠0,则分布式客户端DApp忽略心跳数据包中的其余信息,在本地账本中的区块数据达到指定高度时,周期性执行擦除区间[q_n-p,q_n]中的区块数据$^{[q_n-p,q_n]}\mathcal{C}_p$,其中$q_n$为当前最新区块;

[0045] S3.4、若擦除周期p=0,则分布式客户端DApp执行即时的擦除,擦除本地区块账本数据中指定区间的区块数据$^{[q_s,q_e]}\mathcal{C}_p$。

[0046] 进一步地,所述步骤S4的详细过程如下:

[0047] S4.1、新节点加入许可链网络后,接收节点同步信息确认当前任期中的授权节点,并从许可链中的用户节点同步当前网络中的全账本数据;

[0048] S4.2、若当前许可链网络中正在执行周期擦除,新节点同步到未完成周期擦除的全账本数据后,检索全账本数据$\mathcal{C}_p$,逆序检索擦除周期设置的相关区块中的交易,从其中提取擦除周期{p,q_s,q_e},重新对最近一个周期执行擦除操作,得到与其他节点一致的全账本数据;

[0049] S4.3、若当前许可链网络中正在执行即时擦除,新节点同步到未完成擦除的全账本数据后,从接收到的区块中提取擦除设置{p,q_s,q_e},本地重新执行即时擦除,保证网络中全账本数据的一致。

[0050] 有益效果:与现有技术相比,本发明具有以下优点:

[0051] (1)、本发明中使用分布式客户端执行异地同步擦除,该方案易于部署,在数据写入阶段仅需插入擦除数据索引,避免了现有擦除方案中需要多方安全计算下全网共识所带来的额外网络负载,有效的处理了链上有害信息的永久写入并缓解了区块数据量的快速增长。

[0052] (2)、本发明在链上数据验证阶段,基于擦除状态验证区块数据的完整性和有效性,擦除部分区块数据可通过擦除部分哈希值验证,保障了链上数据的完整性和有效性,用户还可以通过第三方分布式云存储中的加密数据对链上擦除的插入数据进行示证。

[0053] (3)、本发明基于许可链的特性,使用授权节点调整许可链中所有节点的擦除周期,并支持特定场景下的触发擦除,有效避免了许可链上有害数据的大规模传播。

附图说明

[0054] 图1为本发明的整体系统框架图。

[0055] 图2是实施例链上数据擦除阶段示意图。

[0056] 图3是实施例链上数据验证阶段示意图。

具体实施方式

[0057] 下面对本发明技术方案进行详细说明,但是本发明的保护范围不局限于所述实施例。

[0058] 如图1所示,本发明涉及用户节点、授权节点、分布式客户端和非交易数据;用户节点使用分布式客户端与许可链网络进行交互;授权节点对加入许可链网络的分布式客户端进行认证,并对许可链网络中用户节点的擦除操作进行授权;分布式客户端保存许可链中的账本信息,并生成或验证区块中的交易;非交易数据为分布式客户端生成交易时,用户节点在交易的输入脚本和输出脚本插入的辅助交易执行的补充信息。

[0059] 本实施例的许可链上授权的非交易有害数据完全擦除方法,具体包括以下步骤:

[0060] 环节1(异地多步擦除):

[0061] 1.1、新交易写入

[0062] 许可链中的用户节点首先随机生成加密密钥$dk \leftarrow \{0,1\}^{\lambda}$,然后使用对称加密写入信息明文$t_D$得到密文$t_C \leftarrow Enc(dk, t_D)$;用户节点将加密后的密文$t_C$存储到第三方分布式云存储,得到数据存储凭证$hLink_{t_C}$;为验证擦除后交易数据,用户节点计算擦除后的交易哈希值hash(Tx′)和插入数据明文t_D的哈希值$hash(t_D)$,组合得到非交易数据$t_{D'} = \{hLink_{t_C}, hash(t_D), hash(Tx'), t_D\}$,并将其写入所生成交易;

