(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 109087103 B
(45)授权公告日 2022.02.11

(21)申请号 201810911301.8

(22)申请日 2018.08.10

(65)同一申请的已公布的文献号
申请公布号 CN 109087103 A

(43)申请公布日 2018.12.25

(73)专利权人 中国人民解放军国防科技大学
地址 410073 湖南省长沙市砚瓦池正街47号中国人民解放军国防科技大学

(72)发明人 谢瑾 丁烨 谢涛

(74)专利代理机构 湘潭市汇智专利事务所(普通合伙) 43108
代理人 颜昌伟

(51)Int.Cl.
G06Q 20/38(2012.01)

(56)对比文件
US 2018115425 A1,2018.04.26
CN 108322304 A,2018.07.24
CN 108235799 A,2018.06.29

审查员 李慧

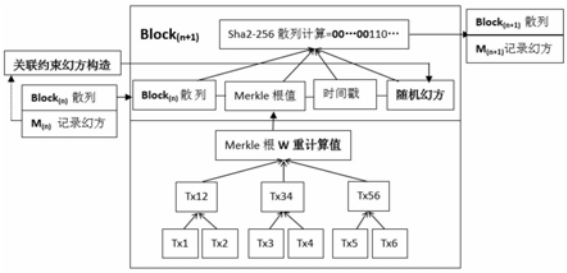
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种基于随机幻方构造的区块链工作量证明方法

(57)摘要

本发明公开一种基于随机幻方构造的区块链工作量证明方法,采用随机幻方构造算法生成投票约束随机幻方取代区块头中投票随机新数nonce,实现工作量证明过程的密码散列值投票计算。上一区块记录随机幻方决定当前区块投票随机幻方的约束条件,当前区块记录随机幻方又决定下一区块投票随机幻方的约束条件,前后区块投票随机幻方的约束数字互不重叠,且不可预测。通过构造前后区块之间具有不可预测的关联约束条件的投票随机幻方,将工作量证明转化为一个约束随机幻方构造NPC问题求解的计算过程,可以实现理想的一CPU一票的区块记录投票权,防止纯密码散列函数计算的工作量证明方法所固有的“计算中心化”、51%攻击与能源浪费,实现公平、安全、稳定、节能的绿色区块链网络技术。



CN 109087103 B

1.一种基于随机幻方构造的区块链工作量证明方法,其特征在于,包括以下步骤:用随机幻方构造算法生成投票随机幻方取代区块头中用来进行工作量证明的投票随机新数nonce,实现区块链工作量证明过程的密码散列值投票计算。

2.根据权利要求1所述的基于随机幻方构造的区块链工作量证明方法,其特征在于:所述投票随机幻方为部分位置数字预先设定为一已知随机幻方的相应位置数字,并作为投票随机幻方的约束数字。

3.根据权利要求2所述的基于随机幻方构造的区块链工作量证明方法,其特征在于:相邻区块的投票随机幻方构造实现部分数字相互关联约束,即当前区块的投票随机幻方的约束位置数字由上一区块的记录随机幻方所确定,当前区块的记录随机幻方又作为下一区块投票随机幻方的约束位置数字,但前后区块投票随机幻方的约束数字位置互不重叠。

4.根据权利要求3所述的基于随机幻方构造的区块链工作量证明方法,其特征在于:所述投票随机幻方的约束数字为单行、单列、多行、多列、中心方阵数字或上下左右四周数字,或选前后相邻两区块投票随机幻方中互不重叠的任意两部分数字。

5.根据权利要求1所述的基于随机幻方构造的区块链工作量证明方法,其特征在于,前后相邻区块的投票随机幻方实现关联约束构造,其步骤如下:

1)计算第0个区块的记录随机幻方:任意生成一个随机幻方,以该幻方的C1位置数字作为第0个区块投票随机幻方的约束条件;计算第0个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在C1位置数字约束条件下生产投票随机幻方,每生成一个投票随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该投票随机幻方为第0个区块的记录随机幻方,第0个区块头保存该记录随机幻方与相应密码散列值;第0个区块记录随机幻方的C2位置数字作为第1个区块投票随机幻方的约束数字,C1与C2分别为相邻区块进行投票随机幻方构造关联约束的两个互不重叠的数字位置区域;

2)计算第1个区块的记录随机幻方:计算第1个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在C2位置数字约束条件下生产投票随机幻方,每生成一个投票随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该约束随机幻方为第1个区块的记录随机幻方,第1个区块头保存该记录随机幻方与相应密码散列值;第1个区块记录随机幻方的C1位置数字作为第2个区块投票随机幻方的约束数字;

