(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 111445247 B
(45)授权公告日 2021.05.28

(21)申请号 202010276328.1

(22)申请日 2020.04.09

(65)同一申请的已公布的文献号
申请公布号 CN 111445247 A

(43)申请公布日 2020.07.24

(73)专利权人 堡垒科技有限公司
地址 英国牛津郡库姆纳教区库姆纳山街查利苑路2号

(72)发明人 安德鲁·威廉·罗斯科 陈邦道

(74)专利代理机构 北京天澜智慧知识产权代理有限公司 11558
代理人 尚继栋 师琦

(51)Int.Cl.
G06Q 20/38(2012.01)
G06F 16/2458(2019.01)
G06F 16/22(2019.01)

(56)对比文件
CN 109033832 A,2018.12.18
CN 109191120 A,2019.01.11
CN 110689345 A,2020.01.14
CN 109447795 A,2019.03.08
CN 108647963 A,2018.10.12
CN 110061851 A,2019.07.26
US 2019268138 A1,2019.08.29
CN 110276613 A,2019.09.24
孙一蓬.基于联盟链的多链式区块链共识性能研究.《中国优秀硕士学位论文全文数据库信息科技辑》.2020,(第 01 期),I138-219.
Congcong Ye等.Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting.《2018 5th International Conference on Dependable Systems and Their Applications (DSA)》.2018,15-24.

审查员 李五俊

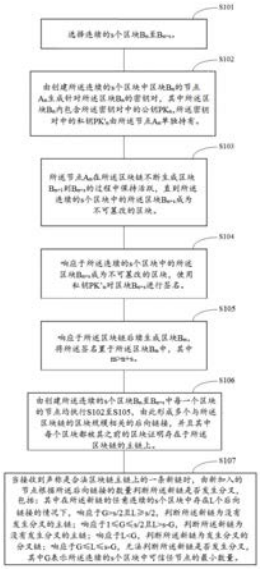
权利要求书4页 说明书16页 附图5页

(54)发明名称

用于防止区块链分叉的方法和设备

(57)摘要

本公开提供了一种防止区块链分叉的方法和设备。该方法包括:选择连续的s个区块B_n至B_{n+s};由创建区块B_n的节点A_n生成针对区块B_n的密钥对;节点A_n在区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃,直到连续的s个区块中的区块B_{n+s}成为不可篡改的区块;响应于连续的s个区块中的区块B_{n+s}成为不可篡改的区块,使用私钥PK'_n对区块B_{n+s}进行签名;响应于区块链后续生成区块B_m,将签名置于区块B_m中;由创建s个区块B_n至B_{n+s}中每一个区块的节点均执行以上步骤,由此形成多个与区块链的区块规模相关的后向链接;由新加入的用于创建新区块的节点根据后向链接的数量判断区块链是否发生分叉。



CN 111445247 B

1.一种防止区块链分叉的方法,其特征在于所述方法通过对所述区块链的每个区块建立后向链接并根据所述后向链接的数量进行判断实现,包括如下步骤:

S101,选择连续的s个区块B_n至B_{n+s};

S102,由创建所述连续的s个区块中区块B_n的节点A_n生成针对所述区块B_n的密钥对,其中所述区块B_n内包含所述密钥对中的公钥PK_n,所述密钥对中的私钥PK'_n由所述节点A_n单独持有;

S103,所述节点A_n在所述区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃,直到所述连续的s个区块中的所述区块B_{n+s}成为不可篡改的区块;

S104,响应于所述连续的s个区块中的所述区块B_{n+s}成为不可篡改的区块,使用私钥PK'_n对区块B_{n+s}进行签名;

S105,响应于所述区块链后续生成区块B_m,将所述签名置于所述区块B_m中,其中$m>n+s$;

S106,由创建所述连续的s个区块B_n至B_{n+s}中每一个区块的节点均执行S102至S105,由此形成多个与所述区块链的区块规模相关的后向链接,并且其中每个区块都被其之前的区块证明存在于所述区块链的主链上;

S107,当接收到声称是合法区块链主链上的一条新链时,由新加入的节点根据所述后向链接的数量判断所述新链是否发生分叉,包括:其中在所述新链的任意连续的s个区块中存在L个后向链接的情况下,响应于$G>s/2$且$L\geq s/2$,判断所述新链为没有发生分叉的主链;响应于$1\leq G\leq s/2$且$L>s-G$,判断所述新链为没有发生分叉的主链;响应于$L<G$,判断所述新链为发生分叉的分叉链;响应于$G\leq L\leq s-G$,无法判断所述新链是否发生分叉,其中G表示所述连续的s个区块中可信任节点的最小数量。

2.根据权利要求1所述的方法,其特征在于所述节点A_n使用且仅使用一次所述私钥PK'_n,对所述连续的s个区块B_n至B_{n+s}中每一个区块所生成的密钥对均为重新生成的。

3.根据权利要求1所述的方法,其特征在于所述公钥PK_n基于哈希签名算法生成,其中所述哈希签名算法包括Lamport算法。

4.根据权利要求1所述的方法,其特征在于还包括将所述签名置于所述区块链的所述区块B_{n+s}以外的其他位置,以确保在所述S105中能够将所述签名置于所述区块B_m中。

5.根据权利要求4所述的方法,其特征在于所述签名作为交易存放在所述区块链中。

6.根据权利要求4所述的方法,其特征在于将所述签名复制以获得复制签名,并将所述签名和所述复制签名均存储在所述区块链上。

7.根据权利要求1所述的方法,其特征在于在执行所述S105之前对所述签名的合法性进行检查,通过所述合法性检查的所述签名继续执行所述S105,而没有通过合法性检查的所述签名被所述区块链视为非法签名从而拒绝执行所述S105。

8.根据权利要求1所述的方法,其特征在于所述签名的过程在可信执行环境中执行。

9.根据权利要求1所述的方法,其特征在于所述区块链为公链。

10.根据权利要求1所述的方法,其特征在于所述区块链的创世区块是被完全信任的,其中由所述创世区块的节点或者所述创世区块授权的其他区块的节点对所述创世区块建立第一个后向链接,并且所述第一个后向链接出现后,在所述第一个后向链接所覆盖的所述连续的s个区块内产生分叉的概率为零。

11.根据权利要求1所述的方法,其特征在于在所述区块链的头部和尾部存在的区块量

较少的情况下,无法判断新区块是否为分叉链上的头部,所述方法包括:

在所述新区块处于最近的疑似分叉点所在位置,所述新区块之前的所有区块均处于主链上,而创建所述新区块的节点尚未形成完整的后向链接并置于区块链中的情况下,对所述新区块的后继区块中已经不可篡改的区块或区块序列进行短期签名,并将所述短期签名放置在一个或多个存储位置,从而当所述新区块的后续拥有后向链接的区块数量小于s的情况下,若所述短期签名不是即时的或者是过期的,采用所述短期签名替代所述后向链接进行判断;

响应于所述短期签名不存在或者过期,判断所述新区块位于分叉链上;或者

持续等待,直到通过执行所述方法的S101-S106从待判断的所述区块开始形成预定数量的所述后向链接,通过判断所述后向链接的数量是否满足S107的数值范围确定待判断的所述区块是否为分叉链上的头部。

12.根据权利要求1所述的方法,其特征在于还包括在所述区块链的主链以外的链上部分进行搜索,确认是否存在对所述后向链接进行重复签名的重复签名者,所述重复签名者表示对两个待生成的区块进行签名的多个节点,所述两个待生成的区块分别处于主链和分叉链上,从而根据所述重复签名者所创建的区块寻找分叉链。

13.根据权利要求1所述的方法,其特征在于针对疑似分叉链,将所述疑似分叉链之前的主链部分和所述疑似分叉链与所述主链交点后的链结构进行比较,其中所述主链包含所述后向链接,如果比较结果显示在所述后向链接的数量上存在显著差异,则确定所述疑似分叉链为分叉链,反之确定所述疑似分叉链为主链。

14.根据权利要求1所述的方法,其特征在于响应于所述S104使用私钥PK'_n对区块B_{n+s}进行签名,删除所述私钥PK'_n以防止其被滥用。

15.一种防止区块链分叉的设备,其特征在于包括区块链和处理器,其中所述区块链能够确保公布在其上的信息不可篡改,并且所述处理器用于:

选择连续的s个区块B_n至B_{n+s};

由创建所述连续的s个区块中区块B_n的节点A_n生成针对所述区块B_n的密钥对,其中所述区块B_n内包含所述密钥对中的公钥PK_n,所述密钥对中的私钥PK'_n由所述节点A_n单独持有;

所述节点A_n在所述区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃,直到所述连续的s个区块中的所述区块B_{n+s}成为不可篡改的区块;

响应于所述连续的s个区块中的所述区块B_{n+s}成为不可篡改的区块,使用私钥PK'_n对区块B_{n+s}进行签名;

响应于所述区块链后续生成区块B_m,将所述签名置于所述区块B_m中,其中$m>n+s$;

由创建所述连续的s个区块B_n至B_{n+s}中每一个区块的节点均执行前述过程,由此形成多个与所述区块链的区块规模相关的后向链接,并且其中每个区块都被其之前的区块证明存在于区块链的主链上;

当接收到声称是合法区块链主链上的一条新链时,由新加入的节点根据所述后向链接的数量判断所述新链是否发生分叉,包括:其中在所述新链的任意连续的s个区块中存在L个后向链接的情况下,响应于$G>s/2$且$L\geq s/2$,判断所述新链为没有发生分叉的主链;响应于$1\leq G\leq s/2$且$L>s-G$,判断所述新链为没有发生分叉的主链;响应于$L<G$,判断所述新链为发生分叉的分叉链;响应于$G\leq L\leq s-G$,无法判断所述新链是否发生分叉,其中G表示连续的

s个区块中可信任节点的最小数量。

16.根据权利要求15所述的设备，其特征在于所述节点A_n使用且仅使用一次所述私钥PK'_n，对所述连续的s个区块B_n至B_{n+s}中每一个区块所生成的密钥对均为重新生成的。

17.根据权利要求15所述的设备，其特征在于所述公钥PK_n基于哈希签名算法生成，其中所述哈希签名算法包括Lamport算法。

18.根据权利要求15所述的设备，其特征在于所述处理器还用于将所述签名置于所述区块链的所述区块B_{n+s}以外的其他位置，以确保响应于所述区块链后续生成区块B_m，能够将所述签名置于所述区块B_m中。

19.根据权利要求18所述的设备，其特征在于所述处理器用于将所述签名作为交易存放在所述区块链中。

20.根据权利要求18所述的设备，其特征在于所述处理器用于将所述签名复制以获得复制签名，并将所述签名和所述复制签名均存储在所述区块链上。

21.根据权利要求15所述的设备，其特征在于所述处理器还用于在响应于所述区块链后续生成区块B_m，将所述签名置于所述区块B_m中之前对所述签名的合法性进行检查，通过所述合法性检查的所述签名继续执行将所述签名置于所述区块B_m中，而没有通过合法性检查的所述签名被所述区块链视为非法签名从而拒绝执行将所述签名置于所述区块B_m中。

