(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106447311 B
(45)授权公告日 2019.11.08

(21)申请号 201610851973.5

(22)申请日 2016.09.26

(65)同一申请的已公布的文献号
申请公布号 CN 106447311 A

(43)申请公布日 2017.02.22

(73)专利权人 北京天德科技有限公司
地址 100089 北京市海淀区知春路113号1708-048

(72)发明人 邓恩艳

(51)Int.Cl.
G06F 21/62(2013.01)
H04L 29/06(2006.01)

(56)对比文件
CN 105592098 A,2016.05.18,
CN 105719172 A,2016.06.29,
US 2016098730 A1,2016.04.07,
CN 101576835 A,2009.11.11,
CN 105719185 A,2016.06.29,

审查员 王阜东

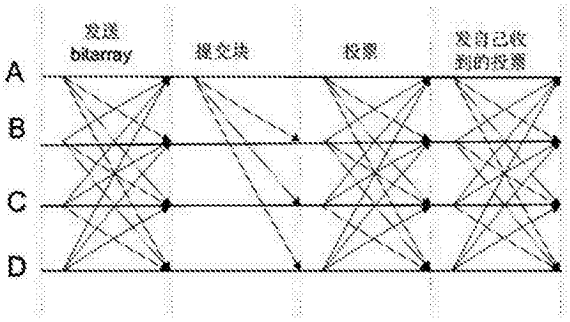
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种四次通信的拜占庭容错算法的区块链建块方法

(57)摘要

本发明提供了一种四次通信的拜占庭容错算法的私有区块链建块方法，包含(1)所有节点对收到的交易进行hash映射，得到一发出给其余所有节点的bitarray，每个节点对收到的bitarray进行2/3与运算，求得2/3以上节点的交易交集对应的bitarray；(2)建块节点根据这个bitarray得到交易集合进行建块，将块提交给其余节点；(3)收到块的节点通过自身的bitarray和块中的交易集合对比完成验证，验证结束后将验证结果的数字签名发给其余所有节点；(4)第二轮投票将所有节点收到的所有对该块的投票签名后转发，从而使得每个节点收到所有节点的投票，对投票进行统计得到最终的结果，从而决定是否接纳该块。



CN 106447311 B

1.一种四次通信的拜占庭容错算法的区块链建块方法,其特征在于包含以下步骤:

步骤(1)交易级别的确认和投票:所有节点对收到的所有交易进行hash映射,hash映射后得到一个0～16^64的整数m,假设bitarray的长度为n,每一位的初值为0,通过m%n运算,得到一个0～n-1之间的整数num,对bitarray的第num位赋值为1;最后得到一个bitarray,然后将这个bitarray发送给其余的所有节点;每个节点对收到的所有bitarray进行2/3与运算,求得2/3以上节点的交易交集对应的bitarray;所述2/3与运算是指在第一次的通信之后,所有节点根据收到的bitarray求2/3交集运算,也就是说每一位如果有2/3以上的bitarray都是1,则运算结果的bitarray在该位为1,否则为0;

步骤(2)建块:建块节点根据运算结果的bitarray得到交易集合进行建块,将块提交给其余节点;

步骤(3)对块进行验证:收到块的节点通过自身的bitarray和块中的交易集合对比完成验证,验证结束后将验证结果及其数字签名发给其余所有节点;所述步骤(3)对块进行验证是通过第一轮投票完成的,包括:(a)所有节点在收到块之后进行验证,利用自身运算的得到的bitarray交集,和收到的块中的交易集合进行对照,若交易集合一致,且建块者是选出的建块节点,则认为块合法;(b)对块的投票结果用0和1表示,0表示不通过,1表示通过,将投票结果和块的hash签名用自己的私钥加密得到数字签名;(c)将投票结果、块的hash签名和数字签名发给其余节点;

步骤(4)每个节点第二轮投票将收到的所有对该块的投票签名后转发,从而使得每个节点收到所有节点的投票,对投票进行统计得到最终的结果,从而决定是否接纳该块;该步骤(4)包括(a)每个节点在收到其余节点第一轮的投票之后,得到一个投票的集合,对这个集合用自己的私钥签名后发出;(b)每个节点在收到第二轮的投票之后对投票结果进行统计,得到最终的结果,从而决定是否要将区块存入链中。