3)计算第2个区块的记录随机幻方:计算第2个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在C1位置数字约束条件下生产投票随机幻方,每生成一个投票随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该约束随机幻方为第2个区块的记录随机幻方,第2个区块头保存该记录随机幻方与相应密码散列值;第2个区块记录随机幻方的C2位置数字作为第3个区块投票随机幻方的约束数字;

4)计算第k个区块的记录随机幻方:计算第k个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在C2位置数字约束条件下生产投票随机幻方,每生成一个投票随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该约束随机幻方为第k个区块的记录随机幻方,第k个区块头保存

该记录随机幻方与相应密码散列值;第k个区块记录随机幻方的C1位置数字作为第k+1个区块投票随机幻方的约束数字;

5)计算第k+1区块的记录随机幻方:计算第k+1个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在C1位置数字约束条件下生产投票随机幻方,每生成一个约束随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该投票随机幻方为第k+1个区块的记录随机幻方,第k+1个区块头保存该记录随机幻方与相应密码散列值;第k+1个区块记录随机幻方的C2位置数字作为第k+2个区块投票随机幻方的约束数字;

6)计算第k+2区块的记录随机幻方:计算第k+2个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在C2位置数字约束条件下生产投票随机幻方,每生成一个约束随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该投票随机幻方为第k+2个区块的记录随机幻方,第k+2个区块头保存该记录随机幻方与相应密码散列值;第k+2个区块记录随机幻方的C1位置数字作为下一区块投票随机幻方的约束数字;

7)此C1位置与C2位置数字约束过程交替重复,为记录下一区块进行工作量证明,工作量证明难度通过线性自适应调节,确保区块链的区块时间间隔的基本一致性;区块链网络每生成一个新区块,通过约束随机幻方构造与密码散列值计算得到满足指定密码散列值难度要求的记录随机幻方,实现区块链数据不可篡改的记录过程。

6.根据权利要求1所述的基于随机幻方构造的区块链工作量证明方法,包括一种适合关联约束随机幻方构造的工作量证明过程的区块链数据结构,其特征在于:区块由区块头与区块体组成,区块头由前一区块的密码散列值、区块体密码散列W重计算根值、时间戳与投票随机幻方组成;区块体由交易数据按密码散列计算Merkle树结构组成,并对区块体的Merkle树根值设置一定的密码散列重复计算次数W,W值由关联约束随机幻方构造的计算时间复杂度决定,使得区块体密码散列W重根值的计算时间大于一个关联约束随机幻方的构造时间。

7.根据权利要求6所述的基于随机幻方构造的区块链工作量证明方法,其特征在于:所述W必须满足下列关系:

$W \geq V_{sha256}/V_{magic}$.

其中V_{magic}为随机幻方的构造速率,V_{sha256}为密码散列函数Sha256的计算速率。

一种基于随机幻方构造的区块链工作量证明方法

技术领域

[0001] 本发明涉及区块链技术领域,特别涉及一种基于随机幻方构造的区块链工作量证明方法。

背景技术

[0002] 区块链作为比特币的基础技术,具有去中心化、去中间人、去信任、匿名、开放、可追溯、分布式与不可篡改等特点,在智能合约、证券交易、电子商务、物联网、社交通讯、文件存储、存在性证明、身份验证、股权众筹等领域具有广泛的革命性应用。区块链网络的安全稳定运行必须解决P2P网络拜占庭将军问题(Byzantine Generals Problem),即在缺乏可信第三方中心节点的条件下,如何在分布式节点之间达成共识形成互信。目前,区块链共识机制分为两类:工作量证明(Proof of Work,PoW)与权益证明(Proof of Stake,PoS),其中权益证明又发展为委任权益证明(Delegated Proof of Stake,DPOS)。

[0003] 尽管PoS共识机制可以解决区块链记录共识机制的能源问题,区块链因而可能成为一种绿色环保的去中心化系统,但在网络安全方面,PoS机制存在固有的缺陷。大部分PoS机制的问题源于该协议只考虑本身区块链上所有交易数据,没有一个类似PoW系统中为解决复杂密码学难题必须投入算力的真实外部物理点作为区块链的定锚。因此,直觉上PoS机制比较容易遭受攻击。此外,实用拜占庭容错算法(PBFT)只在IBM HyperLedger fabric私有区块链中采用,不能在公有链中得到扩展应用。