[0063] 1.2、有害数据判定及擦除授权

[0064] 许可链网络中的用户节点通过心跳机制选举出授权节点,即:当许可链网络中不存在授权节点时,用户节点首先切换到候选状态并进行投票,收到大多数投票认可的用户节点则成为新的授权节点,授权节点周期性的发送心跳信息给所有用户节点来维持其主导地位,若用户节点一段时间没有接收到心跳信息,许可链中则因为没有授权节点重新选出新的授权节点,该许可链中所有用户节点切换到候选状态并进入新的任期,投票选出新的节点;选举结束后,许可链中授权节点检索全账本区块数据$\mathcal{C}_p$,若检测到区块链中存在有害数据或收到涉及用户隐私的敏感数据的擦除请求,则根据数据内容定位区块区间$[q_s, q_e]$,其中“q_s”和“q_e”表示区块高度s和e的区块,生成擦除授权交易;

[0065] 1.3、异地分布式客户端的本地擦除

[0066] 分布式客户端DApp查询当前许可链数据$\mathcal{C}_p$当前区块高度n,确定需要进行擦除的区块区间$[q_s, q_e]$,得到需要擦除的链上区块集合$^{[q_s,q_e]}\mathcal{C}_p$;然后,分布式客户端DApp对交易数据$Tx_{i,j} \in B_i \in^{[q_s,q_e]} \mathcal{C}_p$执行判断$\langle Tx_{i,j}; t_{D'} \rangle \mapsto \{true, false\}$,若结果为true,则该部分数据为非交

易数据并选定,若结果为false则忽略该部分数据内容,其中B_i表示特定区块高度i的区块数据,$T_{x_{i,j}}$表示第i个区块数据中的第j个交易数据;分布式客户端$DApp_i$执行非交易数据擦除算法txPrune擦除选定的非交易数据,其中输入为许可链数据$\mathcal{C}_p$和擦除区块区间$[q_s,q_e]$,输出为擦除后的许可链数据$\{^{[0,q_{s-1}]}\mathcal{C}_p,^{[q_s,q_e]}\mathcal{C}_p',^{[q_{e+1},q_n]}\mathcal{C}_p\}$,其中$\mathcal{C}_p'$为执行擦除操作后的$\mathcal{C}_p$数据,擦除后的非交易数据变为为$t_{D'}^{'}=\{hLink_{t_C},hash(t_D),hash(Tx')\}$,如图2所示。

[0067] 环节2(擦除后的验证与示证):

[0068] 2.1、分布式客户端DApp读取未执行区块擦除操作的许可链区块数据$\{^{[0,q_{s-1}]}\mathcal{C}_p,^{[q_{e+1},q_n]}\mathcal{C}_p\}$,读取其中区块高度为i的区块数据$B_i\in\{^{[0,q_{s-1}]}\mathcal{C}_p,^{[q_{e+1},q_n]}\mathcal{C}_p\}$,首先检查区块$B_i$中所保存的前一区块$B_{i-1}$的哈希值PrevBlockHash是否正确,然后检查区块生成数据是否符合许可链网络设置,最后计算区块中所打包的交易$T_{x_{i,j}}$的MerkleRoot值,对于每个交易$T_{x_{i,j}}$,检查其输出脚本output是否与输入脚本input的值是否对应,并检查交易锁定时间lockTime的有效性,若上述检验均通过,则未擦除部分区块链数据有效;然后,分布式客户端DApp读取已经执行区块链擦除的许可链区块数据$^{[q_s,q_e]}\mathcal{C}_p'$,读取其中区块高度为i的区块数据$B_i\in^{[q_s,q_e]}\mathcal{C}_p'$,计算擦除后的交易哈希值$f(Tx_i,*)=g(Tx_i,1)\cdot g(Tx_i,2)\cdot\ldots g(Tx_i,u)$,其中u为区块$B_i$中保存的交易个数,其中擦除部分交易使用插入数据中的hash(Tx′)校验,若计算结果$f(Tx_i,*)$能验证许可链擦除部分$^{[q_s,q_e]}\mathcal{C}_p'$的完整性和一致性,则验证通过,该部分区块内容有效,否则擦除部分未通过验证,擦除操作无效;