2.根据权利要求1所述的一种四次通信的拜占庭容错算法的区块链建块方法,其特征在于:所述步骤(2)的建块运算包括:在节点内部执行RoundRobin算法,得到唯一的建块节点;所述建块节点自身根据交集集合对应的bitarray,从所收集到的交易中得到所有节点的交易交集,利用这部分交易建块;所述建块节点将自己建的块发给其余节点。

3.根据前述任意一个权利要求所述的一种四次通信的拜占庭容错算法的区块链建块方法,其特征在于:为了容忍f个单机发生拜占庭故障,冗余系统至少需要存在3f+1个单机,为了容忍f个节点的故障或者被攻击,系统需要有3f+1个节点,所述节点在出现故障或者被攻击成功的情况下,如果节点总数超过被控制节点的三倍,系统的容错算法可以保证其余正常节点正常运作。

4.根据权利要求3所述的一种四次通信的拜占庭容错算法的区块链建块方法,其特征在于:若每次投票过程中如果只有少于1/3的节点出现故障或者被攻击控制,系统可以正常运作,异常节点恢复正常之后,会有一个同步机制,向其余节点进行请求,得到完整地区块链,从而保证任何一个节点在恢复正常之后可以正常的参与到新一轮的建块投票中,且保持了分布式系统数据的一致性和每个节点数据的完整性。

5.根据权利要求3所述的一种四次通信的拜占庭容错算法的区块链建块方法,其特征在于:每个节点在进行投票时,利用自己的私钥对投票结果和块哈希值进行加密,得到签名;将数字签名和投票信息一同发给其余所有节点,所有节点在收到载有数字签名的投票

之后，利用发送者的公钥对数字签名进行解密得到加密前的信息，将解密得到的信息和投票信息对比，如果完全一样，则认为收到的信息是可信的，所有的节点在投票过程进行数字签名以保证投票信息的不可抵赖性和不可篡改性。

一种四次通信的拜占庭容错算法的区块链建块方法

技术领域

[0001] 本发明涉及一种基于一致性算法的区块链的建块方法，特别是采用四次通信的拜占庭容错算法进行区块链建块的方法。

背景技术

[0002] 在区块链系统中，多个节点各自维护一个区块链，要保证数据在所有节点的一致性，需要保证每个节点维护的区块链是一样的。随着电子商务网站等分布式应用的高速发展，系统可能会遭受到更多的攻击，从而导致节点中存在“叛徒节点”，要保证系统在这种情况下保持正常运作，且忠诚的正常节点的数据保持一致，在这样的情况下，引入了基于拜占庭算法的建块方式。关键的服务不仅需要能够容忍良性错误，还需要容忍拜占庭错误。相关内容可见参考文献M.Pease,L.Lamport,S.Shostak.The Byzantine generalsproblem[J].ACM Trans.P rogramming Languages and Systems,1982,4(3):382～401。

[0003] 目前的区块链中所存的交易还是来源于系统内部，即系统节点之间产生的交易。对于交易级别的验证是通过数字签名技术来实现，如果要将交易来源扩展到系统外部，一方面，对于系统本身无法验证的交易，系统的单个节点在收到交易后无法单独验证合法性；另一方面，对于建块的过程，目前的区块链(如Bitcoin、以太坊)以挖矿的方式实现，所有节点中挖矿最快的节点的块被大家所接受。所有节点接受最长链，系统的一致性也得到保证。挖矿本身是一种无意义的计算，需要浪费大量的资源，在节点数目有限的情况下，由单个节点建块提交可能会导致拜占庭错误，即数据的不一致性。目前的区块链是一种分布式的账本，会面对由于区块链被修改而导致的经济损失，另外，在面对黑客攻击的情况下，要保障数据的不可篡改性，或者系统中大部分节点数据的不可篡改性，即保证数据的安全性。