[0004] PoW共识机制具有真实的外部物理点作为区块链记录的安全定锚,即为解决复杂密码学难题必须投入足够的算力。PoW区块链共识记录以全网算力作为代价,攻击者对区块链的篡改也需要同样的代价,因此,工作量证明机制(PoW)具有安全区块链共识机制的必要条件。密码散列计算是计算世界中的底层计算,是基于区块链的加密数字货币的物质基础,但密码散列计算的底层计算特点必然导致计算设备的“军备竞赛”,通过“矿力垄断”产生事实上的“计算中心化”,违背“去中心化”的区块链网络设计目标。

发明内容

[0005] 为了解决现有区块链网络共识机制中工作量证明方法存在的安全问题,本发明提出一种安全性好的基于随机幻方构造的区块链工作量证明方法。

[0006] 本发明解决上述技术问题的技术方案是:一种基于随机幻方构造的区块链工作量证明方法其步骤如下:用随机幻方构造算法生成投票随机幻方取代区块头中用来进行工作量证明的投票随机新数nonce,实现区块链工作量证明过程的密码散列值投票计算。

[0007] 上述基于随机幻方构造的区块链工作量证明方法中,所述投票随机幻方为部分位置数字预先设定为一已知随机幻方的相应位置数字,并作为投票随机幻方的约束数字。

[0008] 上述基于随机幻方构造的区块链工作量证明方法中,相邻区块的投票随机幻方构造实现部分位置数字相互关联约束,即当前区块的投票随机幻方的约束位置数字由上一区块的记录随机幻方所确定,当前区块的记录随机幻方又作为下一区块投票随机幻方的约束

位置数字，但前后区块投票随机幻方的约束数字位置互不重叠。

[0009] 上述基于随机幻方构造的区块链工作量证明方法中，所述投票随机幻方的约束数字为单行、单列、选多行、多列、中心方阵数字或上下左右四周数字，或选前后相邻两区块投票随机幻方中互不重叠的任意两部分数字。

[0010] 上述基于随机幻方构造的区块链工作量证明方法中，前后相邻区块的投票随机幻方实现关联约束构造。假设用于相邻区块进行投票随机幻方构造关联约束的两个互不重叠的数字位置区域分别为C1与C2，其步骤可描述如下：

[0011] 1)计算第0个区块的记录随机幻方：任意生成一个随机幻方，以该幻方的C1位置数字作为第0个区块投票随机幻方的约束条件；计算第0个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在C1位置数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该投票随机幻方为第0个区块的记录随机幻方，第0个区块头保存该记录随机幻方与相应密码散列值；第0个区块记录随机幻方的C2位置数字作为第1个区块投票随机幻方的约束数字；

[0012] 2)计算第1个区块的记录随机幻方：计算第1个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在C2位置数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该约束随机幻方为第1个区块的记录随机幻方，第1个区块头保存该记录随机幻方与相应密码散列值；第1个区块记录随机幻方的C1位置数字作为第2个区块投票随机幻方的约束数字；

[0013] 3)计算第2个区块的记录随机幻方：计算第2个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在C1位置数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该约束随机幻方为第2个区块的记录随机幻方，第2个区块头保存该记录随机幻方与相应密码散列值；第2个区块记录随机幻方的C2位置数字作为第3个区块投票随机幻方的约束数字；

[0014] 4)计算第k个区块的记录随机幻方：计算第k个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在C2位置数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该约束随机幻方为第k个区块的记录随机幻方，第k个区块头保存该记录随机幻方与相应密码散列值；第k个区块记录随机幻方的C1位置数字作为第k+1个区块投票随机幻方的约束数字；

[0015] 5)计算第k+1区块的记录随机幻方：计算第k+1个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在C1位置数字约束条件下生产投票随机幻方，每生成一个约束随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该投票随机幻方为第k+1个区块的记录随机幻方，第k+1个区块头保存该记录随机幻方与相应密码散列值；第k+1个区块记录随机幻方的C2位置数字作为第k+2个区块投票随机幻方的约束数字；

[0016] 6)计算第k+2区块的记录随机幻方：计算第k+2个区块体的Merkle树密码散列根值

W次后，通过约束随机幻方构造算法在C2位置数字约束条件下生产投票随机幻方，每生成一个约束随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该投票随机幻方为第k+2个区块的记录随机幻方，第k+2个区块头保存该记录随机幻方与相应密码散列值；第k+2个区块记录随机幻方的C1位置数字作为下一区块投票随机幻方的约束数字；

[0017] 7)此C1位置与C2位置数字约束过程交替重复，为记录下一区块进行工作量证明，工作量证明难度通过线性自适应调节，确保区块链的区块时间间隔的基本一致性；区块链网络每生成一个新区块，通过约束随机幻方构造与密码散列值计算得到满足指定密码散列值难度要求的记录随机幻方，实现区块链数据不可篡改的记录过程。