22.根据权利要求15所述的设备，其特征在于所述签名的过程在可信执行环境中执行。

23.根据权利要求15所述的设备，其特征在于所述区块链为公链。

24.根据权利要求15所述的设备，其特征在于所述区块链的创世区块是被完全信任的，创世区块的节点或者所述创世区块授权的其他区块的节点对所述创世区块建立第一个后向链接，并且所述第一个后向链接出现后，在所述第一个后向链接所覆盖的所述连续的s个区块内产生分叉的概率为零。

25.根据权利要求15所述的设备，其特征在于在所述区块链的头部和尾部存在的区块量较少的情况下，无法判断新区块是否为分叉链上的头部，所述处理器用于：

在所述新区块处于最近的疑似分叉点所在位置，所述新区块之前的所有区块均处于主链上，而创建所述新区块的节点尚未形成完整的后向链接并置于区块链中的情况下，对所述新区块的后继区块中已经不可篡改的区块或区块序列进行短期签名，并将所述短期签名放置在一个或多个存储位置，从而当所述新区块的后续拥有后向链接的区块数量小于s的情况下，若所述短期签名不是即时的或者是过期的，采用所述短期签名替代所述后向链接进行判断；

响应于所述短期签名不存在或者过期，判断所述新区块位于分叉链上；或者

持续等待，直到从待判断的所述区块开始形成预定数量的所述后向链接，通过判断所述后向链接的数量是否满足预定的数值范围确定待判断的所述区块是否为分叉链上的头部。

26.根据权利要求15所述的设备，其特征在于所述处理器还用于在所述区块链的主链以外的链上部分进行搜索，确认是否存在对所述后向链接进行重复签名的重复签名者，所述重复签名者表示对两个待生成的区块进行签名的多个节点，所述两个待生成的区块分别处于主链和分叉链上，从而根据所述重复签名者所创建的区块寻找分叉链。

27.根据权利要求15所述的设备，其特征在于所述处理器用于针对疑似分叉链，将所述

疑似分叉链之前的主链部分和所述疑似分叉链与所述主链交点后的链结构进行比较，其中所述主链包含所述后向链接，如果比较结果显示在所述后向链接的数量上存在显著差异，则确定所述疑似分叉链为分叉链，反之确定所述疑似分叉链为主链。

28.根据权利要求15所述的设备，其特征在于所述处理器用于响应于使用私钥PK'_n对区块B_{n+s}进行签名，删除所述私钥PK'_n以防止其被滥用。

29.一种机器可读存储介质，其上存储有计算机程序，其中所述计算机程序在由处理器执行时实现如权利要求1至14中任一项所述的防止区块链分叉的方法。

用于防止区块链分叉的方法和设备

技术领域

[0001] 本公开总体上涉及区块链技术领域，具体地涉及一种防止区块链分叉的方法和设备。

背景技术

[0002] 随着区块链技术的飞速发展，在设计上提出了很多创新点，主要集中在避免作恶以及共识机制方面。避免作恶基于经济博弈原理。在一个开放的网络中，无法通过技术手段来保证每个人都是合作的，但可以通过经济博弈来让合作者得到利益，让非合作者遭受损失和风险。例如，比特币网络中所有试图参与者都首先要付出挖矿的代价，进行算力的消耗，想拿到新区块的决定权与所抵押的算力成正比。一旦失败，这些算力将会被没收掉，成为沉没成本。当网络中存在众多参与者时，个体试图拿到新区块决定权要付出的算力成本是巨大的。虽然进行一次作恶所要付出的代价可能已经超过带来的好处，但是由于作恶收益也是相对升高的。因此，作恶的趋势和方式仍然会有增无减。

[0003] 此外，传统的共识问题是考虑在一个相对封闭的分布式系统中，允许同时存在正常节点、故障节点的情况下如何快速达成一致，从而继续区块链中区块的生成。而现有区块链所应用的环境大多是完全开放的，可能会面对各种攻击情况。同时基于互联网的网络质量只能保证尽可能配合区块链的应用而不能做到完全配合，从而导致问题更加复杂，使得传统的一致性算法在这种场景下难以使用。目前比较通用的POW(工作量证明)共识机制是基于概率、随时间逐步增强确认的公式，即，现有达成的结果在理论上有可能被推翻，只是攻击者要付出的代价会随时间指数级上升，被推翻的可能性随之指数级下降。

[0004] 区块链是一组区块，其中每个区块都包含其前所有区块的哈希运算值。哈希运算能将任意长度的明文串映射为较短的且通常为固定长度的二进制哈希串，并且不同的明文很难映射为相同的哈希值。区块链所采用的哈希算法在给定明文的情况下，可以在有限时间和有限资源内计算得到哈希值。然而，若给定若干哈希值，在有限时间内却很难，甚至可以说不可能逆推出明文。由于对原始输入信息的变化十分敏感，因此也很难找到两段内容不同的明文可以获得相同的哈希值，即，哈希运算具有抗碰撞性。这些属性直接导致合法主区块链上的每一区块最终向前溯源，均会指向创世区块。

[0005] 然而，由哈希链接支持的区块链结构在本质上并不是链状结构而是一个以区块链为根节点的树状结构。因此，作为合法区块链上的区块，从创世区块开始均会有一条确定数量的演变轨迹，除非创世区块本身还有一个与创世区块接近的区块。

[0006] 关于区块链的设计存在很多重要和有意义的假设。

[0007] 首先，对于树形结构的详细解释。如果存在两条区块链，在某一确定位置处存在的区块内容相同，且区块链的起点均为创世区块，则两条区块链从创世区块到交汇区块部分一定是相同的。该区块链被称为主链，在指定用户所建的DAG(有向无环图)中沿着子-父链接找到一个单链，可以把所有单元都关联在一起。从任意一个顶点开始，都可以构建一条主链。如果以相同的规则从两个不同的顶点开始选择主链，则这两条主链在回溯过程中一旦

相交，它们会在交点之后完全重合，重合部分被称为稳定主链，最不利的情况是两条主链在创世区块相交，所有的单元要么直接在这条稳定主链之上，要么从稳定主链上的单元沿着DAG的边缘通过少量的跳跃可以到达。因此，稳定主链可以在两个冲突的无序单元之间建立总序。

[0008] 其次，当区块链形成的序列中第n个位置的区块自身以及前n-1个位置处不会发生分叉时，定义该第n个区块为不可改变的或者不可篡改的。从区块链以外或者从单个节点的角度来看该区块链的结构，不可改变的部分只会单方向增长。然而，从单个节点所看到的不可改变的序列与从区块链以外部分所看到的不可改变的序列相同或者作为其前置的一部分。

[0009] 第三，在公链上任何人都能发布一个额外的节点，该节点指向有别于最后一个正确区块的其他区块。这种情况下分叉点与真实的头部接近，可以成为正常挖矿协议的一部分，并且有可能建议作为合法链的一个替代方案，从而在区块链生成过程中赢得替代的合法地位。这种情况并不是本发明所讨论的分叉。在实践中，区块链上允许包含一定量的坏节点或者非诚实节点、不可信任节点，其中这些节点可能不会遵守区块链协议，而这里的协议是指描述如何传输或交换数据(特别是在整个网络中)的正式规则集。然而，根据区块链协议的特性，这些坏节点也是挖矿集合中的一员，一旦其哈希值的范围因为符合协议要求而被选中，其自身就可以在任何时间发布区块。此时所发布的区块并未位于合法链上，而是从合法链的某一个位置衍生出来的分叉，此时所发布的区块属于“伪不可修改”。本发明正是从现有区块链机制的缺点出发，修改区块链的基本物理架构，将后向链接机制引入区块链，使得每次发布的新的被认为不可篡改的区块都可以确定无疑地“不可修改”，且任何可信节点都会信任该新区块内的信息的真实性。

[0010] 第四，每个区块都包含时间戳信息，现有区块的时间戳如果位于合法链上，则应当严格大于之前区块的时间戳信息，因为时间戳信息的生成极大程度上与区块发布的真实时间相关并相接近。对于挖矿速率我们期望存在上限和下限，也就是在一定时间间隔内限定产生区块的速率。这一假设例如可以通过区块链中诚实节点对时间或者时间戳采用合理准确的方式进行提醒，比如设置内部时钟，从而判断与时间相关的事件来避免分叉。

[0011] 第五，区块链按照开放对象范围的不同分为公链和联盟链。世界上任何个体或者团体都可以通过公链发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程。正是由于公链的访问门槛低，任何人都可以自由地加入和退出，参与者的身份隐藏但是所有数据都是默认公开的，因此存在分叉的风险更大。

[0012] 将区块链作为一个账本，每一段固定时间内，会随机挑选一个记账人记录该段时间的交易，将其置于区块链中形成“交易页”。当一段时间后，“交易页”形成账本上最新的一页。得益于区块链的数据结构设计，每一页“交易页”在记账人签名后，交易数据都不能被篡改。当后一张交易页确定后，前一张交易页的任意内容都不能被篡改。并且，按照当前的区块链数据结构，当前一交易页确定后，后一张交易页的内容和前一张交易页之间没有任何内容上的关联，只需要页码加1。每个拿到账本的人会查看页码顺序，如果正确就认为“交易页”组成的账本是合法的。然而，如果一组恶意的记账人，可以从账本中间的任意一页开始按照顺序伪造后面的每一页，则当一个新加入的区块创建者拿到这个伪造的账本时，伪造账本的页码顺序依然正确就会误认为是真实的账本。

[0013] 现有技术中采用在两个冲突单元之间建立总序的方式解决分叉问题。首先，给直接位于稳定主链上的单元做个索引，创世单元索引为0，创世单元的子单元索引为1，依此类推。沿着稳定主链给主链上的所有单元分配索引，对于不在稳定主链上的单元找到第一个直接或间接引用此单元的主链单元，这样就给每一个单元分配了一个MCI(主链索引)。然后，对于给定的两个单元，拥有较小MCI单元被认为是更早生成的。如果两个单元的MCI恰好相同并且存在冲突，则拥有较小哈希值的单元有效。主链构建过程实际上是最优父单元选择算法的递归调用过程。最优父单元通过比较可选路径中公证单元的数量(相同公证人发出的单元记一次)来选择，也就是可以通过页码顺序来校验“交易页”。公正单元由见证人发出，见证人是非匿名长期参与社区并拥有良好信誉的人，或是主动维护网络健康发展的组织。虽然期望他们诚实行事，但是完全信任任何一个见证人也是不合理的。因此也会选择不同的见证人，这种方法本身就给了坏节点联合作恶的机会。