发明内容

[0004] 本发明的目的在于提供一种区块链的建块的方法，可以达到保证系统一致性，克服拜占庭错误，防止攻击的目的。

[0005] 一种四次通信的拜占庭容错算法的区块链建块方法，包含以下步骤：

[0006] (1)交易级别的确认和投票：所有节点对收到的交易进行hash映射，得到一个bitarray，将bitarray发出给其余所有节点，每个节点对收到的bitarray进行2/3与运算，求得2/3以上节点的交易交集对应的bitarray；

[0007] (2)建块：建块节点根据这个bitarray得到交易集合进行建块，将块提交给其余节点；

[0008] (3)对块进行验证：收到块的节点通过自身的bitarray和块中的交易集合对比完成验证，验证结束后将验证结果的数字签名发给其余所有节点；

[0009] (4)第二轮投票将所有节点收到的所有对该块的投票签名后转发，从而使得每个节点收到所有节点的投票，对投票进行统计得到最终的结果，从而决定是否接纳该块；

[0010] 优选的，对于步骤(1)，hash映射后得到一个0～16^64的整数m，假设bitarray的长

度为n，每一位的初值为0，通过m%n运算，得到一个0～n-1之间的整数num，对bitarray的第num位赋值为1，然后将这个bitarray发送给其余的所有节点。

[0011] 优选的，所述步骤(2)的建块运算包括：(a)每个节点在得到其余所有节点的bitarray之后开始运算，对所有的bitarray进行与运算，得到所有交易的交集所对应的bitarray，完成对交易的投票；(b)在节点内部执行RoundRobin算法，得到唯一的建块节点；(c)所述建块节点自身根据交集集合对应的bitarray，从所收集到的交易中得到所有节点的交易交集，用这部分交易建块；(d)所述建块节点将自己建的块发给其余节点。

[0012] 优选的，步骤(3)对块进行验证是通过第一轮投票完成的，包括：(a)所有节点在收到块之后进行验证，利用自身运算的得到的bitarray交集，和收到的块中的交易集合进行对照，若交易集合一致，且建块者是选出的建块节点，则认为块合法；(b)对块的验证结果用0和1表示，0表示不通过，1表示通过，将投票结果和块的hash签名用自己的私钥加密得到数字签名；(c)将投票结果和数字签名发给其余节点。

[0013] 优选的，步骤(4)包括(a)每个节点在收到其余节点第一轮的投票之后，得到一个投票的集合，对这个集合用自己的私钥签名后发出；(b)每个节点在收到第二轮的投票之后对投票结果进行统计，得到最终的结果，从而决定是否要将区块存入链中。

[0014] 为了完成目前的区块链的不同节点建块的一致性，安全性，目前设计的方法采用一种分为四个步骤的一致性算法。新的一致性算法需要有四次通信，相比于传统的区块链的一致性算法，具有如下优点：

[0015] (1)该建块方式引入了对交易级别的投票，这样的设计使得对交易的确认和块的确认可以并行的进行，通过增加单个节点的机器数量，或者提升机器性能采用多线程的方式，建块速度可以大大增加，对于系统的扩展性提供了可能。

[0016] (2)允许接受系统外部交易，这使得区块链的使用场景扩大。为了保证对于系统外部的交易的正确性的认证，所有来自于外部的交易，都首先要进行一步投票，即对于交易级别的投票。所有节点对于交易求交集，保证所有交易都是每个节点都收到的，防止一个节点伪造一条交易的情况发生。

[0017] (3)bitarray的使用，使得对交易级别的验证速度大大提高。节点之间的通信只要一个bitarray就可以了，通信速度大幅提高，而在求交集的过程中，bitarray的使用，只需要对bit数组的与运算就可以迅速得到交接交集，bitarray的使用时为交易的验证提供了一种有效的技术手段。

[0018] (4)此后拜占庭算法投票可以保证达成一致，防止拜占庭错误的产生。投票过程利用拜占庭容错算法，保证了在系统中存在1/3以内的叛徒节点的情况下，系统仍然可以正常运转。即系统的可以容忍的出错节点的数量占到节点数的1/3。

[0019] 根据下文结合附图对本发明具体实施例的详细描述，本领域技术人员将会更加明了本发明的上述以及其他目的、优点和特征。

附图说明

[0020] 后文将参照附图以示例性而非限制性的方式详细描述本发明的一些具体实施例。附图中相同的附图标记标示了相同或类似的部件或部分。本领域技术人员应该理解，这些附图未必是按比例绘制的。本发明的目标及特征考虑到如下结合附图的描述将更加明显，