[0018] 上述的区块链网络共识机制中的工作量证明计算方法中，包括一种适合关联约束随机幻方构造的工作量证明过程的区块链数据结构，区块由区块头与区块体组成，区块头由前一区块的密码散列值、区块体密码散列W重计算根值、时间戳与投票随机幻方组成；区块体由交易数据按密码散列计算Merkle树结构组成，并对区块体的Merkle树根值设置一定的密码散列重复计算次数W，W值由关联约束随机幻方构造的计算时间复杂度决定，使得区块体密码散列W重根值的计算时间大于一个关联约束随机幻方的构造时间。

[0019] 上述的区块链网络共识机制中的工作量证明计算方法中，所述W必须满足下列关系：

[0020] $W \geqslant V_{sha256}/V_{magic}$.

[0021] 其中V_{magic}为随机幻方的构造速率，V_{sha256}为密码散列函数Sha256的计算速率。

[0022] 与现有技术相比，本发明的优点是：

[0023] 1)本发明用随机幻方构造算法生成投票随机幻方取代区块头中用来进行工作量证明的投票随机新数nonce，实现区块链工作量证明过程的密码散列值投票计算。随机幻方构造算法一般采用基于启发式知识的智能计算实现，智能计算一般不适合ASIC实现，或者ASIC实现的智能计算算法与CPU程序实现的智能计算算法的能效性没有明显的比较优势。因此，随机幻方构造计算可以防止ASIC计算硬件固有的“军备竞赛”，可以避免因出现“计算中心化”而可能发生的“51％攻击”问题。

[0024] 2)随机幻方构造工作量证明能实现理想的一CPU一票的区块记录权投票共识机制，区块链网络所有参与节点基于CPU计算一律平等，区块链网络因而公平、稳定，特别适合参与计算节点较少的区块链网络共识机制的工作量证明过程，区块链不会产生分叉。

[0025] 3)随机幻方构造工作量证明方法因不会产生计算世界中低层计算硬件的“军备竞赛”问题，专业“矿池”因而无利可图，区块链网络的安全性仅依靠所有参与节点自发维持，避免了比特币网络因计算硬件固有的“军备竞赛”过程所导致的“矿力”指数升级所产生的全球能源巨大浪费，因而是一种节能的环保绿色型工作量证明方法。

[0026] 4)随机幻方构造工作量证明可以实现工作量证明难度的在线线性调节，以随机幻方取代随机新数nonce，工作量证明难度及相应密码散列值为全网随机幻方的构造速率与区块间隔时间之乘积，因此工作量证明难度与参与节点数量成线性关系。

[0027] 5)现有智能计算与枚举方法在随机幻方构造问题的计算效率之比已达到10^{40}以上，采用计算硬件提升节点的随机幻方构造速率远没有通过算法改进提高随机幻方构造算法的构造效率具有经济与技术优势，而且随机幻方构造算法的计算效率越高，计算硬件的

经济与技术优势越低。

[0028] 6)通过实现相邻区块间投票随机幻方构造过程的部分数字随机关联约束,可以使得为争夺当前区块记录权而构造的投票随机幻方在后续区块记录权的投票过程中不再有效,实现了密码散列函数计算的底层计数功能的有效计算工作量不可复用特性。

附图说明

[0029] 图1为本发明的原理方框示意图。

[0030] 图2为本发明中第(n-2)区块的记录随机幻方。

[0031] 图3为本发明中第(n-1)区块记录过程的关联约束投票随机幻方举例。

[0032] 图4为本发明中第(n-1)区块的记录随机幻方。

[0033] 图5为本发明中第n区块记录过程的关联约束投票随机幻方举例。

[0034] 图6为本发明中第n区块的记录随机幻方。

[0035] 图7为本发明中内外嵌套数字关联约束的随机幻方构造示意。

具体实施方式

[0036] 下面结合附图和具体实施例对本发明作进一步的说明,以行关联约束随机幻方构造的工作量证明过程为例。以列关联约束随机幻方构造的工作量证明与以行关联约束随机幻方构造的工作量证明过程完全相同。

[0037] 参见图1,图1为本发明的原理方框示意图。区块链中区块的基本数据结构与比特币区块链相同,仅将比特币中的连续递增或随机变化的变量nonce用随机幻方取代,而区块体的交易支付Merkle树根密码散列值则重复计算W次(W值计算在后面说明)。区块头由前一区块$Block_{(n)}$密码散列值、当前区块$Block_{(n+1)}$区块体交易支付数据Merkle树根的W次重复密码散列计算值、当前区块$Block_{(n+1)}$时间戳以及关联约束随机幻方四部分组成,由Sha256密码散列函数(任何标准密码散列函数均可,本发明以SHA256为例说明)计算该部分数据组成的消息块的密码散列值得到当前区块$Block_{(n+1)}$的一个密码散列值。满足一定工作量证明密码散列值难度(从最高位MSB开始连续一定个数0,比如小于00…0110)要求的区块头密码散列值称为有效密码散列值。

