(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110770732 B
(45)授权公告日 2023.06.27

(21)申请号 201880035829.1
(22)申请日 2018.04.06
(65)同一申请的已公布的文献号
申请公布号 CN 110770732 A
(43)申请公布日 2020.02.07
(30)优先权数据
102017209381.1 2017.06.02 DE
(85)PCT国际申请进入国家阶段日
2019.11.29
(86)PCT国际申请的申请数据
PCT/EP2018/058928 2018.04.06
(87)PCT国际申请的公布数据
WO2018/219533 DE 2018.12.06
(73)专利权人 联邦印刷有限公司
地址 德国柏林市
(72)发明人 A·维尔克 M·帕依斯切克
I·科马罗夫
(74)专利代理机构 南京苏创专利代理事务所(普通合伙) 32273
专利代理师 常晓慧
(51)Int.Cl.
G06F 21/64(2006.01)
H04L 9/32(2006.01)
(56)对比文件
JP 2007520842 A,2007.07.26
US 4829445 A,1989.05.09
WO 2017170912 A1,2017.10.05
审查员 陈玲

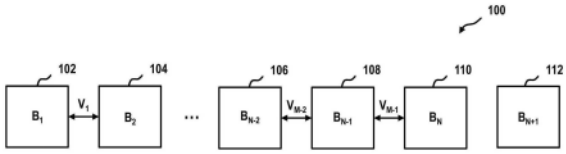
权利要求书4页 说明书19页 附图5页

(54)发明名称

采用双向链接的区块链结构在电子存储器中防篡改存储数据的方法、电子数据存储系统和电信系统

(57)摘要

本发明涉及一种在电子存储器中防篡改存储数据的方法。该方法包括:提供一个双向链接的区块链结构(100);生成一个用于扩展区块链结构(100)的附加区块(112),该附加区块包含待存储数据(210)并且设置用于与区块链结构(100)的最后区块(110)双向链接,其中区块链结构(100)的最后区块(110)包含存储的数据;计算用于最后区块(110)与附加区块(112)的双向链接的第一区块相关链接函数(122),其中该链接函数(122)的计算包括在使用存储在最后区块(110)中的数据和要存储在附加区块(112)中的数据(210)的情况下计算所述最后区块和附加区块(110,112)的组合的区块相关校验值,以及将组合校验值与区块无关的链接过程独立函数关联;将第一区块相关链接函数(122)添加至最后区块(110)和附加区块(112)。



CN 110770732 B

1.一种采用双向链接的区块链结构(100)在电子存储器中防篡改存储数据的方法,其中,该方法包括:

• 提供双向链接的区块链结构(100),

• 提供待存储数据(210),

• 生成用于扩展该区块链结构(100)的附加区块(112),该附加区块包含待存储数据(210)并且设置用于与该区块链结构(100)的最后区块(110)双向链接,其中,该区块链结构(100)的最后区块(110)包含存储数据,

• 计算用于最后区块(110)与附加区块(112)的双向链接的第一区块相关链接函数(122),其中,该链接函数(122)的计算包括:

o在采用存储在最后区块(110)中的数据和待存储在附加区块(112)中的数据(210)的情况下,计算所述最后区块和附加区块(110,112)的组合的区块相关校验值,

o将组合校验值与区块无关的链接过程独立函数关联,

• 将第一区块相关链接函数(122)添加至最后区块(110),

• 将第一区块相关链接函数(122)添加至附加区块(112),

• 存储被扩展了附加区块(112)的区块链结构(130)。

2.根据权利要求1所述的方法,其中,该区块链结构(100)的最后区块(110)还包括该最后区块(110)与该区块链结构(100)的倒数第二区块(108)的双向链接的第二区块相关链接函数,其中,将第一区块相关链接函数(122)添加至最后区块(110)包括:将第一区块相关链接函数(122)与第二区块相关链接函数关联。

3.根据前述权利要求之一所述的方法,其中,该区块无关的链接过程独立函数是包含许多区块无关的链接过程独立函数的函数集中的一个函数,其中,该函数集的每个函数分别配属有一个序数,并且以第一序数开始,该第一序数对应于该链结构的第一区块和第二区块之间的双向链接的区块链结构(100)的第一双向链接,该函数集的函数根据预定的缔合规范而设置用于以升序分别单独配属该双向链接的区块链结构(100)的两个区块的双向链接并被用来计算取决于相应两个区块的链接函数(122)。

