(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 106453286 B
(45)授权公告日 2020.03.17

(21)申请号 201610857137.8

(22)申请日 2016.09.27

(65)同一申请的已公布的文献号
申请公布号 CN 106453286 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.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 12/24(2006.01)

(56)对比文件
US 6671821 B1,2003.12.30,
CN 101170410 A,2008.04.30,
CN 102467717 A,2012.05.23,
CN 105592098 A,2016.05.18,
US 2002129087 A1,2002.09.12,
Wei-Tek Tsai等.A System View of Financial Blockchains.《2016 IEEE Symposium of Service-Oriented System Engineering》.2016,

审查员 李昕萌

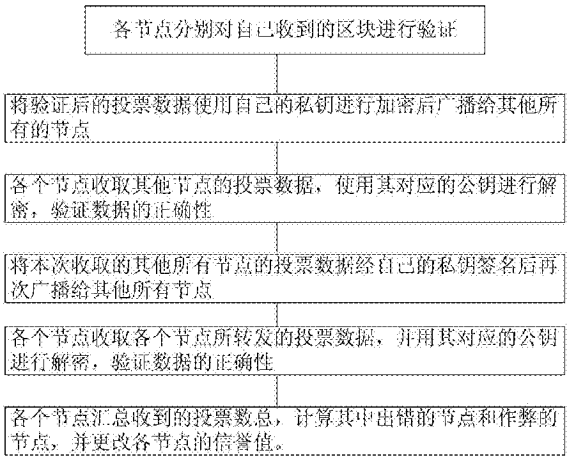
权利要求书2页 说明书4页 附图1页

(54)发明名称

一种基于区块链的信誉方法和系统

(57)摘要

本发明提供了一种区块链中的信誉方法和系统，包括N个节点，(1)各节点分别对自己收到的区块进行验证；(2)将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点；(3)各个节点收取其他节点的投票数据，使用其对应的公钥进行解密，验证数据的正确性；(4)待步骤(3)中收取完其他所有节点的投票数据后，将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点；(5)各个节点收取步骤(4)中各个节点所转发的投票数据，并用其对应的公钥进行解密，验证数据的正确性；(6)各个节点汇总步骤(5)中收到的投票数总，计算其中出错的节点和作弊的节点，并更改各节点的信誉值。



CN 106453286 B

1.一种区块链中的信誉方法,包括N个节点,各节点会维护一份其他节点的信誉值,并且各个节点在每轮建块时执行以下步骤:

(1)各节点分别对自己收到的区块进行验证;

(2)将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点;

(3)各个节点收取其他节点的投票数据,使用其对应的公钥进行解密,验证数据的正确性;

(4)待步骤(3)中收取完其他所有节点的投票数据后,将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点;

(5)各个节点收取步骤(4)中各个节点所转发的投票数据,并用其对应的公钥进行解密,验证数据的正确性;

(6)各个节点汇总步骤(5)中收到的投票数据,计算其中出错的节点和作弊的节点,并更改各节点的信誉值。

2.根据权利要求1所述的一种区块链中的信誉方法,其特征在于:

初始时,各个节点的信誉值(Reputation)为$R_i(t)=0.01$,$i=1\cdots N$,t为当前区块的建块轮次,只更新$R_i(t)>0$的节点,$R_i(t)$为0的节点被标识成作弊的节点被剔除在外。

3.根据权利要求1所述的一种区块链中的信誉方法,其特征在于:

如果节点i发送不一致的数据给不同的节点,信誉值直接降为0:$R_i(t)=0$。

4.根据权利要求1所述的一种区块链中的信誉方法,其特征在于:

如果节点i给其他节点的投票数据是一致的,但和大多数的节点不一样,即该节点i不同意大多数节点,则降低该节点i的信誉值:$R_i(t)=XR_i(t-1)$,其中$0<X<1$。

5.根据权利要求1所述的一种区块链中的信誉方法,其特征在于:

如果某节点给其他节点的投票数据是一致的,但只发送投票数据给了一部分节点,即节点i丢失消息,则降低信誉值:$R_i(t)=Y*R_i(t-1)/m$,其中$0<X<Y<1$,$m>=1$,m为连续发生错误的轮数。

6.根据权利要求1所述的一种区块链中的信誉方法,其特征在于:

如果节点i给其他节点的投票数据是一致的,且和大多数节点的投票是一致的,即该节点i同意大多数的节点,增加其信誉值:$R_i(t)=(1-Z)*R_i(t-1)+n/(n+1)*Z$,其中$n>=1$,为连续正确的轮数;$0<Z<1$,Z大时,节点信誉值增加的快,Z小时增加缓慢。

7.根据权利要求1所述的一种区块链中的信誉方法,其特征在于:

当节点i信誉值降为0时失去投票的权利,进行离线处理,使该节点i恢复正常状态并重新进入系统参加投票。

8.一种区块链中的信誉系统,包括N个节点,各节点会维护一份其他节点的信誉值,并且系统各个节点在每轮建块时执行以下步骤:

(1)各节点分别对自己收到的区块进行验证;

(2)将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点;

(3)各个节点收取其他节点的投票数据,使用其对应的公钥进行解密,验证数据的正确性;

(4)待步骤(3)中收取完其他所有节点的投票数据后,将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点;

(5)各个节点收取步骤(4)中各个节点所转发的投票数据，并用其对应的公钥进行解密，验证数据的正确性；

(6)各个节点汇总步骤(5)中收到的投票数据，计算其中出错的节点和作弊的节点，并更改各节点的信誉值。

9.根据权利要求8所述的一种区块链中的信誉系统，其特征在于：

初始时，各个节点的信誉值(Reputation)为$R_i(t)=0.01$，$i=1\cdots N$，t为当前区块的建块轮次，只更新$R_i(t)>0$的节点，$R_i(t)$为0的节点被标识成作弊的节点被剔除在外。

10.根据权利要求8所述的一种区块链中的信誉系统，其特征在于：

如果节点i发送不一致的数据给不同的节点，信誉值直接降为0：$R_i(t)=0$。

11.根据权利要求8所述的一种区块链中的信誉系统，其特征在于：

如果节点i给其他节点的投票数据是一致的，但和大多数的节点不一样，即该节点i不同意大多数节点，则降低该节点i的信誉值：$R_i(t)=XR_i(t-1)$，其中$0<X<1$。

12.根据权利要求8所述的一种区块链中的信誉系统，其特征在于：

如果某节点给其他节点的投票数据是一致的，但只发送投票数据给了一部分节点，即节点i丢失消息，则降低信誉值：$R_i(t)=Y*R_i(t-1)/m$，其中$0<X<Y<1$，$m>=1$，m为连续发生错误的轮数。

13.根据权利要求8所述的一种区块链中的信誉系统，其特征在于：

如果节点i给其他节点的投票数据是一致的，且和大多数节点的投票是一致的，即该节点i同意大多数的节点，增加其信誉值：$R_i(t)=(1-Z)*R_i(t-1)+n/(n+1)*Z$，其中$n>=1$，为连续正确的轮数；$0<Z<1$，Z大时，节点信誉值增加的快，Z小时增加缓慢。

14.根据权利要求8所述的一种区块链中的信誉系统，其特征在于：

当节点i信誉值降为0时失去投票的权利，进行离线处理，使该节点i恢复正常状态并重新进入系统参加投票。

一种基于区块链的信誉方法和系统

技术领域

[0001] 本发明涉及区块链领域,特别涉及一种基于区块链的信誉方法和系统。

背景技术

[0002] 在多节点自治的系统中,系统通常要防止出错节点和作弊的节点,比如被黑客攻击的情况。在传统的拜占庭解决方案中,只是为了在各个不受信的节点中达成公识,没有涉及到叛徒和出错节点的寻找。所以本发明就是在传统的拜占庭将军问题的解决方案上增加了信誉机制。信誉系统在许多在线系统(如网银和电商系统)中有重要应用,然而在拜占庭将军问题的解决方案引入信誉机制用于识别内部叛徒及出错节点是本发明的贡献。相关内容可参见文献M.Castro,B.Liskov,Practical byzantine fault tolerance and proactive recovery[J].ACM Transactions on Computer Systems,2002。Ferry Hendrikx,Kris Bubendorfer,Ryan Chard,Reputation systems:A survey and taxonomy [J].Journal of Parallel Distributed Computing,2015.Pp.184-197.