[0038] $Block_{(n+1)}$区块有效密码散列值(工作量证明)计算过程

[0039] 由关联约束随机幻方构造算法(参见发明专利02114288.2)构造的投票随机幻方作为随机新数nonce,作为区块头消息块中不断改变的消息部分计算整个区块头的密码散列值,所有参与节点中第一个得到当前区块有效密码散列值的节点才有可能获得对该区块的记录权。当前区块$Block_{(n+1)}$有效密码散列值中被多数节点校验并承认的密码散列值成为当前区块$Block_{(n+1)}$的工作量证明密码散列值,下一区块的密码散列值基于该有效密码散列值计算。

[0040] 区块链工作量证明难度值与密码散列值hashcash调节计算

[0041] 记第n个区块的工作量证明难度值与相应的密码散列值分别为$diff_n$与$hashcash_n$,假设约束随机幻方构造算法每个CPU一分钟能构造2^{10}左右个关联约束随机幻方,区块时间间隔为10分钟,并且假设开始阶段整个区块链网络仅有一个节点一个CPU参与工作量证明。我们可以取创世区块的工作量证明难度值为$diff_0=2^{14}$,以连续K个区块为工作量证明

难度值的时间调节基准，区块时间间隔为T(比如10分钟)，T_K为最近K个区块的实际记录时间，KT为K个区块的标准记录时间。从第K个区块开始，我们可以得到如下工作量证明难度值调节与hashcash值调节计算公式：

[0042] $diff_{n+1}=diff_n\times KT/T_K$

[0043] $hashcash_n=2^{256}/diff_n$

[0044] 初始块工作量证明$hashcash_0=2^{256}/2^{14}=2^{242}$

[0045] 或者直接计算：$hashcash_{n+1}=hashcash_n\times T_K/KT$

[0046] 区块$Block_{(n+1)}$记录随机幻方$M_{(n+1)}$

[0047] 区块链P2P网络节点在争夺第(n+1)个区块$Block_{(n+1)}$的记录权过程中，由约束随机幻方构造算法产生并且满足区块头设定工作量证明密码散列值目标($hashcash_{n+1}$)要求的特定关联约束投票随机幻方。当有节点第一个找到这个关联约束投票随机幻方时，则该节点所生成的$Block_{(n+1)}$可被该节点成功记录并向网络所有节点进行广播，$Block_{(n+1)}$区块的记录随机幻方记为$M_{(n+1)}$。

[0048] 区块链P2P网络计算节点获得当前区块记录权的概率计算

[0049] 区块链以整个联网节点的约束随机幻方构造总速率作为工作量证明的计算基准，以每区块时段内关联约束随机幻方的网络总生产数量作为系统工作量证明难度的设定基础，通过密码散列函数检验随机幻方生产的数量是否已达到设定值。每个区块的记录时间段内，每个参与计算节点获得该区块记录权的概率跟该节点构造约束随机幻方的速率成正比，跟网络构造约束随机幻方的总速率成反比。假设网络由m个计算节点组成，第i个计算节点构造约束随机幻方的速率为V_i，则第i个计算节点获得当前区块的记录权的概率(轮盘赌概率)为$P_i=V_i/\sum_{j=1}^{m}V_j$。

[0050] 区块体Merkle树密码散列根值W次重复计算数的确定方法

[0051] 计算Merkle树密码散列根值W次是为了防止通过修改交易数据改变区块体密码散列值的可能攻击方法。所谓交易修改攻击，就是指通过修改Merkle树根节点下的叶节点交易数据来改变Merkle树根值，从而相应改变$Block_{(n+1)}$的密码散列值。密码散列计算函数的时间复杂度与随机幻方构造的时间复杂度相比可以忽略，因此，在保持$Block_{(n+1)}$特定记录随机幻方不变的前提下通过修改交易数据可快速得到满足工作量证明难度要求的$Block_{(n+1)}$有效密码散列值，从而可实现区块链分叉达到双花攻击的目的。为了防止通过交易修改攻击区块链产生双花问题，必须对区块体中Merkle树根的密码散列值计算设置一定的重复计算次数下限W，以达到一定的计算复杂度，使得该计算复杂度大于约束随机幻方构造当前算法的计算复杂度。对于同一计算CPU硬件，假设当前约束随机幻方的构造速率为V_{magic}，密码散列函数Sha256的计算速率为V_{sha256}，则W的下限设置必须满足下列关系：$W\times V_{magic}\geq V_{sha256}$，即$W\geq V_{sha256}/V_{magic}$.随着约束随机幻方构造算法的效率不断提高，通过交易修改攻击区块链的方法从计算代价上越来越不可行。

