(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 108846297 A
(43)申请公布日 2018.11.20

(21)申请号 201810774852.4

(22)申请日 2018.07.16

(71)申请人 佛山伊苏巨森科技有限公司
地址 528200 广东省佛山市南海区桂城街道夏南路61号创越时代文化创意园1号楼创业工场孵化器有限公司内210室之五

(72)发明人 刘祎 马克西姆·马修斯 王大卫

(74)专利代理机构 佛山粤进知识产权代理事务所(普通合伙) 44463
代理人 张敏

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)

权利要求书1页 说明书4页

(54)发明名称

一种在具有对等节点的区块链网络上分发和检索数据的方法

(57)摘要

本发明提供了一种在具有对等节点的区块链网络上分发和检索数据的方法,包括:用私密密钥加密包含所述数据的文件;将加密文件分成加密块并将私密密钥分成成私密共享;将块和私密共享分发给对等节点;根据客户端的请求访问文件,通过一个对等节点检索加密块以重建加密文件,并检索至少一些私密共享用于重建私密密钥,并用重建的私密密钥解密加密文件;所述对等节点共享区块链,以形成区块链网络;并且还通过在区块链网络上发送的消息将私密共享发送到对等节点以及通过在区块链网络上发送的消息完成请求和检索私密共享。

CN 108846297 A

1.一种在具有对等节点的区块链网络上分发和检索数据的方法,包括:

(i)用私密密钥加密包含所述数据的文件;

(ii)将加密文件分成加密块并将私密密钥分成成私密共享;

(iii)将块和私密共享分发给对等节点;

(iv)根据客户端的请求访问文件,通过一个对等节点检索加密块以重建加密文件,并检索至少一些私密共享用于重建私密密钥,并用重建的私密密钥解密加密文件;

其特征在于,所述对等节点共享区块链,以形成区块链网络;并且在步骤(iii)中,还通过在区块链网络上发送的消息将私密共享发送到对等节点;在步骤(iv),通过在区块链网络上发送的消息完成请求和检索私密共享。

2.根据权利要求1所述的方法,特征在于,所述私密共享还使用对等节点的公钥对进行加密。

3.根据前述权利要求之1的方法,其特征在于,其中请求和检索私密共享的每个消息包含:识别发送消息的对等节点,识别所述消息的对等节点接收者,以及识别发送或检索的私密共享的信息,所述信息是可由区块链网络的所有对等节点公开访问。

4.根据前述权利要求之1的方法,其特征在于,在步骤中识别私密共享的传送,请求和检索的每个消息中的私密共享的信息分别标识与私密密钥相关的私密共享的IIV,

以及与之相关的文件。

5.根据前述权利要求之1的方法,其特征在于,识别私密共享的传输,请求和检索的每个消息中的私密共享的信息,其中步骤(ii i)和(iv)还分别标识私密共享的版本。

6.根据前述权利要求5的方法,其特征在于,私密共享的版本可以通过从对等节点之一发送到所有剩余节点的消息来撤销。

7.根据前述权利要求6的方法,其特征在于,请求和检索私密共享的每个消息分别由发送消息的对等节点进行数字签名。

8.根据前述权利要求之1的方法,其特征在于,步骤(iv)包括在发送消息之前从一个对等节点向所有剩余的对等节点发送私密共享请求的消息从所述剩余的对等节点检索所述私密共享。

一种在具有对等节点的区块链网络上分发和检索数据的方法

技术领域

[0001] 本发明涉及分布式计算领域，具体而言，涉及一种在具有对等节点的区块链网络上分发和检索数据的方法。

背景技术

[0002] 块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。系统是开放的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开，任何人都可以通过公开的接口查询区块链数据和开发相关应用，因此整个系统信息高度透明。区块链采用基于协商一致的规范和协议(比如一套公开透明的算法)使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。一旦信息经过验证并添加至区块链，就会永久的存储起来，除非能够同时控制住系统中超过51％的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。由于节点之间的交换遵循固定的算法，其数据交互是无需信任的(区块链中的程序规则会自行判断活动是否有效)，因此交易对手无须通过公开身份的方式让对方对自己产生信任，对信用的累积非常有帮助。

[0003] 区块链作为新一代计算机系统，其实际应用中的亟待处理的实际问题还有很多未提出具体的解决方案。

发明内容

[0004] 本发明提出了一种在具有对等节点的区块链网络上分发和检索数据的方法，包括：(i)用私密密钥加密包含所述数据的文件；(ii)将加密文件分成加密块并将私密密钥分成成私密共享；(iii)将块和私密共享分发给对等节点；(iv)根据客户端的请求访问文件，通过一个对等节点检索加密块以重建加密文件，并检索至少一些私密共享用于重建私密密钥，并用重建的私密密钥解密加密文件；所述对等节点共享区块链，以形成区块链网络；并且在步骤(iii)中，还通过在区块链网络上发送的消息将私密共享发送到对等节点；在步骤(iv)，通过在区块链网络上发送的消息完成请求和检索私密共享。