[0014] 现有技术中区块链采用POW机制与此相关，POW机制相比其他挖矿协议的一个重要优势在于其可以防止分叉。根据前述对POW内部协议工作机制的描述，在奖励的驱使下，潜在的用户即使同时获得主链和作为分叉的作恶链的信息，其更愿意选择主链作为继续工作的基础。因此，POW机制下的最长链模型提供了最有效的安全理论，但是该安全理论仅在所有节点都可以且已经获知实际上没有分叉的合法链头部的存在，同时必须从区块链的头部开始对其后续的所有区块进行分析的前提下才能实施。换言之，目前的区块链架构下，当某个节点正在确定提出的头部是否是真实的还是存在于分叉链上的伪装的头部时，通常该节点采用如下方式：获得区块的整个生成的过程或者向周围节点(传输协议规定的连接节点)搜索区块链相关信息，以此为基础判断是否分叉；然而，由于网络中分布式系统的难以预测的变化，节点会暂时的从主链所在的存储部分断开或者受到恶意节点的攻击，后面过程的一些数据暂时无法读取，而跟随指针寻找的进程并未察觉到这一点，此时可能会给出关于是否在主链上继续生成区块的错误结论，后续会引起一系列错误的操作，在这种情况下检查指定的区块链是否为主链会存在不确定性。因此，需要提出对于以上方式的改进，即只以可以接收到的有限的区块链信息为基础进行判断，寻找数据信息的方式，从而在获得信息量有限的情况下或者在网络通信暂时失去或区块链受到恶意节点攻击的情况下，仍然能够获得比较确定的关于判断主链或分叉链的校验结果。

[0015] 针对现有技术中存在的公链协议POW的一些漏洞(即，挖矿模型的不甚完美)，区块链生成维护过程中搜索方式的缺陷以及现实世界中网络通信并不能做到完全支撑公链应用的实际情况，有必要提出一种新的区块链基本架构方式，即，不将安全性建立在从头部开始向上搜索的基础上，从而减少分叉的风险。

发明内容

[0016] 鉴于上述技术问题，本公开内容提出了一种防止区块链分叉的方法和设备。

[0017] 在本公开内容的一个方面，提供了一种防止区块链分叉的方法，用于防止将分叉链误判为主链从而导致主链不被接受，方法通过对区块链的每一个区块建立后向链接并对后向链接的数量进行判断实现，包括如下步骤：S101，选择连续的s个区块B_n至B_{n+s}；S102，由创建连续的s个区块中区块B_n的节点A_n生成针对区块B_n的密钥对，其中区块B_n内包含密钥对中的公钥PK_n，密钥对中的私钥PK'_n由节点A_n单独持有；S103，节点A_n在区块链不断生成区块

B_{n+1}到B_{n+s}的过程中保持活跃，直到连续的s个区块中的区块B_{n+s}成为不可篡改的区块；S104，响应于连续的s个区块中的区块B_{n+s}成为不可篡改的区块，使用私钥PK'_n对区块B_{n+s}进行签名；S105，响应于区块链后续生成区块B_m，将签名置于区块B_m中，其中m>n+s；S106，由创建连续的s个区块B_n至B_{n+s}中每一个区块的节点均执行S102至S105，由此形成多个与区块链的区块规模相关的后向链接，并且其中每个区块都被其之前的区块证明存在于区块链的主链上；S107，当接收到声称是合法区块链主链上的一条新链时，由新加入的节点根据后向链接的数量判断新链是否发生分叉，包括：其中在新链的任意连续的s个区块中存在L个后向链接的情况下，响应于G>s/2且L≥s/2，判断新链为没有发生分叉的主链；响应于1≤G≤s/2且L>s-G，判断新链为没有发生分叉的主链；响应于L<G，判断新链为发生分叉的分叉链；响应于G≤L≤s-G，无法判断新链是否发生分叉，其中G表示连续的s个区块中可信任节点的最小数量。

[0018] 在一些实施方式中，节点A_n使用且仅使用一次私钥PK'_n，对连续的s个区块B_n至B_{n+s}中每一个区块所生成的密钥对均为重新生成的。

[0019] 在一些实施方式中，公钥PK_n基于哈希签名算法生成，其中哈希签名算法包括Lamport算法。

[0020] 在一些实施方式中，还包括将签名置于区块链的区块B_{n+s}以外的其他位置，以确保在S105中能够将所述签名置于所述区块B_m中。

[0021] 在一些实施方式中，签名作为交易存放在区块链中。

[0022] 在一些实施方式中，将所述签名复制以获得复制签名，并将所述签名和所述复制签名均存储在区块链上。

[0023] 在一些实施方式中，执行S105前对签名的合法性进行检查，通过合法性检查的签名继续执行S105，没有通过合法性检查的签名被区块链视为非法签名而拒绝执行S105。

[0024] 在一些实施方式中，签名的过程在可信执行环境(TEE，Trusted Execution Environment)中执行。

[0025] 在一些实施方式中，区块链为公链。

[0026] 在一些实施方式中，区块链的创世区块是被完全信任的，其中由创世区块的节点或者创世区块授权的其他区块的节点对创世区块建立第一个后向链接，并且第一个后向链接出现后，在第一个后向链接所覆盖的连续的s个区块内产生分叉的概率为零。

[0027] 在一些实施方式中，在区块链的头部和尾部存在的区块量较少的情况下，无法判断新区块是否为分叉链上的头部，方法包括：在新区块处于最近的疑似分叉点所在位置，新区块之前的所有区块均处于主链上，而创建新区块的节点尚未形成完整的后向链接并置于区块链中的情况下，对新区块的后继区块中已经不可篡改的区块或区块序列进行短期签名，并将所述短期签名放置在一个或多个存储位置，从而当所述新区块的后续拥有后向链接的区块数量小于s的情况下，若所述短期签名不是即时的或者是过期的，采用所述短期签名替代所述后向链接进行判断；响应于所述短期签名不存在或者过期，判断所述新区块位于分叉链上；或者持续等待，直到通过执行方法的S101-S106从待判断的区块开始形成预定数量的后向链接，通过判断后向链接的数量是否满足S107的数值范围确定待判断的区块是否为分叉链上的头部。

[0028] 在一些实施方式中，在区块链的主链以外的链上部分进行搜索，确认是否存在对

后向链接进行重复签名的重复签名者，重复签名者表示对两个待生成的区块进行签名的多个节点，两个待生成的区块分别处于主链和分叉链上，从而根据重复签名者所创建的区块寻找分叉链。

[0029] 在一些实施方式中，针对疑似分叉链，将疑似分叉链之前的主链部分和疑似分叉链与主链交点后的链结构进行比较，其中主链包含后向链接，如果比较结果显示在后向链接的数量上存在显著差异，则确定疑似分叉链为分叉链，反之疑似分叉链确定为主链。

[0030] 在一些实施方式中，响应于S104使用私钥PK'_n对区块B_{n+s}进行签名，删除私钥PK'_n以防止其被滥用。

[0031] 在本公开内容的一个方面，提供了一种防止区块链分叉的设备，包括区块链和处理器，其中区块链能够确保公布在其上的信息不可篡改，处理器可以用于：选择连续的s个区块B_n至B_{n+s}；由创建连续的s个区块中区块B_n的节点A_n生成针对区块Bn的密钥对，其中区块B_n内包含密钥对中的公钥PK_n，密钥对中的私钥PK'_n由节点A_n单独持有；节点A_n在区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃，直到连续的s个区块中的区块B_{n+s}成为不可篡改的区块；响应于连续的s个区块中的区块B_{n+s}成为不可篡改的区块，使用私钥PK'_n对区块B_{n+s}进行签名；响应于区块链后续生成区块B_m，将签名置于区块B_m中，其中$m>n+s$；由创建连续的s个区块B_n至B_{n+s}中每一个区块的节点均执行上述过程(对应方法中的步骤S102到S105)，由此形成多个与区块链的区块规模相关的后向链接，并且其中每个区块都被其之前的区块证明存在于区块链的主链上；当接收到声称是合法区块链主链上的一条新链时，由新加入的节点根据后向链接的数量判断新链是否发生分叉，包括：其中在新链的任意连续的s个区块中存在L个后向链接的情况下，响应于$G>s/2$且$L\geq s/2$，判断新链为没有发生分叉的主链；响应于$1\leq G\leq s/2$且$L>s-G$，判断新链为没有发生分叉的主链；响应于$L<G$，判断新链为发生分叉的分叉链；响应于$G\leq L\leq s-G$，无法判断新链是否发生分叉，其中G表示连续的s个区块中可信任节点的最小数量。

[0032] 在一些实施方式中，所述节点A_n强制使用且仅使用一次所述私钥PK'_n，对连续的s个区块B_n至B_{n+s}中每一个区块所生成的密钥对均为重新生成的。

[0033] 在一些实施方式中，所述公钥PK_n基于哈希签名算法生成，其中哈希签名算法包括Lamport算法。

[0034] 在一些实施方式中，处理器还用于将签名放置在区块链的区块B_{n+s}以外的其他位置，以确保响应于所述区块链后续生成区块B_m能够将所述签名置于所述区块B_m中。

[0035] 在一些实施方式中，处理器用于将签名作为交易存放在区块链中。

[0036] 在一些实施方式中，处理器用于将签名复制以获得复制签名，并将签名和复制签名均存储在区块链上。

[0037] 在一些实施方式中，处理器还用于在响应于区块链后续生成区块B_m，将签名置于区块B_m中之前对签名的合法性进行检查，通过合法性检查的签名继续执行将签名置于所述区块B_m中，而没有通过合法性检查的签名被区块链视为非法签名从而拒绝执行将签名置于所述区块B_m中。

[0038] 在一些实施方式中，签名过程在可信执行环境中执行。

[0039] 在一些实施方式中，区块链为公链。

[0040] 在一些实施方式中，区块链的创世区块是被完全信任的，其中由创世区块的节点

或者创世区块授权的其他区块的节点对创世区块建立第一个后向链接，并且第一个后向链接出现后，在所述第一个后向链接所覆盖的连续的s个区块内产生分叉的概率为零。

[0041] 在一些实施方式中，在区块链的头部和尾部存在的区块量较少的情况下，无法判断新区块是否为分叉链上的头部，处理器用于：在新区块处于最近的疑似分叉点所在位置，新区块之前的所有区块均处于主链上，而创建新区块的节点尚未形成完整的后向链接并置于区块链中的情况下，对新区块的后继区块中已经不可篡改的区块或区块序列进行短期签名，并将所述短期签名放置在一个或多个存储位置，从而当所述新区块的后续拥有后向链接的区块数量小于s的情况下，若所述短期签名不是即时的或者是过期的，采用所述短期签名替代所述后向链接进行判断；响应于所述短期签名不存在或者过期，判断所述新区块位于分叉链上；或者持续等待，直到从待判断的区块开始形成预定数量的后向链接，通过判断后向链接的数量是否满足预定的数值范围确定待判断的区块是否为分叉链上的头部。

[0042] 在一些实施方式中，处理器还用于在区块链的主链以外的链上部分进行搜索，确认是否存在对后向链接进行重复签名的重复签名者，重复签名者表示对两个待生成的区块进行签名的多个节点，两个待生成的区块分别处于主链和分叉链上，从而根据重复签名者所创建的区块寻找分叉链。

[0043] 在一些实施方式中，处理器用于针对疑似分叉链，将疑似分叉链之前的主链部分和疑似分叉链与主链交点后的链结构进行比较，其中主链包含后向链接，如果比较结果显示在后向链接的数量上存在显著差异，则确定疑似分叉链为分叉链，反之确定疑似分叉链为主链。

[0044] 在一些实施方式中，处理器用于响应于使用私钥PK'_n对区块B_{n+s}进行签名，删除私钥PK'_n以防止其被滥用。

[0045] 在本公开内容的一个方面，还提供了一种机器可读存储介质，其上存储有计算机程序，其中所述计算机程序在由处理器执行时实现如上文所述的用于防止区块链分叉的方法。