附图中：

[0021] 图1是根据本发明优选实施例的四次通信示意图；

[0022] 图2是根据本发明优选实施例的BitArray构造原理图；

[0023] 图3是根据本发明优选实施例的投票信息示意图；

[0024] 图4是根据本发明优选实施例统计投票信息示意图。

具体实施方式

[0025] 根据M.Pease,L.Lamport,S.Shostak.The Byzantine generals problem[J].ACM Trans.Programming Languagesand Systems,1982,4(3):382～401中有关拜占庭算法的相关内容可知，为了容忍f个单机发生拜占庭故障，冗余系统至少需要存在3f+1个单机，也就是说系统至少要有4个节点，4个节点可以容忍一个节点出现故障或者被攻击。为了容忍f个节点的故障或者被攻击，系统需要有3f+1个节点。如果系统要容忍最多2个节点出现故障或者被攻击。则需要有至少7个节点。节点在出现故障或者被攻击成功的情况下，如果节点总数超过被控制节点的三倍，系统的容错算法可以保证其余正常节点正常运作。

[0026] 在进行一轮建块的过程中，如果出现了建块失败，即最终大家的肯定投票数量不足总结点数的2/3，则认为本轮建块失败，开始新一轮建块，此时区块链的高度不会增加。每次投票过程中如果只有少于1/3的节点出现故障或者被攻击控制，系统可以正常运作。异常节点恢复正常之后，会有一个同步机制。向其余节点进行请求，得到完整地区块链。这样的方式保证了任何一个节点在恢复正常之后可以正常的参与到新一轮的建块投票中，保持了分布式系统数据的一致性和每个节点数据的完整性。

[0027] 所有节点在进行投票过程中会使用数字签名，因此本发明的拜占庭算法是一种投票信息可识别且不可伪造的拜占庭算法。每个节点在进行投票时，利用自己的私钥对投票结果和块哈希值进行加密，得到签名，数字签名和投票信息一同发给其余所有节点。所有节点在收到载有数字签名的投票之后，利用发送者的公钥对数字签名进行解密得到加密前的信息，将解密得到的信息和投票信息对比，如果完全一样，则认为收到的信息是可信的。所有的节点在投票过程进行数字签名中保证了投票信息的不可抵赖性和不可篡改性。

[0028] 实施例

[0029] 假设区块链系统中有4个节点(即M＝4)，分别为节点A、节点B、节点C、节点D，当采用本发明的方法进行建块时，每个节点首先将交易映射得到一个bitarray，如图2所示，得到bitarray之后，第一次通信为：

[0030] 节点A:将自己收到的交易映射到bitarray上，得到一个bitarray发给节点B、C、D；

[0031] 节点B:将自己收到的交易映射到bitarray上，得到一个bitarray发给节点A、C、D；

[0032] 节点C:将自己收到的交易映射到bitarray上，得到一个bitarray发给节点A、B、D；

[0033] 节点D:将自己收到的交易映射到bitarray上，得到一个bitarray发给节点A、B、C；

[0034] 在第一次的通信之后，所有节点根据得到的bitarray求2/3交集运算，运算结果记为BA，也就是说每一位如果有2/3以上的bitarray都是1，则运算结果的bitarray在该位为1，否则为0，运算结果记为BA。

[0035] 在系统中运行RoundRobin算法，随机得到一个leader，具体的做法是根据当前块的高度H和轮次R做hash映射，hash映射结果对M取模，根据取模结果得到第几个节点来建

块，从而得到leader节点。不失一般性，假设节点A被选为leader，此时节点A根据BA和自己收到的交易，得到一个交易集合BS，BS满足其中的每一个交易映射到BA上所对应的位都为1。利用这个交易集合构建一个块AB，开始第二轮通信：

[0036] 节点A：将块AB发给节点B、C、D；

[0037] 节点B、C、D在收到块AB之后，利用自己的BA，遍历块AB中的交易，如果块中的某一个交易映射到BA中的一位对应位置为0，则认为投票信息为0+hash(AB)，否则为1+hash(AB)。节点A的投票信息为1+hash(AB)。对投票信息利用自己的私钥进行加密，得到数字签名，投票信息结构如图3所示。开始第三次通信，也就是第一轮投票：