[0005] 进一步的,所述私密共享还使用对等节点的公钥对进行加密。

[0006] 进一步的,其中请求和检索私密共享的每个消息包含:识别发送消息的对等节点,识别所述消息的对等节点接收者,以及识别发送或检索的私密共享的信息,所述信息是可由区块链网络的所有对等节点公开访问。

[0007] 进一步的,在步骤中识别私密共享的传送,请求和检索的每个消息中的私密共享的信息分别标识与私密密钥相关的私密共享的IIV,以及与之相关的文件。

[0008] 进一步的,识别私密共享的传输,请求和检索的每个消息中的私密共享的信息,其中步骤(iii)和(iv)还分别标识私密共享的版本。

[0009] 进一步的,私密共享的版本可以通过从对等节点之一发送到所有剩余节点的消息来撤销。

[0010] 进一步的,请求和检索私密共享的每个消息分别由发送消息的对等节点进行数字签名。

[0011] 进一步的,步骤(iv)包括在发送消息之前从一个对等节点向所有剩余的对等节点发送私密共享请求的消息从所述剩余的对等节点检索所述私密共享。

[0012] 本发明给出了一种区块链实用的非常安全高效的文件传输方法。

具体实施方式

[0013] 为了使得本发明的目的、技术方案及优点更加清楚明白,以下结合其实施例,对本发明进行进一步详细说明;应当理解,此处所描述的具体实施例仅用于解释本发明,并不用于限定本发明。对于本领域技术人员而言,在查阅以下详细描述之后,本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内、包括在本发明的范围内,并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征,并且这些特征根据以下将详细描述将是显而易见的。

[0014] 实施例一。

[0015] 本实施例提出了一种在具有对等节点的区块链网络上分发和检索数据的方法,包括:

[0016] (i)用私密密钥加密包含所述数据的文件;(ii)将加密文件分成加密块并将私密密钥分成成私密共享;(iii)将块和私密共享分发给对等节点;(iv)根据客户端的请求访问文件,通过一个对等节点检索加密块以重建加密文件,并检索至少一些私密共享用于重建私密密钥,并用重建的私密密钥解密加密文件;所述对等节点共享区块链,以形成区块链网络;并且在步骤(iii)中,还通过在区块链网络上发送的消息将私密共享发送到对等节点;在步骤(iv),通过在区块链网络上发送的消息完成请求和检索私密共享。

[0017] 进一步的,所述私密共享还使用对等节点的公钥对进行加密。

[0018] 进一步的,其中请求和检索私密共享的每个消息包含:识别发送消息的对等节点,识别所述消息的对等节点接收者,以及识别发送或检索的私密共享的信息,所述信息是可由区块链网络的所有对等节点公开访问。

[0019] 进一步的,在步骤中识别私密共享的传送,请求和检索的每个消息中的私密共享的信息分别标识与私密密钥相关的私密共享的IIV,以及与之相关的文件。

[0020] 进一步的,识别私密共享的传输,请求和检索的每个消息中的私密共享的信息,其

中步骤(iii)和(iv)还分别标识私密共享的版本。

[0021] 进一步的,私密共享的版本可以通过从对等节点之一发送到所有剩余节点的消息来撤销。

[0022] 进一步的,请求和检索私密共享的每个消息分别由发送消息的对等节点进行数字签名。

[0023] 进一步的,步骤(iv)包括在发送消息之前从一个对等节点向所有剩余的对等节点发送私密共享请求的消息从所述剩余的对等节点检索所述私密共享。

[0024] 实施例二。

[0025] 本发明提出了一种在具有对等节点的区块链网络上分发和检索数据的方法,包括:(i)用私密密钥加密包含所述数据的文件;(ii)将加密文件分成加密块并将私密密钥分成成私密共享;(iii)将块和私密共享分发给对等节点,并且在区块链日志中包含在步骤(iii)中传输请求和检索所述私密共享的所有消息,所述消息包含在区块链的哈希树中;(iv)根据客户端的请求访问文件,通过一个对等节点检索加密块以重建加密文件,并检索至少一些私密共享用于重建私密密钥,并用重建的私密密钥解密加密文件;所述对等节点共享区块链,以形成区块链网络;并且在步骤(iii)中,还通过在区块链网络上发送的消息将私密共享发送到对等节点;在步骤(iv),通过在区块链网络上发送的消息完成请求和检索私密共享。

[0026] 步骤(ii)中,基于秘密共享技术将秘密密钥分成k个秘密份额,其中在步骤(iii)和(iv)处传送,请求和检索秘密共享的每个消息,分别包含识别秘密共享的信息,以及值n和k以及所述秘密共享的版本。