[0052] 基于约束随机幻方构造的区块链工作量证明方法

[0053] 以行关联约束随机幻方构造的工作量证明为例。为争夺区块记录权构造投票随机幻方，通过前后相邻区块关联约束的方式构造随机幻方，可以消除投票随机幻方的后续复用问题(progress freeness)。具体地，为争夺当前区块的记录权而构造的投票随机幻方的部分数字必须由前一区块的记录随机幻方随机决定，当前区块的记录随机幻方又随机决定

后一区块的投票随机幻方的部分数字，但与前一区块的关联约束数字位置不可重叠。如此前后区块投票随机幻方部分数字交替关联约束构造的随机幻方是不可复用的。比如，以10阶随机幻方为例。假定第(n-2)区块的记录随机幻方如图2所示，如果第(n-2)区块所有投票随机幻方的最后一行数字要求被第(n-3)区块记录随机幻方的相应行所设定，第(n-1)区块的所有投票随机幻方的第一行数字则由第(n-2)区块记录随机幻方相应行设定，如图3所示。

[0054] 对于第(n-1)个区块，假定某计算节点经过k_{n-1}次投票(构造不同的第一行关联约束随机幻方作为投票随机幻方计算区块头的密码散列值)得到第(n-1)区块的记录随机幻方，其第一行由第(n-2)区块记录随机幻方相应行数字设定，如图4所示。同样，第n区块的所有投票随机幻方的最后一行数字则由第(n-1)区块的记录随机幻方相应行数字所设定，如图5所示。对于第n个区块，假定某计算节点经过k_n次投票(构造不同的最后一行关联约束随机幻方作为投票随机幻方计算区块头的密码散列值)得到第n区块的记录随机幻方如图6所示，其最后一行数字则由第(n-1)区块的记录随机幻方相应行数字所设定。

[0055] 区块链工作量证明计算步骤：

[0056] 1)计算第0个区块的记录随机幻方：任意生成一个随机幻方，以该幻方的首行数字作为第0个区块投票随机幻方的约束条件；计算第0个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在首行数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该投票随机幻方为第0个区块的记录随机幻方，第0个区块头保存该记录随机幻方与相应密码散列值；第0个区块记录随机幻方的末行作为第1个区块投票随机幻方的约束数字；

[0057] 2)计算第1个区块的记录随机幻方：计算第1个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在末行数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该约束随机幻方为第1个区块的记录随机幻方，第1个区块头保存该记录随机幻方与相应密码散列值；第1个区块记录随机幻方的首行作为第2个区块投票随机幻方的约束数字；

[0058] 3)计算第2个区块的记录随机幻方：计算第2个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在首行数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该约束随机幻方为第2个区块的记录随机幻方，第2个区块头保存该记录随机幻方与相应密码散列值；第2个区块记录随机幻方的末行作为第3个区块投票随机幻方的约束数字；

[0059] 4)计算第k个区块的记录随机幻方：计算第k个区块体的Merkle树密码散列根值W次后，通过约束随机幻方构造算法在末行数字约束条件下生产投票随机幻方，每生成一个投票随机幻方计算一次区块头的密码散列值，直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方，并记该约束随机幻方为第k个区块的记录随机幻方，第k个区块头保存该记录随机幻方与相应密码散列值；第k个区块记录随机幻方的首行作为第k+1个区块投票随机幻方的约束数字；

[0060] 5)计算第k+1区块的记录随机幻方:计算第k+1个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在首行数字约束条件下生产投票随机幻方,每生成一个约束随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该投票随机幻方为第k+1个区块的记录随机幻方,第k+1个区块头保存该记录随机幻方与相应密码散列值;第k+1个区块记录随机幻方的末行作为第k+2个区块投票随机幻方的约束数字;

[0061] 6)计算第k+2区块的记录随机幻方:计算第k+2个区块体的Merkle树密码散列根值W次后,通过约束随机幻方构造算法在末行数字约束条件下生产投票随机幻方,每生成一个约束随机幻方计算一次区块头的密码散列值,直到发现满足指定工作量证明密码散列值难度要求的投票随机幻方,并记该投票随机幻方为第k+2个区块的记录随机幻方,第k+2个区块头保存该记录随机幻方与相应密码散列值;第k+2个区块记录随机幻方的首行作为下一区块投票随机幻方的约束数字;