[0038] 节点A：将投票信息和数字签名发给节点B、C、D；

[0039] 节点B：将投票信息和数字签名发给节点A、C、D；

[0040] 节点C：将投票信息和数字签名发给节点A、B、D；

[0041] 节点D：将投票信息和数字签名发给节点A、B、C；

[0042] 每个节点会收到3个投票，根据数字签名验证收到的投票信息的真伪性。抛弃所有的非法投票信息后，得到一个投票集合，对这个投票集合求hash散列值之后，利用自己的私钥对其加密得到数字签名，具体发送信息的结构如图4所示。接下来开始第四次通信即第二轮投票：

[0043] 节点A：发送投票列表和数字签名给节点B、C、D；

[0044] 节点B：发送投票列表和数字签名给节点A、C、D；

[0045] 节点C：发送投票列表和数字签名给节点A、B、D；

[0046] 节点D：发送投票列表和数字签名给节点A、B、C；

[0047] 每个节点可以得到节点的投票信息，利用数字签名进行合法性认证，认为不合法的投票信息都是投否定票。对所有的投票信息进行统计汇总。不失一般性，以节点A对投票结果的统计为例展示每个节点的统计方式，A节点根据B在第三次通信发给自己的投票和节点C、D在第四次通信发给自己的他们所收到的B的次一轮投票，得到了B投给A、C、D三个节点的投票信息，假设B的投票结果为(A:1,C:1,D:1)，由于肯定票的个数大于2/3，认定B的投票结果为1，否则认为B的投票为0。对于节点C、D，利用同样的方式即可得到其最终的投票结果。

[0048] 根据节点B、C、D以及自己的投票，如果投肯定票的数量超过3个(节点总数的2/3)，则认为这个块合法，将其存入链中。否则抛弃。

[0049] 以上仅对M＝4的情况进行了说明，当M＝5或6时，其进行两轮通信的原理和方法与M＝4的情况相同。

[0050] 虽然本发明已经参考特定的说明性实施例进行了描述，但是不会受到这些实施例的限定而仅仅受到附加权利要求的限定。本领域技术人员应当理解可以在不偏离本发明的保护范围和精神的情况下对本发明的实施例能够进行改动和修改。