[0027] 所述私密共享还使用对等节点的公钥对进行加密,这里的加密算法选在128或者256位的AES算法。

[0028] 进一步的,其中请求和检索私密共享的每个消息包含:识别发送消息的对等节点,识别所述消息的对等节点接收者,以及识别发送或检索的私密共享的信息,所述信息是可由区块链网络的所有对等节点公开访问。

[0029] 在步骤中识别私密共享的传送,请求和检索的每个消息中的私密共享的信息分别标识与私密密钥相关的私密共享的IIV,以及与之相关的文件。识别私密共享的传输,请求和检索的每个消息中的私密共享的信息,其中步骤(iii)和(iv)还分别标识私密共享的版本。私密共享的版本可以通过从对等节点之一发送到所有剩余节点的消息来撤销。请求和检索私密共享的每个消息分别由发送消息的对等节点进行数字签名。

[0030] 步骤(iv)包括在发送消息之前从一个对等节点向所有剩余的对等节点发送私密共享请求的消息从所述剩余的对等节点检索所述私密共享。

[0031] 每个对等节点包括唯一标识符,数据存储空间,网络管理器,公钥,优选地在证书内提供,以及私钥。在步骤(iii),将块和秘密共享存储在对等节点的数据存储空间上。

[0032] 实施例三。

[0033] 本发明提出了一种在具有对等节点的区块链网络上分发和检索数据的方法,包括:(i)用私密密钥加密包含所述数据的文件,在本实施例中随机生成所述私密密钥;(ii)将加密文件分成加密块并将私密密钥分成成私密共享;(iii)将块和私密共享分发给对等节点,并且在区块链日志中包含在步骤(iii)中传输请求和检索所述私密共享的所有消息,

所述消息包含在区块链的哈希树中;(iv)根据客户端的请求访问文件,

[0034] 通过一个对等节点检索加密块以重建加密文件,并检索至少一些私密共享用于重建私密密钥,并用重建的私密密钥解密加密文件;所述对等节点共享区块链,以形成区块链网络;并且在步骤(iii)中,还通过在区块链网络上发送的消息将私密共享发送到对等节点,基于分布式散列算法将块关联并分发到对等节点,还在该步骤(iii)产生分布式网络;在步骤(iv),通过在区块链网络上发送的消息完成请求和检索私密共享。

[0035] 步骤(ii)中,基于秘密共享技术将秘密密钥分成k个秘密份额,其中在步骤(iii)和(iv)处传送,请求和检索秘密共享的每个消息,分别包含识别秘密共享的信息,以及值n和k以及所述秘密共享的版本。

[0036] 所述私密共享还使用对等节点的公钥对进行加密,这里的加密算法选在128或者256位的AES算法。

[0037] 进一步的,其中请求和检索私密共享的每个消息包含:识别发送消息的对等节点,识别所述消息的对等节点接收者,以及识别发送或检索的私密共享的信息,所述信息是可由区块链网络的所有对等节点公开访问。

[0038] 在步骤中识别私密共享的传送,请求和检索的每个消息中的私密共享的信息分别标识与私密密钥相关的私密共享的IIV,以及与之相关的文件。识别私密共享的传输,请求和检索的每个消息中的私密共享的信息,其中步骤(iii)和(iv)还分别标识私密共享的版本。私密共享的版本可以通过从对等节点之一发送到所有剩余节点的消息来撤销。请求和检索私密共享的每个消息分别由发送消息的对等节点进行数字签名。步骤(iv)包括在发送消息之前从一个对等节点向所有剩余的对等节点发送私密共享请求的消息从所述剩余的对等节点检索所述私密共享。

[0039] 每个对等节点包括唯一标识符,数据存储空间,网络管理器,公钥,优选地在证书内提供,以及私钥。在步骤(iii),将块和秘密共享存储在对等节点的数据存储空间上。

[0040] 实施例四。

[0041] 在本实施例中还构造了一种计算机程序,包括可由计算机执行的指令,所述指令被配置为当在所述计算机上运行时执行根据实施例一至四之一所述的方法的步骤。

[0042] 其还是用网络附加存储,即通过存储介质存储所述计算机程序。

[0043] 本实施例还进一步构造一种具有对等节点的计算机网络,每个对等节点包括唯一标识符,数据存储空间,网络管理器,优选地在证书内提供的公钥和私钥;每个网络管理器被配置用于执行根据实施例一至四之一所述的方法。

[0044] 虽然上面已经参考各种实施例描述了本发明,但是应当理解,在不脱离本发明的范围的情况下,可以进行许多改变和修改。因此,其旨在上述详细描述被认为是例示性的而非限制性的,并且应当理解,以下权利要求(包括所有等同物)旨在限定本发明的精神和范围。以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后,技术人员可以对本发明作各种改动或修改,这些等效变化和修饰同样落入本发明权利要求所限定的范围。