[0046] 与现有技术相比，本公开内容的有益效果为：首先，本公开内容的技术方案是确保在仅获知创世区块信息的新用户仍然可以非常安全的加入到主链中并确保区块生成，这种安全加入的实现仅依靠区块链自身的状态，而不依赖区块链所在网络系统的性质。其次，由于依据本公开内容的技术方案，意欲产生分叉的坏节点在获知该公链新的协议方式的情况下，在经过博弈的考量下将放弃分叉的作恶。

附图说明

[0047] 在所附权利要求书中具体阐述了本发明的新颖特征。通过参考对在其中利用到本发明原理的说明性实施方式加以阐述的以下详细描述和附图，将会对本发明的特征和优点获得更好的理解。附图仅用于示出实施方式的目的，而并不应当认为是对本发明的限制。而且在整个附图中，用相同的附图标记表示相同的元素，在附图中：

[0048] 图1示出了依据本公开内容示例性实施方式的防止区块链分叉的方法流程图；

[0049] 图2示出了依据本公开内容示例性实施方式的单个后向链接示意图；

[0050] 图3示出了依据本公开内容示例性实施方式的加入后向链接机制下恶意节点可能的行为模式示意图；

[0051] 图4示出了依据本公开内容示例性实施方式的在区块链的头部和尾部存在的区块量较少的情况下无法依据常规方法判断新区块是否为分叉链上的头部时的状态图；

[0052] 图5示出了依据本公开内容示例性实施方式的在整个区块链上始终存在三种与后向链接相关的链接形式示意图；

[0053] 图6示出了依据本公开内容示例性实施方式的在不存在区块B_m的情况下无法依据常规方法判断新区块是否为分叉链上的头部时的状态图；

[0054] 图7示出了依据本公开内容示例性实施方式在区块B_{n+s}还没有成为不可篡改的区块的情况下无法依据常规方法判断新区块是否为分叉链上的头部时的状态图；

[0055] 图8示出了依据本公开内容示例性实施方式在区块B_n还没有形成的情况下无法依据常规方法判断新区块是否为分叉链上的头部时的状态图；

[0056] 图9示出了依据本公开内容示例性实施方式的后向链接机制形成后在区块链主链上同时存在完整后向链接、计算但未放置的链接(即区块B_m尚未出现的情况下)以及未使用的链接(即区块B_{n+s}未出现的情况下)的情况下所形成的后向链接模式示意图；以及

[0057] 图10示出了依据本公开内容示例性实施方式的防止区块链分叉的设备结构示意图。

具体实施方式

[0058] 下面将参照附图更详细地描述本公开内容的示例性实施方式。虽然附图中显示了本公开内容的示例性实施方式，然而应当理解，可以以各种形式实现本公开内容而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本公开内容，并且能够将本公开内容的范围完整地传达给本领域技术人员。在以下详细描述中没有任何内容旨在表明任何特定组件、特征或步骤对于本发明是必不可少的。本领域技术人员将会理解，在不脱离本公开内容的范围内各种特征或步骤可以彼此替代或结合。

[0059] 本实施方式所应用的区块链在任一时间都是由一系列区块构成，也就是说公链的格式是由一系列数值区块构成。本领域技术人员可以理解，对于区块的数目，可以采用本领域现在已知或者将来可知的任何方式中的区块数量定义，如几百万或者更多，本发明在此方面并不作出限制。

[0060] 图1示出了依据本公开内容示例性实施方式的防止区块链分叉的方法流程图。如图1所示，示出了一种用于防止区块链分叉的后向链接方法，该后向链接方法的提出基于如下对于区块链架构的假设。

[0061] 第一，每个人都知晓整条区块链由创世区块(此后定义该创世区块为B_0)确定和识别，包括其创世区块B_0的数值，而不是特定存储位置。

[0062] 第二，任一时间都会存在若干活跃节点的集合与所在的公链交互，所有活跃节点都具有目前比较可靠的签名方式，如密钥对的方式。并且假设其中大部分节点都是可信节点，对于协议这些可信节点应当会积极地响应和支持。

[0063] 第三，活跃节点集合中的所有节点都能够获知区块链头部及其附近发生的变化，除了刚刚成为活跃节点的部分，活跃节点集合中的其他好节点均知晓头部及其附近的变化。

[0064] 第四，随着多个区块成为不可篡改的区块，不可篡改的性质通知活跃节点集合中

的所有节点最终成为全网广播后的共识，活跃节点集合中的节点以及仅关注该主链而没有参与其中的用户都能被通知哪些区块成为不可篡改的区块，节点和用户之间也相互知晓对方已经获知上述信息。

[0065] 第五，节点可以自由地离开或者加入活跃节点，加入活跃节点的方式是必须知晓区块链头部的多个区块的数值，而加入的方式是本发明关注的重点，即如何确定加入时对应的是主链真实的头部。

[0066] 第六，一旦节点成功地识别了主链真实的头部信息，就会对节点附近的所有信息和活动变得熟悉，并且能够准确地跟随整条主链的发展。

[0067] 基于以上假设提出的构想试图在现有区块链已经保有传统的向下指向链接的情况下，将向上指向链接，也就是本发明的后向链接植入区块链中。然而，这种植入不能以改变区块链中已有区块为代价，这是不可取也不可能的。为此要设计一些精巧的机制，由生成在先区块的归属于同一集合的节点在没有任何关于该集合特征或者仅从区块链外部视角观测的情况下完成后向链接的植入。从较大程度上以前面所有节点的可信性角度来看这种做法并不是完全安全的，但是可以在概率基础上防止区块链分叉。

[0068] 该方法的实施是在一个正在开发的区块链环境中运行，具有以下属性的区块创建算法。

[0069] I.每个区块的创建者(矿工或节点)是通过一个过程选择的，在这个过程中，假设所选创建者为诚实创建者的概率至少为p，p为大于0.5的值。

[0070] II.已决定对一序列区块B_n(可能是所有区块)结合参数s使用以下后向链接协议，以便在后向链接协议的支持下有效地判断任何s个连续区块中的任意一个区块既不属于上述序列之一又是由诚实创建者创建的情况是否是不可能的(即这种情况发生的概率为负)。优选地，判断任何s个连续块中由诚实创建者创建的区块数量小于或等于总区块数量的一半的概率是否是负的，即是否是不可能的。

[0071] III.所有参与者都知晓所选以区块B_n为首的序列。

[0072] 基于以上内容，该方法包括如下步骤：S101，选择连续的s个区块B_n至B_{n+s}，根据区块链的基本假设，如果该连续区块均处于区块链的主链上，那么连续的s个区块中有超过50％的区块是由可信任节点创建，即创建连续的s个区块的所有节点中可信任节点的比例至少为p，而不信任节点的比例为q，其中q＝1-p，p，q的数值唯一且p>q；考虑区块B_n至B_{n+s}在两者之间创建一个链接，在该链接下，B_n实际上证明了B_{n+s}，并通过传统的区块链链接证明了$B_{n+1}\cdots B_{n+s-1}$中的每一个区块。将创建B_n的节点命名为A_n；S102，由创建连续的s个区块中区块B_n的节点A_n生成针对区块B_n的密钥对，其中区块B_n内包含密钥对中的公钥PK_n，密钥对中的私钥PK'_n由节点A_n单独持有；S103，节点A_n在区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃，即节点一直参与区块链的建设，不会成为僵尸节点，直到连续的s个区块中的区块B_{n+s}成为不可篡改的区块；S104，响应于连续的s个区块中的区块B_{n+s}成为不可篡改的区块，使用私钥PK'_n对区块B_{n+s}进行签名；S105，响应于区块链后续生成区块B_m，将签名放置在区块B_m内，其中m>n+s；S106，当对连续的s个区块中每个区块，其生成节点都完成上述步骤时，由此形成多个与区块链的区块规模相关的后向链接；由于签名由节点A_n生成区块B_n的密钥对中私钥对区块B_{n+s}进行签名获得，因此，对于区块B_m的访问过程实际上包含了从区块B_n到区块B_{n+s}的链接的验证，从而确保区块链的生长过程是在主链上进行的，并且每个区块都被较早的

区块证明;S107,当接收到声称是合法区块链的主链上新链时,由新加入的节点根据后向链接的模式和数量判断区块链是否发生分叉。所谓后向链接的模式,即通过步骤S101-S105的循环实现的后向链接的特定链接形式,并且本领域技术人员应当熟知,根据区块链现有的架构,在进行新区块是否属于区块链分叉链头部的判断之前,首先需要判断新区块是否属于合法区块链,如果不属于该条合法区块链上的区块,就没有必要进行后续的判断了。所谓合法区块链,其包含同一区块链上衍生的主链和分叉链,如果新区块不属于合法区块链,那么对于区分其处于主链还是分叉链上是没有意义的。本实施方式对此的判断方式根据区块链所具有的如下结构特点进行:包含交易信息的区块从后向前有序链接起来的数据结构形成区块链,每个区块都指向前一个区块,而每个区块头都包含它的前一区块哈希值,这样创建了一条一直可以追溯到第一个区块(创世区块)的链条。根据该树状结构特点,通过判断该新区块是否通过传统的区块链链接最终指向区块链的创世区块来确定该新区块是否位于一条合法区块链上,如果是,则新区块位于合法区块链上,反之则不属于该合法区块链上。当然,本领域技术人员还可以通过现有技术中其他合理的符合区块链架构特点的方式对此进行判断。

[0073] 对于位于合法区块链上的区块,通过判断后向链接的数量进一步判定其是否位于分叉链上,包括:其中新链的任意连续的s个区块中存在L个后向链接的情况下,响应于G>s/2,且仅当L≥s/2,判断区块链为没有发生分叉的主链;响应于1≤G≤s/2,且仅当L>s-G,判断区块链为没有发生分叉的主链;响应于L<G,判断区块链为发生分叉的分叉链;响应于G≤L≤s-G,无法判断是否发生分叉,还需要其他类型的证据进行判断,其中G表示连续的s个区块中可信任节点的最小数量。

[0074] 根据以上方法形成的单个后向链接示意图如图2所示,图2为了清晰起见,仅示出了间距较小的三个节点之间所包含的后向链接关系,这种后向链接减少或者消除了以往所需的密钥量。

[0075] 在一些实施方式中,节点A_n使用且仅使用一次私钥PK'_n,对s个区块B_n至B_{n+s}中每一个区块所生成的密钥对均为重新生成的。

[0076] 在一些实施方式中,公钥基于哈希签名算法生成,哈希签名算法包括Lamport算法。

[0077] 在一些实施方式中,还包括将签名放置在区块链的区块B_{n+s}以外的其他位置,以确保在S105中能够将签名置于区块B_m中。

[0078] 在一些实施方式中,签名作为交易存放在区块链中。由于将签名进行了“变形”形成交易放在区块链上,现有机制无法确保这种作为签名的交易一定会和其他普通交易数据一起在相同的时间量值范围内成为不可篡改的,如果没有一定的延时机制保证,该交易有可能会被丢弃,因此通常会配合一定的延时机制使用。

[0079] 在一些实施方式中,将签名复制以获得复制签名,并将签名和复制签名均存储在区块链上。

[0080] 在一些实施方式中,执行S105前对签名的合法性进行检查,通过合法性检查的签名继续执行S105,没有通过合法性检查的签名被区块链作为非法签名而拒绝执行S105。