[0062] 7)此过程交替重复,为记录下一区块进行工作量证明,工作量证明难度通过线性自适应调节,确保区块链的区块时间间隔的基本一致性;区块链网络每生成一个新区块,通过约束随机幻方构造与密码散列值计算得到满足指定密码散列值难度要求的记录随机幻方,实现区块链数据不可篡改的记录过程。

[0063] 通过如此前后相邻区块投票随机幻方的头尾交替关联约束设定方法,为每一区块构造的投票随机幻方只能为争夺本区块记录权的临时投票过程服务,不再对争取后续区块记录权的投票过程有效,即节点为争夺区块记录权而构造的投票关联约束随机幻方在工作量证明过程中无继承性。对于10阶随机幻方的智能构造算法,经过实验测试,普通笔记本电脑构造随机幻方的速度约为3000个/分钟左右,固定一行数字(第一行或最后一行,任意行列均可)构造约束随机幻方的速度下降为约1000个/分钟左右,即为完全自由随机幻方构造速度的1/3左右。经过计算,由当前区块的投票随机幻方构造过程猜测下一区块的投票随机幻方的关联约束随机数字的概率约为$100^{-10}=10^{-20}$。因此,通过一行或一列以上数字实现关联约束随机幻方构造的工作量证明过程已经足够安全!

[0064] 其它以随机幻方任何两两互不重叠且规模基本相同的数字部分进行关联约束的随机幻方构造工作量证明机制与行关联约束基本相同,再以内外嵌套数字关联约束的随机幻方构造工作量证明机制为例说明。

[0065] 内外嵌套数字关联约束随机幻方构造工作量证明

[0066] 非常容易将行或列关联约束随机幻方构造推广至内外嵌套关联约束随机幻方构造的工作量证明。所谓内外嵌套关联约束随机幻方构造是指,如果先固定一个已知随机幻方的中央部分,如图7所示,固定10阶随机幻方的中央6×6方阵数字部分(36个数字),再随机组合周围64个数字,可以构造具有同一中央数字部分的很多不同随机幻方。同样,如果固定周围一圈数字(36个数字)而随机组合其中央数字部分(64个数字),也可以构造很多四周数字固定的不同随机幻方。如同行或列关联约束的随机幻方构造一样,前后区块记录过程中投票随机幻方通过中央或四周数字的交替关联约束,可以构成有效的计算结果不可复用的工作量证明机制。与行或列关联约束的随机幻方构造工作量证明机制相比,内外数字关联约束的随机幻方构造工作量证明机制必须适当选择中央方阵约束数字的数量规模与四周约束数字数量规模,使得内外关联约束随机幻方构造算法的计算复杂度或随机幻方的解

空间分布密度基本相同,从而间接使得相邻区块记录的工作量证明过程难度基本相等。此外,Block(n+1)区块工作量证明计算步骤,区块链工作量证明难度值与密码散列值hashcash的计算与调节方法,区块链P2P网络计算节点获得当前区块记录权的概率计算方法,以及区块体Merkle树密码散列根值W次重复计算数的确定方法,与行或列关联约束随机幻方构造工作量证明机制完全相同。