发明内容

[0003] 本发明就是在传统的拜占庭将军问题的解决方案上增加了信誉系统,给各个节点增加信誉分数,这样在节点出错时会相应的减少其信誉值,作弊也会有更严格的惩罚,在多节点自治的系统中,找出出错节点和作弊的节点,比如被黑客攻击的情况,当信誉分数低于某阈值,这些出错节点和作弊的节点将被从系统中剔除在外;等到这些节点回复正常,可再重回系统中。这样使得整个系统的运行更加可靠。

[0004] 有鉴于此,本发明设计了一种区块链中的信誉方法和系统。

[0005] 一种区块链中的信誉方法,包括N个节点,其特征在于还包括以下步骤:

[0006] (1)各节点分别对自己收到的区块进行验证;

[0007] (2)将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点;

[0008] (3)各个节点收取其他节点的投票数据,使用其对应的公钥进行解密,验证数据的正确性;

[0009] (4)待步骤(3)中收取完其他所有节点的投票数据后,将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点;

[0010] (5)各个节点收取步骤(4)中各个节点所转发的投票数据,并用其对应的公钥进行解密,验证数据的正确性;

[0011] (6)各个节点汇总步骤(5)中收到的投票数据,计算其中出错的节点和作弊的节点,并更改各节点的信誉值。

[0012] 优选的,初始时,各个节点的信誉值(Reputation)为$R_i(t)=0.01$,$i=1\cdots N$,t为当前区块的建块轮次,只更新$R_i(t)>0$的节点,$R_i(t)$为0的节点被标识成作弊的节点被剔除在外。

[0013] 优选的,如果节点i发送不一致的数据给不同的节点,信誉值直接降为0:$R_i(t)=$

0。

[0014] 优选的，如果节点i给其他节点的投票数据是一致的，但和大多数的节点不一样，即该节点i不同意大多数节点，则降低该节点i的信誉值：$R_i(t)=XR_i(t-1)$，其中$0<X<1$。

[0015] 优选的，如果某节点给其他节点的投票数据是一致的，但只发送投票数据给了一部分节点，即节点i丢失消息，则降低信誉值：$R_i(t)=Y*R_i(t-1)/m$，其中$0<X<Y<1$，$m>=1$，m为连续发生错误的轮数。

[0016] 优选的，如果节点i给其他节点的投票数据是一致的，且和大多数节点的投票是一致的，即该节点i同意大多数的节点，增加其信誉值：$R_i(t)=(1-Z)*R_i(t-1)+n/(n+1)*Z$，其中$n>=1$，为连续正确的轮数；$0<Z<1$，Z大时，节点信誉值增加的快，Z小时增加缓慢；

[0017] 优选的，当节点i信誉值降为0时失去投票的权利，进行离线处理，使该节点i恢复正常状态并重新进入系统参加投票。

[0018] 一种区块链中的信誉系统，包括N个节点，其特征在于该系统的各个节点执行以下步骤：

[0019] (1)各节点分别对自己收到的区块进行验证；

[0020] (2)将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点；

[0021] (3)各个节点收取其他节点的投票数据，使用其对应的公钥进行解密，验证数据的正确性；

[0022] (4)待步骤(3)中收取完其他所有节点的投票数据后，将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点；

[0023] (5)各个节点收取步骤(4)中各个节点所转发的投票数据，并用其对应的公钥进行解密，验证数据的正确性；

[0024] (6)各个节点汇总步骤(5)中收到的投票数据，计算其中出错的节点和作弊的节点，并更改各节点的信誉值。

[0025] 优选的，初始时，各个节点的信誉值(Reputation)为$R_i(t)=0.01$，$i=1\cdots N$，t为为当前区块的建块轮次，只更新$R_i(t)>0$的节点，$R_i(t)$为0的节点被标识成作弊的节点被剔除在外。

[0026] 优选的，如果节点i发送不一致的数据给不同的节点，信誉值直接降为0：$R_i(t)=0$。

[0027] 优选的，如果节点i给其他节点的投票数据是一致的，但和大多数的节点不一样，即该节点i不同意大多数节点，则降低该节点i的信誉值：$R_i(t)=XR_i(t-1)$，其中$0<X<1$。

[0028] 优选的，如果某节点给其他节点的投票数据是一致的，但只发送投票数据给了一部分节点，即节点i丢失消息，则降低信誉值：$R_i(t)=Y*R_i(t-1)/m$，其中$0<X<Y<1$，$m>=1$，m为连续发生错误的轮数。

[0029] 优选的，如果节点i给其他节点的投票数据是一致的，且和大多数节点的投票是一致的，即该节点i同意大多数的节点，增加其信誉值：$R_i(t)=(1-Z)*R_i(t-1)+n/(n+1)*Z$，其中$n>=1$，为连续正确的轮数；$0<Z<1$，Z大时，节点信誉值增加的快，Z小时增加缓慢；