[0081] 对于S104的执行,动用私钥对交易区块签名是唯一的安全屏障,这里没有服务器端的安全保障。签名只是一种控制手段。如果不把签名过程纳入TEE飞地环境中执行,无异

于毫无系统安全性。因此，整个方法的实施确保是在可信执行环境中进行，以构造一种安全的飞地环境，从而可以在可信计算领域提供可信根，对驻留的程序与数据提供安全保障。存放在TEE中的私钥，甚至于本发明所涉及方法的程序能做到永远不泄露到飞地之外或无法导出被用于破解分析，从而执行过程(尤其调用输入输出时)也有安全保障。由于破解驻留在TEE中的程序通常被认为是很困难的，因此可以选择使用TEE设备固定厂商号与序列号，以便唯一标识此设备。

[0082] 在一些实施方式中，区块链为公链。

[0083] 在一些实施方式中，区块链的创世区块是被完全信任的，其中由创世区块的节点或者创世区块授权的其他区块的节点对创世区块建立第一个后向链接，并且第一个后向链接出现后，在第一个后向链接所覆盖的连续的s个区块内产生分叉的概率为零，这是因为对于任意一个在B_0到B_s内的区块，新节点首先通过从B_s开始追溯父区块哈希确定能追溯到B_0，然后因为B_0的后向链接唯一证明了B_s是自己的合法后继区块，因此唯一确定了区块B_0到B_s在主链上。

[0084] 在一些实施方式中，在区块链的头部和尾部存在的区块量较少的情况下无法判断新区块是否为分叉链上的头部时，该方法包括：第一种方式，新区块处于最近的疑似分叉点所在位置，新区块之前的所有区块均处于主链上，而创建新区块的节点尚未形成完整的后向链接并置于区块链中，对新区块的后继区块中已经不可篡改的区块或区块序列进行短期签名，并将所述短期签名放置在一个或多个存储位置，从而当所述新区块的后续拥有后向链接的区块数量小于s的情况下，若所述短期签名不是即时的或者是过期的，采用所述短期签名替代所述后向链接进行判断；响应于所述短期签名不存在或者过期，判断所述新区块位于分叉链上；或者第二种方式，持续等待，直到从待判断的区块开始形成足够数量的后向链接，数量可以根据区块链的应用场景灵活进行定义，该数量会根据区块链的实际应用场景确定，其规模量通常为几百甚至更多。对于第一种方式，本实施方式的具体实施方式为：假定B_i是我们能确认的最近的疑似分叉点，亦即该区块的所有前置区块都在主链上。该区块之前的区块创建节点$A_j(i-j\leqslant s)$尚未将其后向链接置于区块链中，协议要求这些节点继续关注区块链的增长，对其后继的区块中已经不可篡改的区块或区块序列进行短期签名，并将短期签名放置在某些存储位置(例如交易池)中。由此扩展上述方法，当B_i的后续区块数少于s个时，如果短期签名不是即时的或者是过期的，就可以用短期签名替代原后向链接进行判断。如果反之这些短期签名不存在或者过期，就可以判断B_i位于分叉链上。确定的存储位置可以为交易池，在搜索后向链接的同时在交易池中寻找区块是否已经成为主链上不可篡改的区块的线索，交易池中存储有经过签名的短期签名信息，短期签名信息为未提供后向链接的节点提供的认定区块链头部位置的确认信息，通过访问交易池中的短期签名信息对区块是否为分叉链上的头部进行判断。本实施方式例如可以通过统计短期签名中所包含的投票信息来判断该区块是否为区块链主链上的区块，如果超过50％的短期签名中所包含的投票信息确定该区块为主链上的区块，则认定该新区块为主链上的区块并接受；否则，确定新区块为分叉链上的区块。这样设置的目的在于尝试寻找更多关于新区块是否为分叉链头部的证据作为补充，重复签名者会采用一个公钥签两个区块，从而暴露了自己的身份的同时暴露了自己在分叉链上所生成的新区块，而该新区块反之会反映分叉链的位置所在。

[0085] 参见图4，区块链上包含主链上的不可篡改的区块41，具有非法双链接的区块42，分叉链上没有链接的区块43以及分叉链上具有链接的区块44，大部分的不可篡改的区块41形成完整的后向链接45，然而仍有部分靠近头部区块只是完成了密钥对的形成以及部分签名的形成，经过运算后仍然没有达到进行第二次签名，即步骤S105的时间节点，从而形成经过计算但还未放置的链接46；甚至一些更靠近头部的区块还未形成可用链接，即形成不可用链接47。那些靠近头部的区块，无论是在分叉链还是在主链上，均称为临时区块48。

[0086] 图5至图8对图4中所出现的两种情况分别进行了详细的图解说明。

[0087] 图5中，在整个区块链上始终存在三种与后向链接相关的链接形式：即完整后向链接45，计算但未放置的链接46以及未使用的链接47。

[0088] 图6中描述了方法仅执行到步骤S104的情况，即B_n到B_{n+s}的区块均已经形成，但B_{n+s}之后的区块都没有生成，或者仅生成了若干个区块，还未生成区块B_m，此时区块链同时处于两个状态下：即状态61，公钥材料位于B_n中；以及状态62，该阶段签名/链接还处于区块链外部，尚未对该签名经过检查，因此执行第一种方法下的短期签名校验方式，此时短期签名可能位于交易池内。当然也可以采用第二种等待的方式。

[0089] 图7中描述了方法仅执行到步骤S102的情况，即B_n到B_{n+s}的区块均已经形成，但B_{n+s}还没有成为不可篡改的区块，也就是更未生成区块B_m，此时区块链同时处于三个状态下：即状态71，当前区块B_n成为不可篡改的区块；状态72，区块B_n中的公钥不可使用；以及状态73，B_{n+s}生成，但是还未形成不可篡改的区块，从而后向链接还未形成可用的后向链接。实际上图7对应的状态是图6对应状态的前一个时间节点下的状态。因此仍然需要执行第一种方法下的短期签名校验方式，此时短期签名可能位于交易池内。当然也可以采用第二种等待的方式。

[0090] 图8中描述了方法仅执行到步骤S101的情况，即B_n还未生成，此时在B_n到B_{n+s}的状态不存在不可篡改的区块，也就是更未生成区块B_m，此时区块链同时处于两个状态下：即状态81，当前区块B_n还未生成；以及状态82，公钥材料未形成，密钥对也未形成，此时也没有可以使用的后向链接。实际上图8对应的状态是图7对应状态的更早的一个时间节点下的状态。因此仍然需要执行第一种方法下的短期签名校验方式，此时短期签名可能位于交易池内。当然也可以采用第二种等待的方式。

[0091] 图9所示为后向链接机制形成后在区块链主链上同时存在完整后向链接45，计算但未放置的链接46(即区块B_m尚未出现的情况下)以及未使用的链接47(即区块B_{n+s}未出现的情况下)的情况下所形成的后向链接模式。其中，在选定的s个区块序列中每个区块上以及此后生成的主链上的区块上均存在公钥材料，即每个区块的创建者均生成了相应的密钥对。换言之，仅在第一次执行S105时形成的B_m(本实施方式中为第6个区块)及其之后主链上的区块上存在完整的后向链接部分(采用实线箭头表示)，该区块链结构中还存在未经检查而放置的签名(图中采用虚线箭头指示)。这种情况下可以执行第一种方法下的短期签名校验方式，此时短期签名可能位于交易池内。当然也可以采用第二种等待的方式。

[0092] 在一些实施方式中，还包括在主链以外的链上部分进行搜索，确认是否存在对后向链接进行重复签名的重复签名者，重复签名者表示对两个要生成的区块进行签名的多个节点，两个要生成的区块分别处于主链和分叉上，从而根据重复签名者所生成的区块寻找分叉。

[0093] 在一些实施方式中，对疑似分叉链，通过比较疑似分叉链之前的主链和疑似分叉链交点后由后向链接形成的链结构，如果疑似分叉链之前的主链和疑似分叉链的其中一条在交点后链的后向链接形成的链结构存在显著差异，则确定疑似分叉链为分叉链，反之确定为主链。具体的一种方式为：针对疑似分叉链，将疑似分叉链之前的主链部分和疑似分叉链与主链交点后的链结构进行比较，其中主链包含后向链接，如果比较结果显示在后向链接的数量上存在显著差异，则确定疑似分叉链为分叉链，反之疑似分叉链确定为主链。当然，本领域技术人员也可以不必计算具体的后向链接数量以节约计算资源，仅通过链结构上后向链接数据规模的直观比较完成。

[0094] 在一些实施方式中，响应于使用私钥PK'_n对区块B_{n+s}进行签名，删除私钥PK'_n以防止其被滥用。

[0095] 将后向链接机制嵌入区块链中后，我们对其中一个区块(定义为区块B)进行测试，测试的内容为算法逻辑执行情况，算法的逻辑包括：(1)所有哈希指针回溯到各自的根节点，也就是创世区块B_0，如果没有回溯到创世区块，则区块B确定不是区块链的一部分；(2)对于外部确定的常数r和s，设定区块B处于第m级，则对于区块B_{n+s}($n+s<m-r$)，使用与包含在区块B_n中的公钥对应的私钥对区块B_{n+s}签名，其中常数r的含义为至少等待r个区块，签名才能被包含在后续的区块中，这里的r的数值范围由区块链涉及的所有包含在内的节点根据区块的生成速度、交易的打包速度等因素提前约定，例如为20个区块之内必须生成确定的后向链接，从而确定后向链接判断时的块生成范围，并完成后向链接的校验，提高方法的可操作性。

[0096] 算法的两个逻辑也是校验的逻辑，如果两个校验的逻辑中至少一个没有通过，那么在协议遵守从创世区块开始的主链的假设下，校验者(也就是对应的节点)就可以确定区块B并不是主链的一部分。

[0097] 该方法具备完备的安全性，防止分叉的产生。上述实施方式中区块的顺序产生依次为B_n，B_{n+s}以及B_m，从而明确了后向链接的实际物理含义，即区块B_n中的公钥对应的私钥对区块B_{n+s}的签名揭示了两者独特真实的继承关系，而后向链接实际包含在区块B_{n+s}之后的r个区块内，从而揭示与时间戳相关的假设，确保检验的真实性和确定性。从而，根据后向链接的生成规则，以当前区块前r处的区块为界，之前生成的区块链可以保证没有分叉。

[0098] 该方法执行的前提是在区块链中心部分的每个连续区块对上应当有s个独立的后向链接覆盖，但是在区块链头部和尾部的位置这种情况却由于前向和后向区块数量的不足呈现不同的样貌，此时容易发生短分叉(short fork)现象。

[0099] 同样地，在区块链的初始部分，存在的区块数量小于s的情况下，根本无法启动后向链接机制，当然同样在s较小的情况下也无法制造长分叉(long fork)。