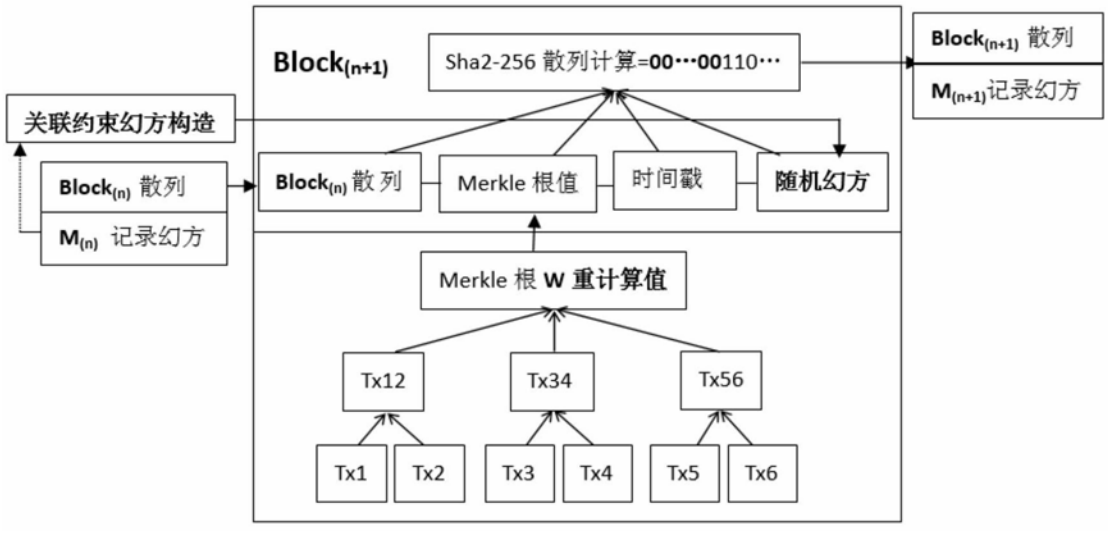


图1

91	15	69	78	74	14	35	21	51	57
67	50	33	96	62	47	48	29	10	63
42	46	4	24	12	84	58	38	97	100
7	71	79	19	56	87	66	70	18	32
40	20	81	31	54	55	59	60	28	77
8	86	44	5	90	25	65	64	73	45
92	17	43	36	3	88	80	52	85	9
94	95	37	76	34	6	2	99	49	13
23	75	26	72	98	83	39	61	1	27
41	**30**	**89**	**68**	**22**	**16**	**53**	**11**	**93**	**82**

图2

91	15	69	78	74	14	35	21	51	57
96	50	56	90	68	8	72	30	26	9
89	92	52	17	22	31	3	43	85	71
10	19	4	97	24	59	53	64	94	81
23	6	82	5	38	99	80	58	87	27
84	60	39	75	70	7	100	48	2	20
61	47	63	12	40	98	18	86	34	46
13	95	67	16	79	55	33	42	29	76
37	77	11	49	36	41	28	88	65	73
1	44	62	66	54	93	83	25	32	45

图3

91	15	69	78	74	14	35	21	51	57
3	30	73	97	10	76	85	90	23	18
56	20	45	98	4	46	50	92	22	72
36	83	64	9	63	62	1	80	42	65
94	34	24	16	48	68	95	2	49	75
55	53	12	58	88	96	8	52	43	40
60	86	6	39	77	87	54	25	66	5
84	44	31	29	71	17	61	28	93	47
19	99	100	11	32	26	89	33	37	59
7	41	81	70	38	13	27	82	79	67

图4

22	29	48	49	92	10	77	61	17	100
90	80	60	28	4	74	42	88	30	9
87	63	91	62	55	15	12	75	43	2
46	20	36	14	66	97	86	6	35	99
11	57	72	16	94	52	65	3	71	64
34	5	19	95	40	54	78	51	96	33
93	68	76	56	24	53	8	50	18	59
89	84	1	32	69	39	37	44	85	25
26	58	21	83	23	98	73	45	31	47
7	41	81	70	38	13	27	82	79	67

图5

83	9	40	32	23	76	47	74	75	46
1	11	36	97	62	100	43	64	85	6
93	77	21	5	19	8	91	98	56	37
61	89	63	80	54	59	16	28	35	20
49	39	96	50	86	45	3	17	30	90
60	48	66	58	73	12	53	22	26	87
34	95	29	15	92	42	68	71	57	2
84	31	55	94	14	51	69	25	10	72
33	65	18	4	44	99	88	24	52	78
7	41	81	70	38	13	27	82	79	67

图6

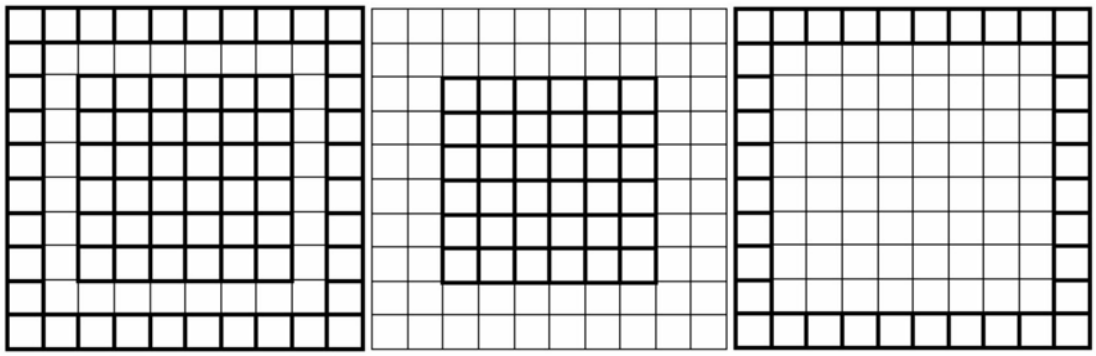


图7