[0069] 2.2、擦除后插入相应数据的用户节点可使用第三方分布式云存储中的加密副本结合区块交易中的数据存储凭证进行示证,需要对已擦除的链上擦除数据进行示证的用户提供相应数据的加密密钥dk,示证方通过擦除部分交易的$t_{D'}^{'}=\{hLink_{t_C},hash(t_D),hash(Tx')\}$得到$hLink_{t_C}$和$hash(t_D)$;示证方通过下载第三方分布式存储中的加密数据$t_C$并使用dk解密得到$t_D$,计算$hash(t'_D)$,若$hash(t'_D)=hash(t_D)$,则被擦除的数据得到验证。

[0070] 环节3(调节设置擦除周期)

[0071] 3.1、许可链中的授权节点基于共识确认擦除操作来生成擦除授权交易,其中交易转账金额为0,擦除相关信息设置为$\{p,q_s,q_e\}$,其中p为擦除周期,编码后设置为转入账户地址,将擦除授权写入账本数据;

[0072] 3.2、许可链网络中的分布式客户端DApp接收到新的区块后,若区块中存在由授权节点发起的转账金额为0的交易,则解码转入账户地址,提取出擦除设置$\{p,q_s,q_e\}$,然后进行擦除设置判断,开始调整节点的本地擦除设置;若擦除周期$p\neq0$,则分布式客户端DApp忽略心跳数据包中的其余信息,在本地账本中的区块数据达到指定高度时,周期性执行擦除区间$[q_n-p,q_n]$中的区块数据$^{[q_n-p,q_n]}\mathcal{C}_p$,其中$q_n$为当前最新区块;擦除周期$p=0$,则分布式客户端DApp执行即时的擦除,擦除本地区块账本数据中指定区间的区块数据$^{[q_s,q_e]}\mathcal{C}_p$。

[0073] 环节4(初始化新用户节点)

[0074] 4.1、新节点加入许可链网络后,接收节点同步信息确认当前任期中的授权节点,并从许可链中的用户节点同步当前网络中的全账本数据;

[0075] 4.2、若当前许可链网络中正在执行周期擦除，新节点同步到未完成周期擦除的全账本数据后，检索全账本数据$\mathcal{C}_p$，逆序检索擦除周期设置的相关区块中的交易，从其中提取擦除周期{p，q_s，q_e}，重新对最近一个周期执行擦除操作，得到与其他节点一致的全账本数据；若当前许可链网络中正在执行即时擦除，新节点同步到未完成擦除的全账本数据后，从接收到的区块中提取擦除设置{p，q_s，q_e}，本地重新执行即时擦除，保证网络中全账本数据的一致，如图3所示。

[0076] 通过上述实施例可以看出，本发明通过分布式客户端执行本地擦除操作，可以有效的处理链上有害信息的永久写入，并设计方案使用擦除数据的哈希值验证链上数据的完整性和有效性，且使用第三方分布式云存储保存加密副本实现基于密码学的用户示证。此外，允许擦除周期可变使得许可链网络可以更灵活的应对非法数据插入的突发情况。