[0100] 对于以上两种情况，在一些实施方式中，区块链的头部和尾部存在的区块量较少的情况下，一种方法是在判断区块是否为分叉链上的头部时持续等待，直到从待判断的区块开始形成足够数量的后向链接，另一种方法是在区块搜索后向链接的同时在交易池中寻找区块是否为主链上的区块线索，交易池中存储的信息是未提供后向链接的多个节点所提供的关于其认定区块链头部位置所在的经过签名的复制信息，通过交易池访问这些复制信息进行判断而无需将复制信息存储在链上，签名也无需为长期签名。

[0101] 再次参见图3，特别是在s的取值较小的情况下，坏节点控制了足够多的已经被挖

矿的区块，使得在主链和分叉链之间进行区分更为困难。因此，在创世区块中对于相关操作涉及的区块数量也需要根据系统应用的需求进行设定。按照通用规则，假定后向链接检测协议设定在每s个连续区块中，至少具有L个期望的签名，形成L条后向链接才可以将该区块链认定为官方链或者主链。如果对L没有适当的取值范围限定，会出现如下两种情况：(1)假阳性：协议将分叉错误的认定为官方链或主链；(2)假阴性：由于攻击者试图限制签名的数量小于L，因此没有形成L条后向链接，从而协议拒绝接受真实的官方链或主链。

[0102] 通过选择L的取值范围可以避免以上两种情况同时出现。假设提供签名的诚实节点一定会在协议限定的时刻尽快提供签名，并且所提供的签名立即被区块链接受，这一假设存在的基础在于常数r的选择足够大，至少会有一个诚实矿工会遵守协议，将签名包含在区块中。设定s个连续区块中诚实节点的最小数量为G，如果L>G，并且如果没有坏矿工提供任何签名，则根据协议就会发生假阴性的情况。如果L小于或者等于坏矿工的最大数量s-G，则根据协议就会极易发生坏矿工生成分叉的情况，继而发生假阳性的情况，因此L的取值范围应当介于s-G和G之间，即$s-G<L\leqslant G$，且$G>s/2$。

[0103] 对于非诚实节点或坏节点发动攻击存在一个典型的博弈过程，首先这些节点需要明确s个连续区块中自身的比例，并且互相知晓对方的存在并达成合作，在不提供签名而造成矿工费或者押金损失之前就可以判断分叉的成功概率。并且这些坏节点也可以伪造时间戳，使得诚实节点无法察觉到分叉的节点直到广播到全网。正是由于博弈的存在，对于攻击者来说也存在两难的处境，一方面正常参与主链的生成和发展可以获得预期的收入，而同时又需要伪装自己伺机分叉，在其应当公布签名而不公布之时，除了在经济上的损失之外，实际上也暴露了自己可能成为非诚实节点的概率和身份，这样在分叉行为发生之前就可能会被发现并导致失败，非诚实节点作恶的动机丧失，从而将非诚实节点向在公有链上不作恶的方向推动。此外，该防御机制主要用于防止长的分叉，参与者有更长的时间组织防御和施加惩罚，若所选择的s较大，则需要确保s个区块是否在主链上等候的时间就会更长，矿工所需要花费的等待时间更长，然而在无需更多签名次数，即仍然是一个矿工提供一份签名的前提下，相对于为区块链带来的防止分叉的安全性相比，这仍然是值得的。

[0104] 在一些实施方式中，通过搜索其他链寻找后向链接的重复签名者，即对两个要生成的区块进行签名的多个节点，从而寻找分叉。

[0105] 在一些实施方式中，对一小部分(根据区块链的应用场景，这一部分通常为数个或数十个不等)不确定是官方链的疑似分叉链，通过比较两条链交点后的链的构成，如果两条链的其中一条在交点后链的构成存在巨大差异，可以确定为分叉链，反之可以确定为官方链(即，主链)。

[0106] 图10示出了依据本公开内容示例性实施方式的防止区块链分叉的设备的结构示意图。如图10所示，该防止区块链分叉的设备包括区块链1001和处理器1002，其中区块链1001能够确保公布在其上的信息不可篡改，众所周知区块链是将数据以一系列区块的方式按时间顺序相连形成的一种链式数据结构，并且还是以密码学方式保证数据的不可篡改和不可伪造的分布式账本。区块链利用诸如哈希和签名等加密技术以及共识算法建立信任机制，让抵赖、篡改和欺诈行为的成本巨大，保证了数据的不可篡改和不可伪造。可以认识到，区块链可以采用本领域现在已知或者将来可知的任何方式来实现，例如比特币、以太坊等等。处理器1002可以用于：

[0107] 选择连续的s个区块B_n至B_{n+s}，根据区块链的基本假设，如果该连续区块均处于区块链的主链上，那么连续的s个区块中有超过50％的区块是由可信任节点创建，即创建连续的s个区块的所有节点中可信任节点的比例至少为p，而不信任节点的比例为q，其中q＝1-p，p，q的数值唯一且p>q；考虑区块B_n至B_{n+s}在两者之间创建一个链接，在该链接下，B_n实际上证明了B_{n+s}，并通过传统的区块链链接证明了$B_{n+1}\cdots B_{n+s-1}$中的每一个区块。将创建B_n的节点命名为A_n；由创建连续的s个区块中区块B_n的节点A_n生成针对区块B_n的密钥对，其中区块B_n内包含密钥对中的公钥PK_n，密钥对中的私钥PK'_n由节点A_n单独持有；节点A_n在区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃，即节点一直参与区块链的建设，不会成为僵尸节点，直到连续的s个区块中的区块B_{n+s}成为不可篡改的区块；响应于连续的s个区块中的区块B_{n+s}成为不可篡改的区块，使用私钥PK'_n对区块B_{n+s}进行签名；响应于区块链后续生成区块B_m，将签名放置在区块B_m内，当对连续的s个区块中每个区块，其生成节点都完成上述步骤时，由此形成多个与区块链的区块规模相关的后向链接，其中m>n+s；由于签名由节点A_n生成区块B_n的密钥对中私钥对区块B_{n+s}进行签名获得，因此，对于区块B_m的访问过程实际上包含了从区块B_n到区块B_{n+s}的链接的验证，从而确保区块链的生长过程是在主链上进行的，并且每个区块都被较早的区块证明；当接收到声称是在合法区块链的主链上的新链时，由新加入的节点根据后向链接的模式和数量判断区块链是否发生分叉。所谓后向链接的模式，即通过此前所实施步骤的循环实现的后向链接的特定链接形式，并且本领域技术人员应当熟知，根据区块链现有的架构，在进行新区块是否属于区块链分叉链头部的判断之前，首先需要判断新区块是否属于合法区块链，如果不属于该条合法区块链上的区块，就没有必要进行后续的判断了。本实施方式对此的判断方式根据区块链所具有的如下结构特点进行：包含交易信息的区块从后向前有序链接起来的数据结构形成区块链，每个区块都指向前一个区块，而每个区块头都包含它的前一区块哈希值，这样创建了一条一直可以追溯到第一个区块(创世区块)的链条。根据该树状结构特点，可以通过判断该新区块是否能够通过传统的区块链链接最终指向该区块链的创世区块来确定该新区块是否位于一条合法区块链上，即，当前区块链结构是否满足基本的树状结构特点。当然，本领域技术人员还可以通过现有技术中其他合理的符合区块链架构特点的方式对此进行判断。

[0108] 对于位于合法区块链上的新链，通过判断后向链接的数量进一步判定其是否位于分叉链上，包括：其中在新链的任意连续的s个区块中存在L个后向链接的情况下，响应于G>s/2，且仅当L≥s/2，判断区块链为没有发生分叉的主链；响应于1≤G≤s/2，且仅当L>s-G，判断区块链为没有发生分叉的主链；响应于L<G，判断区块链为发生分叉的分叉链；响应于G≤L≤s-G，无法判断是否发生分叉，还需要其他类型的证据进行判断，其中G表示连续的s个区块中可信任节点的最小数量。

[0109] 在一些实施方式中，节点A_n使用且仅使用一次私钥PK'_n，对s个区块B_n至B_{n+s}中每一个区块所生成的密钥对均为重新生成的。

[0110] 在一些实施方式中，公钥基于哈希签名算法生成，哈希签名算法包括仅能使用私钥进行一次签名的Lamport算法。

[0111] 在一些实施方式中，处理器1002还用于将签名放置在区块链的区块B_{n+s}以外的其他位置，以确保响应于区块链后续生成区块B_m，能够将签名置于区块B_m中。

[0112] 在一些实施方式中，处理器1002用于将签名作为交易存放在区块链中。

[0113] 在一些实施方式中，处理器1002用于将签名复制以获得复制签名，并将签名和复制签名均存储在区块链上。

[0114] 在一些实施方式中，处理器1002用于响应于连续的s个区块中的区块B_{n+s}成为不可篡改的区块，使用私钥PK'_n对区块B_{n+s}进行签名前对签名的合法性进行检查，通过合法性检查的签名继续执行将签名置于区块B_m中，没有通过合法性检查的签名被区块链作为非法签名而拒绝执行将签名置于区块B_m中。

[0115] 在一些实施方式中，签名的过程在可信执行环境中执行。

[0116] 在一些实施方式中，区块链为公链。

[0117] 在一些实施方式中，区块链的创世区块是被完全信任的，其中由创世区块的节点或者创世区块授权的其他区块的节点对创世区块建立第一个后向链接，并且第一个后向链接出现后，在第一个后向链接所覆盖的连续的s个区块内产生分叉的概率为零，这是因为对于任意一个在B_0到B_s内的区块，新节点首先通过从B_s开始追溯父区块哈希确定能追溯到B_0，然后因为B_0的后向链接唯一证明了B_s是自己的合法后继区块，因此唯一确定了区块B_0到B_s在主链上。

[0118] 在一些实施方式中，在区块链的头部和尾部存在的区块量较少的情况下无法判断新区块是否为分叉链上的头部时，处理器1002用于实施：第一种方法，新区块处于最近的疑似分叉点所在位置，新区块之前的所有区块均处于主链上，而创建新区块的节点尚未形成完整的后向链接并置于区块链中，对新区块的后继区块中已经不可篡改的区块或区块序列进行短期签名，并将所述短期签名放置在一个或多个存储位置，从而当所述新区块的后续拥有后向链接的区块数量小于s的情况下，若所述短期签名不是即时的或者是过期的，采用所述短期签名替代所述后向链接进行判断；响应于所述短期签名不存在或者过期，判断所述新区块位于分叉链上；响应于短期签名不存在或者过期，判断新区块位于分叉链上；或者第二种方法，持续等待，直到从待判断的区块开始形成足够数量的后向链接，数量可以根据区块链的应用场景灵活进行定义，该数量会根据区块链的实际应用场景确定，其规模量通常为几百甚至更多。对于第一种方式，本实施方式的具体实施方式为：假定B_i是我们能确认的最近的疑似分叉点，亦即该区块的所有前置区块都在主链上。该区块之前的区块创建节点$A_j(i-j\leqslant s)$尚未将其后向链接置于区块链中，协议要求这些节点继续关注区块链的增长，对其后继的区块中已经不可篡改的区块或区块序列进行短期签名，并将短期签名放置在某些存储位置(例如交易池)中。由此扩展上述方法，当B_i的后续区块数少于s个时，如果短期签名不是即时的或者是过期的，就可以用短期签名替代原后向链接进行判断。如果反之这些短期签名不存在或者过期，就可以判断B_i位于分叉链上。确定的存储位置可以为交易池，在搜索后向链接的同时在交易池中寻找区块是否已经成为主链上不可篡改的区块的线索，交易池中存储有经过签名的短期签名信息，短期签名信息为未提供后向链接的节点提供的认定区块链头部位置的确认信息，通过访问交易池中的短期签名信息对区块是否为分叉链上的头部进行判断。本实施方式例如可以通过统计短期签名中所包含的投票信息来判断该区块是否为区块链主链上的区块，如果超过50％的短期签名中所包含的投票信息确定该区块为主链上的区块，则认定该新区块为主链上的区块并接受；否则，确定新区块为分叉链上的区块。这样设置的目的在于尝试寻找更多关于新区块是否为分叉链头部的证据作为补充，重复签名者会采用一个公钥签两个区块，从而暴露了自己的身份的同时暴露了自