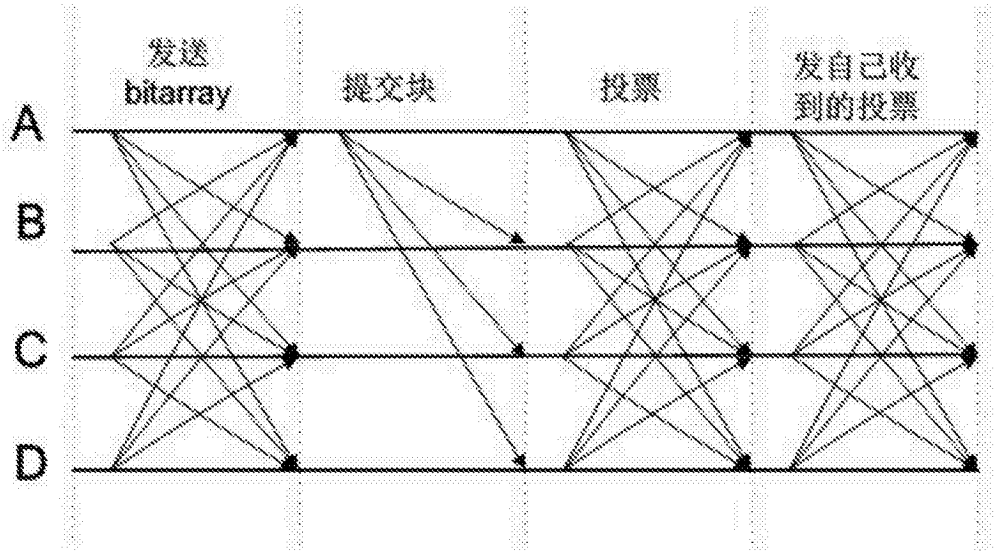

发送
bitarray
提交块
投票
发自己收
到的投票
A
B
C
D

图1

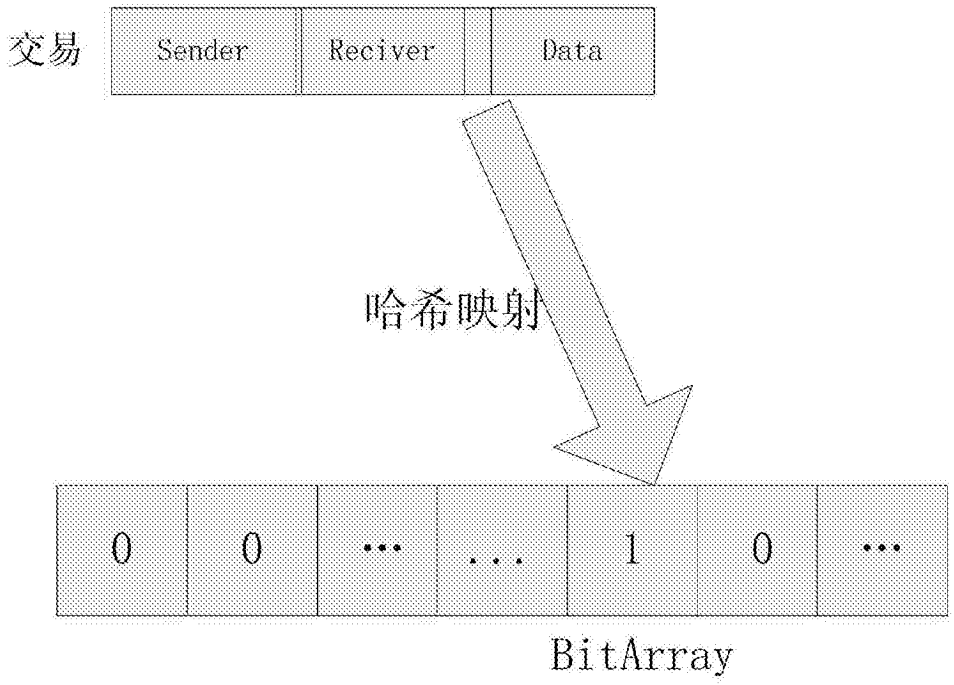

交易
Sender
Reciver
Data
哈希映射
0
0
…
…
1
0
…
BitArray

图2


B:1
Hash（Block）
Signature
一轮投票信息

图3

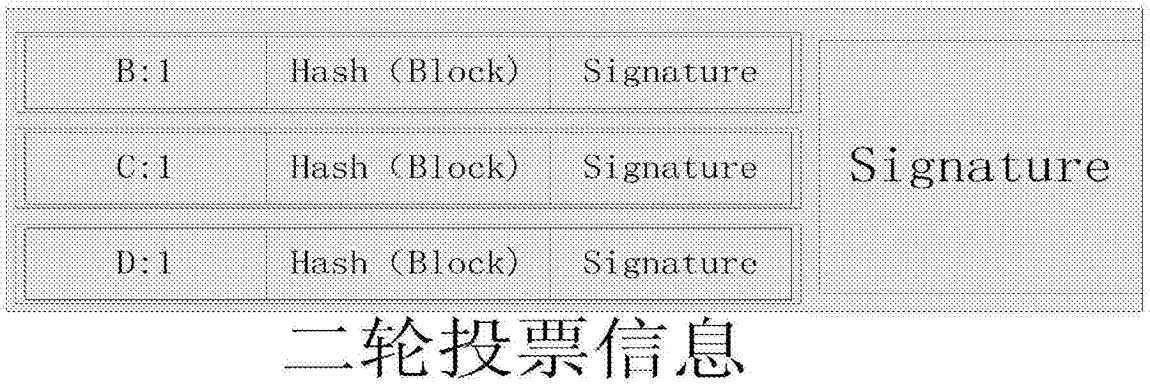

B:1
Hash（Block）
Signature
C:1
Hash（Block）
Signature
D:1
Hash（Block）
Signature
Signature
二轮投票信息

图4