[0030] 优选的，当节点i信誉值降为0时失去投票的权利，进行离线处理，使该节点i恢复正常状态并重新进入系统参加投票。

附图说明

[0031] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要的附图做简单的介绍，显而易见地，下面描述的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0032] 图1为本发明的基于区块链的信誉方法。

具体实施方式

[0033] 参见图1，一种基于区块链的信誉方法和系统，该系统包括N个节点，通过信誉方法，各节点会维护一份其他节点的信誉值。

[0034] 系统的各个节点在每轮建块时都进行投票结果的广播-验证-再广播-再验证-汇总并更新信誉值。各个节点执行以下步骤：

[0035] (1)各节点分别对自己收到的区块进行验证；

[0036] (2)将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点；

[0037] (3)各个节点收取其他节点的投票数据，使用其对应的公钥进行解密，验证数据的正确性；

[0038] (4)待步骤(3)中收取完其他所有节点的投票数据后，将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点；

[0039] (5)各个节点收取步骤(4)中各个节点所转发的投票数据，并用其对应的公钥进行解密，验证数据的正确性；

[0040] (6)各个节点汇总步骤(5)中收到的投票数据，计算其中出错的节点和作弊的节点，并更改各节点的信誉值。

[0041] 具体的信誉值计算方法如下：

[0042] 初始时，各个节点的信誉(Reputation)值为$R_i(t)=0.01$，$i=1\cdots N$，t为当前区块的建块轮次。而且信誉方法只更新$R_i(t)>0$的节点，$R_i(t)$为0的节点被标识成作弊的节点并剔除在外。

[0043] 降低信誉：

[0044] (1)如果节点i发送不一致的数据给不同的节点，信誉值直接降为0：$R_i(t)=0$；

[0045] (2)如果节点i给其他节点的投票数据是一致的，但和大多数的节点不一样，即该节点i不同意大多数节点，则降低该节点i的信誉值：$R_i(t)=XR_i(t-1)$，其中$0<X<1$。

[0046] (3)如果某节点给其他节点的投票数据是一致的，但只发送投票数据给了一部分节点，即节点i丢失消息，则降低信誉值：$R_i(t)=Y*R_i(t-1)/m$，其中$0<X<Y<1$，$m>=1$，m为连续发生错误的轮数。

[0047] 增加信誉：

[0048] (1)如果节点i给其他节点的投票数据是一致的，且和大多数节点的投票是一致的，即该节点i同意大多数的节点，增加其信誉值：$R_i(t)=(1-Z)*R_i(t-1)+n/(n+1)*Z$，其中$n>=1$，为连续正确的轮数；$0<Z<1$，Z大时，节点信誉值增加的快，Z小时增加缓慢；

[0049] (2)当节点i信誉值降为0时失去投票的权利，进行离线处理，清除影响，使该节点i恢复正常状态并重新进入系统参加投票。

[0050] 实施例：

[0051] 假设区块链系统中有4个节点，分别为A节点、B节点、C节点、D节点，当采用本发明的方法处理时，第一轮的投票情况如下，

[0052] A节点：将A节点的带数字签名的投票数据a分别发送给B节点、C节点和D节点；

[0053] B节点：将B节点的带数字签名的投票数据b分别发送给A节点、C节点和D节点；

[0054] C节点：将C节点的带数字签名的投票数据c分别发送给A节点、B节点和D节点；

[0055] D节点：将D节点的带数字签名的投票数据d分别发送给A节点、B节点和C节点。

[0056] 在第一轮投票信息交换结束后，4个节点分别获得a、b、c、d的数据。由于在数据发送过程中可能发生故障，某节点可能给不同节点发送不一样的数据，使得每个节点得到的a、b、c、d的数据不一致，因此需要进行第二轮投票。

[0057] 在进行第二轮投票时，各节点转发数据a、b、c、d，具体情况如下：

[0058] A节点：将数据a、b、c、d组合在一起形成一维数组，并加上自己的数字签名，分别发送给B节点、C节点和D节点；

[0059] B节点：将数据a、b、c、d组合在一起形成一维数组，并加上自己的数字签名，分别发送给A节点、C节点和D节点；

[0060] C节点：将数据a、b、c、d组合在一起形成一维数组，并加上自己的数字签名，分别发送给A节点、C节点和D节点；

[0061] D节点：将数据a、b、c、d组合在一起形成一维数组，并加上自己的数字签名，分别发送给A节点、C节点和D节点；

[0062] 4个节点此时已经收到了分别来自其他节点及自己节点的数据a、b、c、d，组成了一个数据a、b、c、d的二维数组，根据此二维数组判断其中出错的节点和作弊的节点，进而相应的增减其信誉。