己在分叉链上所生成的新区块，而该新区块反之会反映分叉链的位置所在。

[0119] 在一些实施方式中，处理器1002还用于在主链以外的链上部分进行搜索，确认是否存在对后向链接进行重复签名的重复签名者，重复签名者表示对两个待生成的区块进行签名的多个节点，两个待生成的区块分别处于主链和分叉链上，从而根据重复签名者所生成的区块寻找分叉链。

[0120] 在一些实施方式中，处理器1002用于针对疑似分叉链，将疑似分叉链之前的主链部分和疑似分叉链与主链交点后的链结构进行比较，其中主链包含后向链接，如果比较结果显示在后向链接的数量上存在显著差异，则确定疑似分叉链为分叉链，反之疑似分叉链确定为主链。

[0121] 在一些实施方式中，处理器1002用于响应于使用私钥PK'_n对区块B_{n+s}进行签名，删除私钥PK'_n以防止其被滥用。

[0122] 由此，该方法保证区块链的前方交易页对后面的交易页产生限制。由于该机制中区块数量选择足够大，因此满足区块链的基本假设前提，即恶意的记账人占少数，所以后端能迁移到伪造账本上的链接绳的数量是少数的，因此不能通过方法中对后向链接数量的校验，也就不能成功伪造分叉。

[0123] 在本公开内容的一个方面，还提供了一种机器可读存储介质，该机器可读存储介质上存储有计算机程序，其中计算机程序在由处理器执行时实现上文所描述的防止区块链分叉的方法。对于防止区块链分叉的方法的技术方案，在上文已经进行了详细描述，在此不再赘述。在一些实施方式中，机器可读存储介质是数字处理设备的有形组件。在另一些实施方式中，机器可读存储介质可选地是可从数字处理设备移除的。在一些实施方式中，举非限制性示例而言，机器可读存储介质可以包括U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、闪速存储器、可编程只读存储器(PROM)、可擦除可编程只读存储器(EPROM)、固态存储器、磁碟、光盘、云计算系统或服务等。

[0124] 应当理解，本公开内容的方法实施方式中记载的各个步骤可以按照不同的顺序执行，和/或并行执行。此外，方法实施方式可以包括附加的步骤和/或省略执行示出的步骤。本发明的范围在此方面不受限制。

[0125] 在本文所提供的说明书中，说明了大量具体细节。然而，应当理解，本公开内容的实施方式可以在没有这些具体细节的情况下实践。在一些实施方式中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0126] 虽然本文已经示出和描述了本发明的示例性实施方式，但对于本领域技术人员容易理解的是，这样的实施方式只是以示例的方式提供的。本领域技术人员现将会在不偏离本发明的情况下想到许多更改、改变和替代。应当理解，在实践本发明的过程中可以采用对本文所描述的本发明实施方式的各种替代方案。以下权利要求旨在限定本发明的范围，并因此覆盖这些权利要求范围内的方法和结构及其等同项。

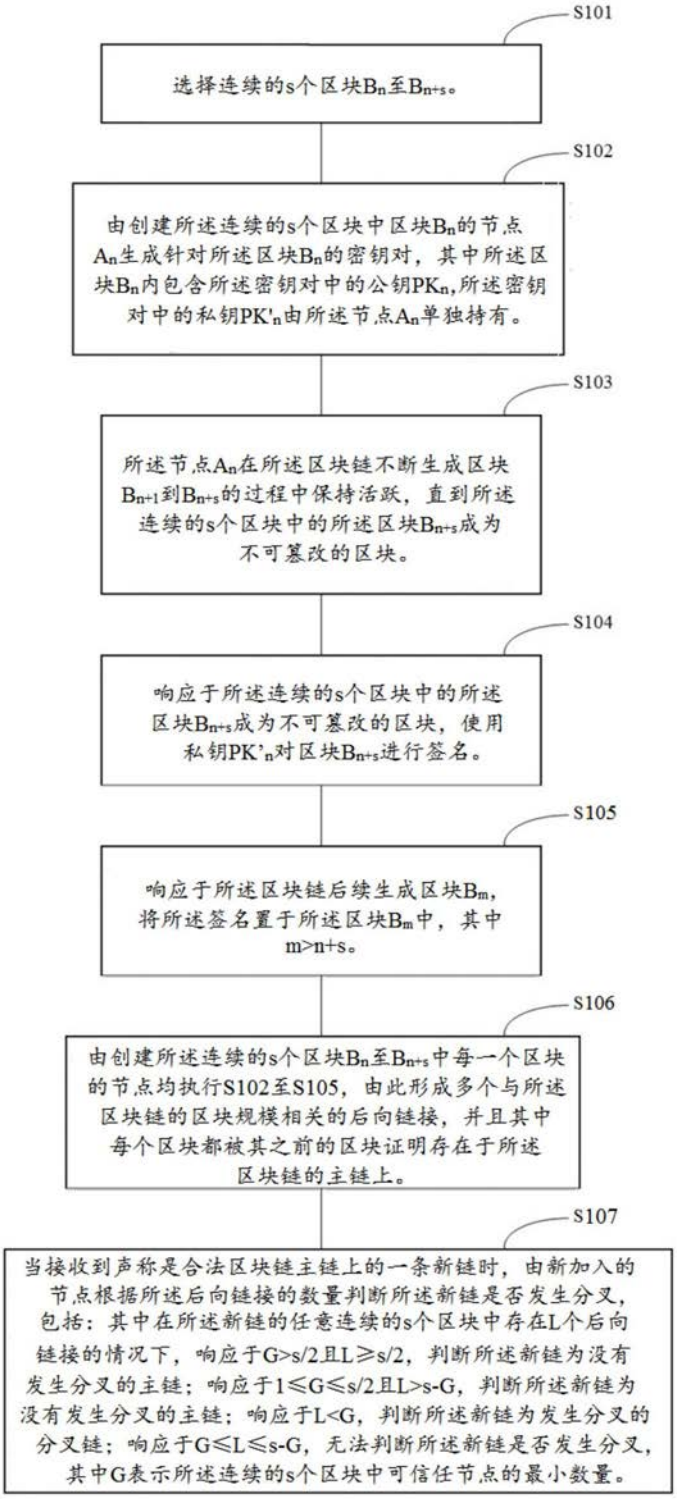

S101
选择连续的s个区块B_n至B_{n+s}。
S102
由创建所述连续的s个区块中区块B_n的节点A_n生成针对所述区块B_n的密钥对，其中所述区块B_n内包含所述密钥对中的公钥PK_n,所述密钥对中的私钥PK'_n由所述节点A_n单独持有。
S103
所述节点A_n在所述区块链不断生成区块B_{n+1}到B_{n+s}的过程中保持活跃，直到所述连续的s个区块中的所述区块B_{n+s}成为不可篡改的区块。
S104
响应于所述连续的s个区块中的所述区块B_{n+s}成为不可篡改的区块，使用私钥PK'_n对区块B_{n+s}进行签名。
S105
响应于所述区块链后续生成区块B_m，将所述签名置于所述区块B_m中，其中m>n+s。
S106
由创建所述连续的s个区块B_n至B_{n+s}中每一个区块的节点均执行S102至S105，由此形成多个与所述区块链的区块规模相关的后向链接，并且其中每个区块都被其之前的区块证明存在于所述区块链的主链上。
S107
当接收到声称是合法区块链主链上的一条新链时，由新加入的节点根据所述后向链接的数量判断所述新链是否发生分叉，包括：其中在所述新链的任意连续的s个区块中存在L个后向链接的情况下，响应于G>s/2且L≥s/2，判断所述新链为没有发生分叉的主链；响应于1≤G≤s/2且L>s-G，判断所述新链为没有发生分叉的主链；响应于L<G，判断所述新链为发生分叉的分叉链；响应于G≤L≤s-G，无法判断所述新链是否发生分叉，其中G表示所述连续的s个区块中可信任节点的最小数量。