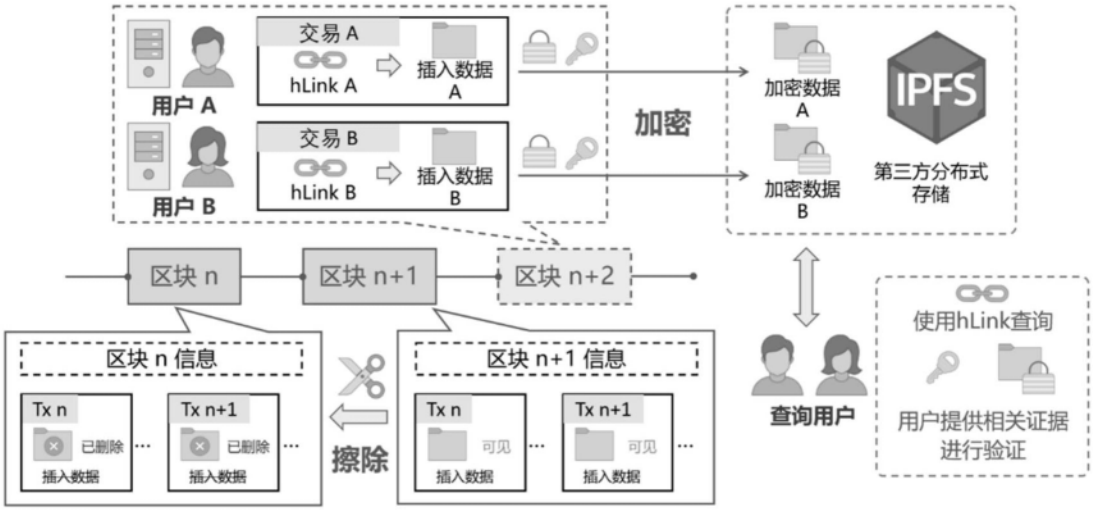

用户 A
交易 A
hLink A
插入数据 A
用户 B
交易 B
hLink B
插入数据 B
加密
加密数据 A
加密数据 B
IPFS
第三方分布式存储
区块 n
区块 n+1
区块 n+2
区块 n 信息
区块 n+1 信息
Tx n
Tx n+1
已删除
插入数据
擦除
可见
查询用户
使用hLink查询
用户提供相关证据进行验证

图1

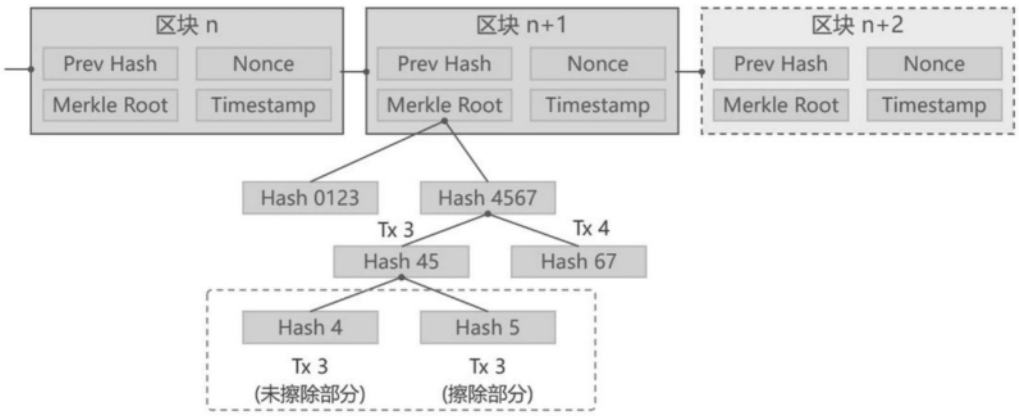

区块 n
区块 n+1
区块 n+2
Prev Hash
Nonce
Merkle Root
Timestamp
Hash 0123
Hash 4567
Tx 3
Tx 4
Hash 45
Hash 67
Hash 4
Hash 5
Tx 3
(未擦除部分)
Tx 3
(擦除部分)

图2

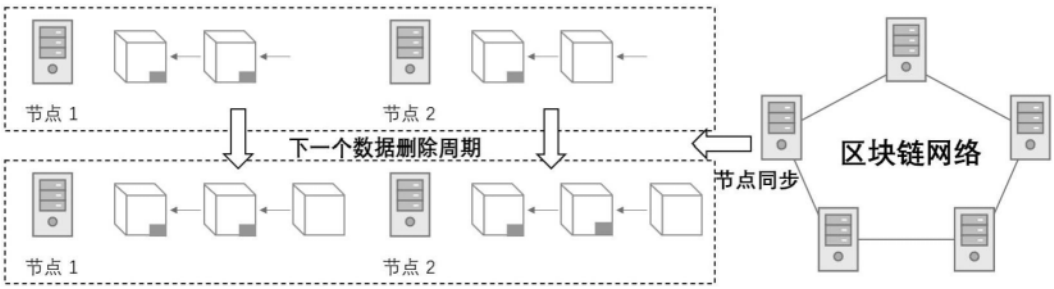

节点 1
节点 2
下一个数据删除周期
节点 1
节点 2
节点同步
区块链网络

图3