[0063] 以上所述，仅是本发明的实例，并非对本发明做任何形式上的限制。任何精于本专业的技术人员，在不脱离本发明技术方案范围内，当可利用上述揭示的技术内容做出其他种种的改良或修饰为等同变化的等效实例，但凡是未脱离本发明技术方案内容，依据本发明的技术实质对以上实施所做的任何简单修改、等同变化与修饰，均仍属于本发明技术方案的范围内。

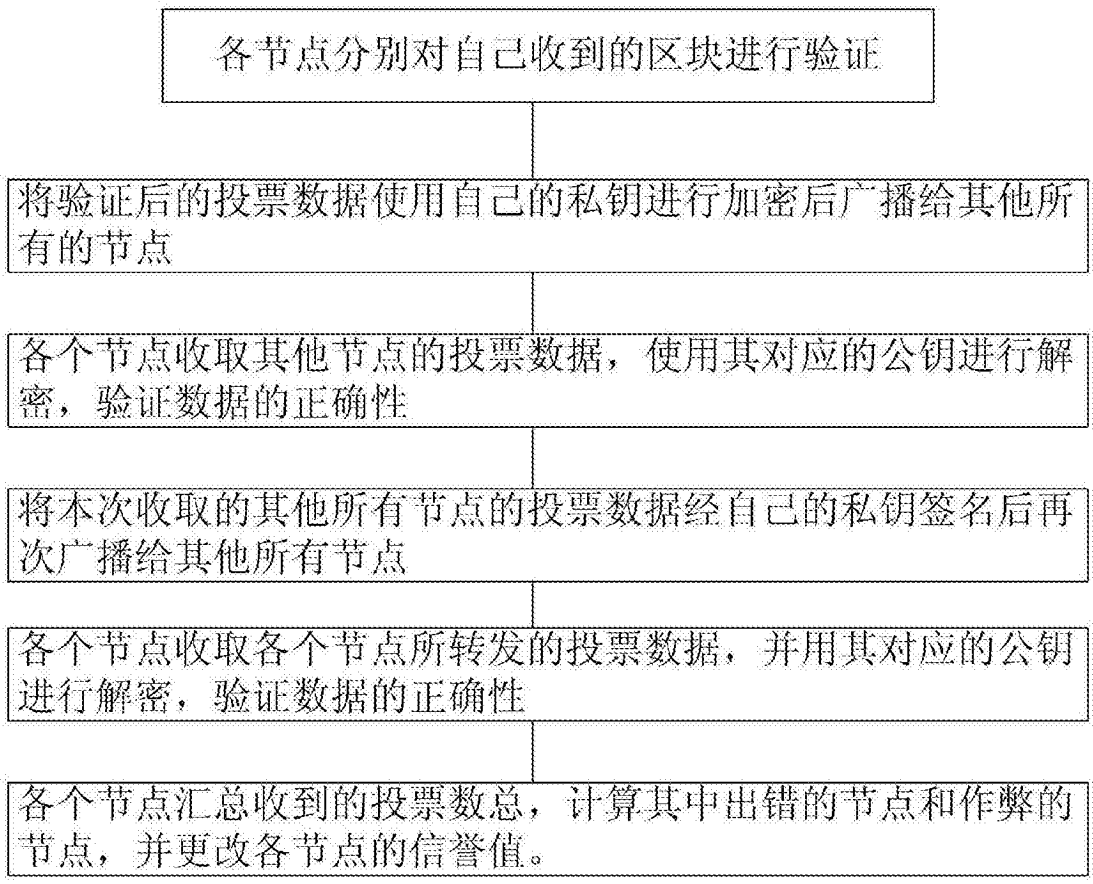

各节点分别对自己收到的区块进行验证
将验证后的投票数据使用自己的私钥进行加密后广播给其他所有的节点
各个节点收取其他节点的投票数据，使用其对应的公钥进行解密，验证数据的正确性
将本次收取的其他所有节点的投票数据经自己的私钥签名后再次广播给其他所有节点
各个节点收取各个节点所转发的投票数据，并用其对应的公钥进行解密，验证数据的正确性
各个节点汇总收到的投票数总，计算其中出错的节点和作弊的节点，并更改各节点的信誉值。

图1