图1

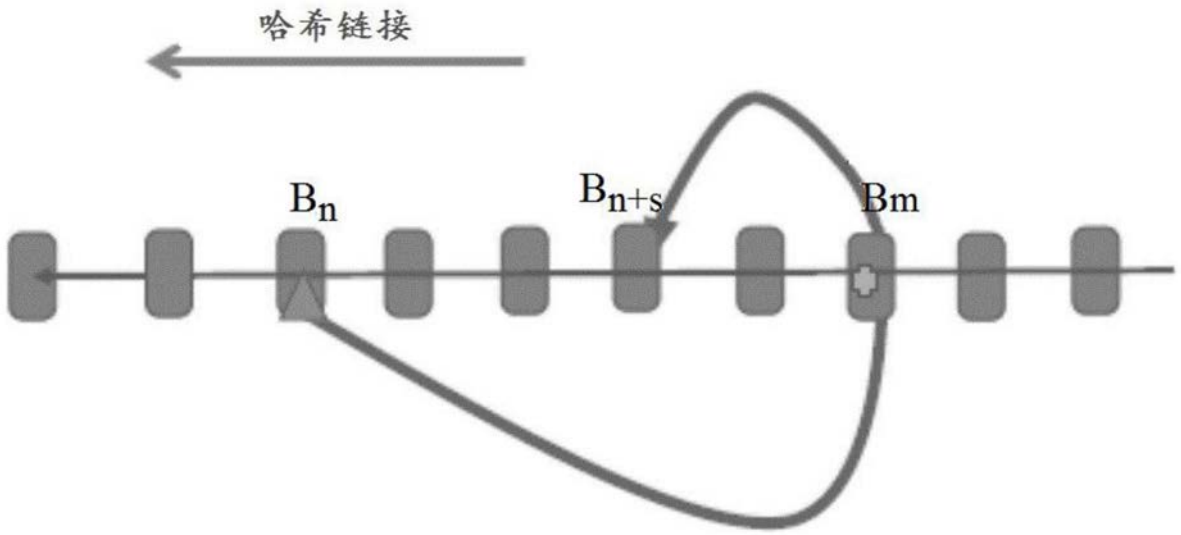

哈希链接
B_n
B_{n+s}
Bm

图2

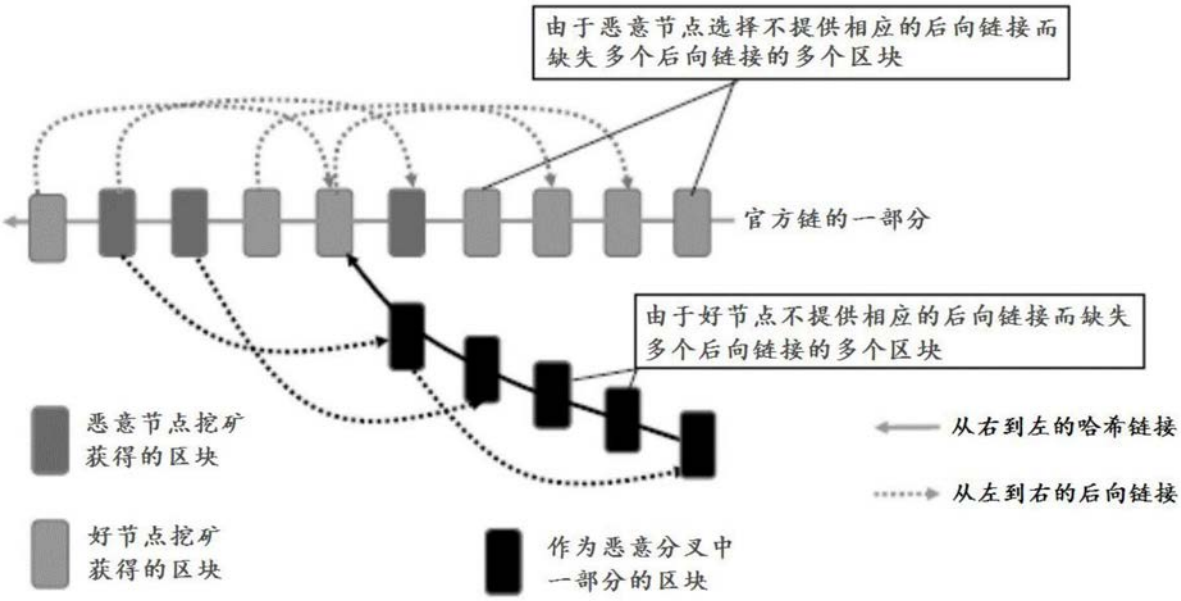

由于恶意节点选择不提供相应的后向链接而缺失多个后向链接的多个区块
官方链的一部分
由于好节点不提供相应的后向链接而缺失多个后向链接的多个区块
恶意节点挖矿获得的区块
好节点挖矿获得的区块
作为恶意分叉中一部分的区块
从右到左的哈希链接
从左到右的后向链接

图3

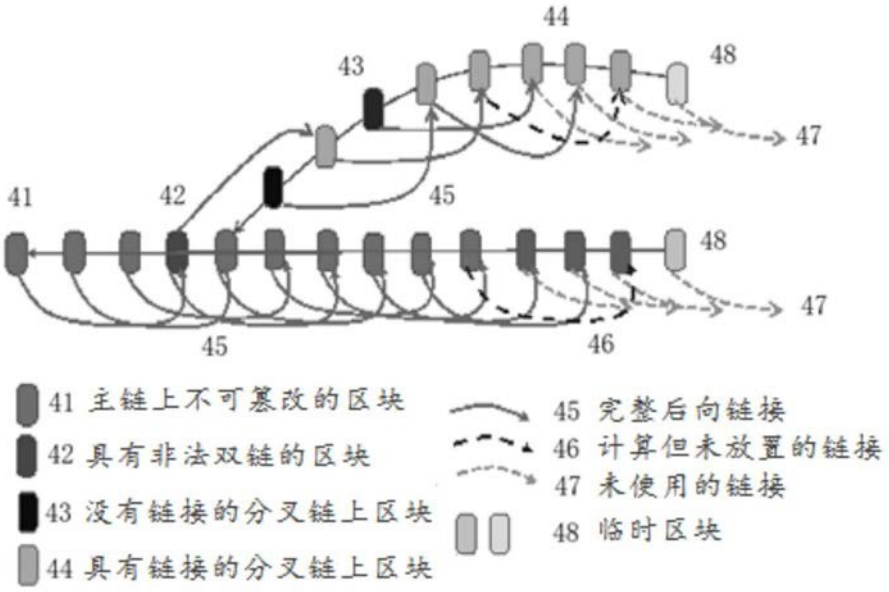

44
43
48
47
41
42
45
48
47
45
46
41 主链上不可篡改的区块
42 具有非法双链的区块
43 没有链接的分叉链上区块
44 具有链接的分叉链上区块
45 完整后向链接
46 计算但未放置的链接
47 未使用的链接
48 临时区块

图4

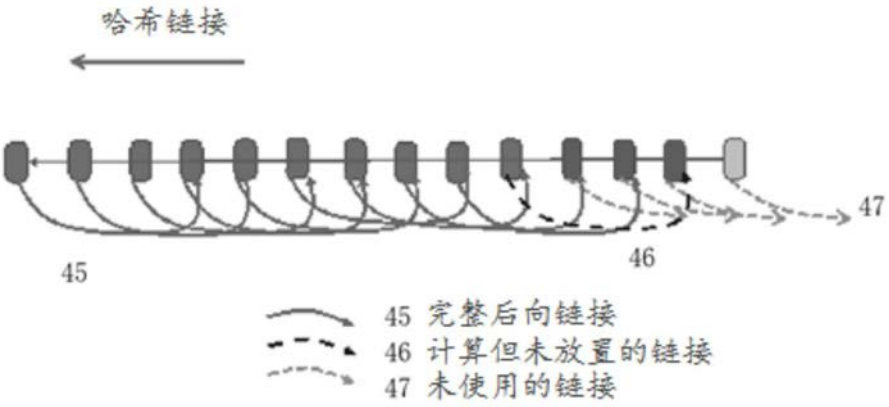

哈希链接
47
45
46
45 完整后向链接
46 计算但未放置的链接
47 未使用的链接

图5

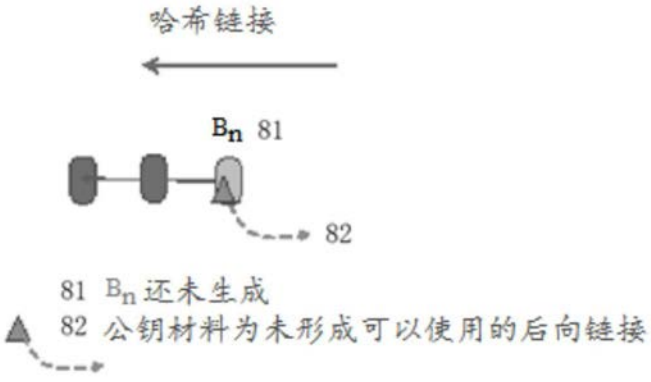

哈希链接
Bn 81
82
81 Bn 还未生成
82 公钥材料为未形成可以使用的后向链接

图6

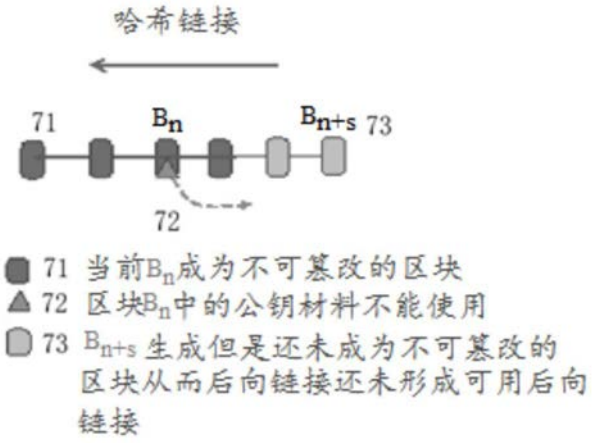

哈希链接
71
B_n
B_{n+s} 73
72
71 当前B_n成为不可篡改的区块
72 区块B_n中的公钥材料不能使用
73 B_{n+s}生成但是还未成为不可篡改的区块从而后向链接还未形成可用后向链接

图7

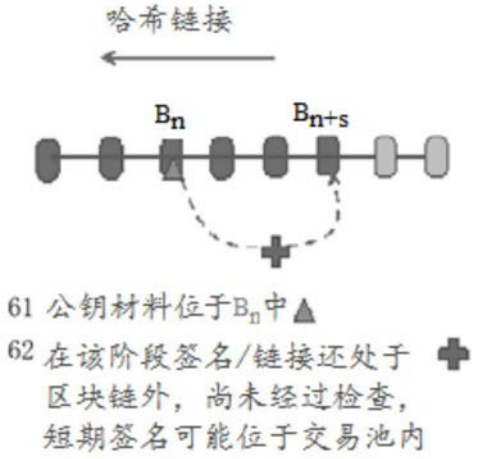

哈希链接
B_n
B_{n+s}
61 公钥材料位于B_n中
62 在该阶段签名/链接还处于区块链外，尚未经过检查，短期签名可能位于交易池内

图8

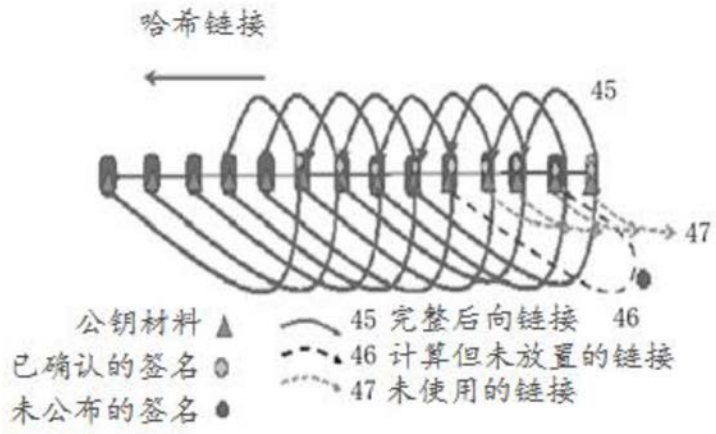

哈希链接
45
47
公钥材料
已确认的签名
未公布的签名
45 完整后向链接 46
46 计算但未放置的链接
47 未使用的链接

图9

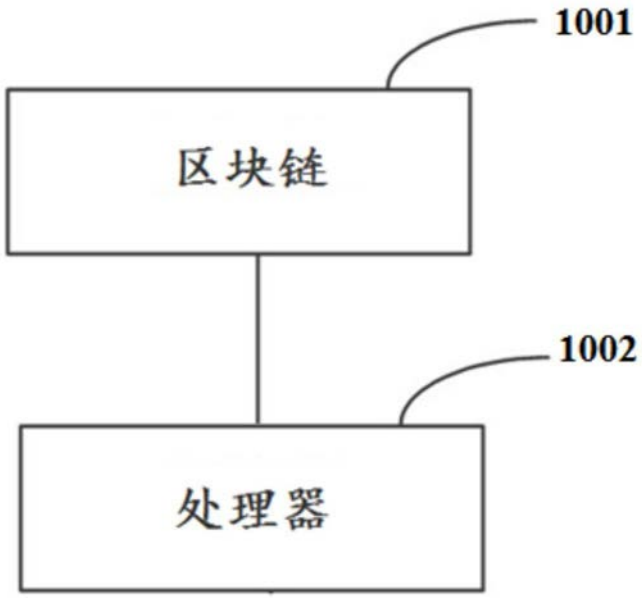


图10