4.根据权利要求3所述的方法,其中,该区块无关的链接过程独立函数包含第M阶多项式,其中,M是自然数。

5.根据权利要求4所述的方法,其中,该区块无关的链接过程独立函数包含第M阶多项式与指数函数的关联,其中,该指数函数的指数包含大于等于2阶的多项式。

6.根据权利要求1所述的方法,其中,最后区块和附加区块(110,112)的组合的区块相关校验值的计算包括:将哈希函数用到存储在最后区块(110)中的数据和待存储在附加区块(112)中的数据(210)。

7.根据权利要求1所述的方法,其中,在该区块链结构(100)的区块中的数据分别被存储在一个正方形(TxT)矩阵结构(160,170)中,其中,T是大于等于2的自然数,其中,最后区块和附加区块(110,112)的组合的区块相关校验值的计算包括:

o计算第一矩阵结构(160)的每列(162)的和,其由存储在最后区块(110)中的数据和待存储在附加区块(112)中的数据(210)的两个矩阵结构(160,170)提供,

o计算第二矩阵结构(170)的每行(172)的和,其由存储在最后区块(110)中的数据和待存储在附加区块(112)中的数据(210)的两个矩阵结构(160,170)提供,

o计算第i列的和与第i行的和的组合和,其中,i是自然数并且从1变至T,

o通过所述组合和的相互关联来形成组合的区块相关校验值。

8.根据权利要求7所述的方法,其中,所述组合和的相互关联包括组合和的排列成行。

9.根据权利要求1所述的方法,其中,该双向链接的区块链结构(100)的前后相继的区块分别被双向相互链接,其中,两个双向相互链接的区块都分别包括共用的区块相关链接函数(122),其中,该共用的区块相关链接函数(122)分别包括在两个前后相继的区块中存储的数据的组合的区块相关校验值。

10.根据权利要求1所述的方法,其中,该区块链结构(100)被一个缩短的区块链结构(150)替换,其中,该缩短的区块链结构(150)被缩短了该区块链结构(100)的至少一个内链段(142),其中,该内链段(142)包含至少一个区块。

11.根据权利要求10所述的方法,其中,该方法还包括:

• 提供区块无关的若干变换函数,它们配置用于将区块相关的链接函数(122)的区块无关的链接过程独立函数相互变换,

• 检查缩短的区块链结构(150)是否一致,其中,该缩短的区块链结构(150)的从其之间取出该内链段(142)的两个紧邻区块的区块相关链接函数(122)的区块无关的链接过程独立函数在采用变换函数情况下被相互变换并且变换结果被检查是否一致。

12.根据权利要求11所述的方法,其中,该区块无关变换函数配置用于分别将区块相关链接函数(122)的区块无关的链接过程独立函数作为升算子变换为根据升序的下一较高的区块无关的链接过程独立函数和/或作为降算子分别将区块相关链接函数的区块无关的链接过程独立函数变换为根据升序的下一较低的区块无关链接过程独立函数。

13.根据权利要求11所述的方法,其中,该区块相关链接函数(122)$k_M(x)$具有以下形式:

$k_M(x) = g(D_N, D_{N+1})\, f_M(x)$

其中,$g(D_N, D_{N+1})$表示区块链结构(100)的第N和第(N+1)区块的组合的区块相关校验值,D_N表示存储在第N区块中的数据,D_{N+1}表示待存储在第(N+1)区块中的数据(210),其中,该区块无关链接过程独立函数$f_M(x)$具有以下形式:

$$f_M(x)=c\, H_M\left(\sqrt{b}\, x\right) e^{-\frac{1}{2} b x^2},$$

其中,M表示自然数,其明确无疑地对应配属于独立链接过程,其中,b和c分别表示一个固定参数,而x表示一个变量,其中,$H_M\left(\sqrt{b}\, x\right)$表示具有以下形式的厄米特多项式:

$$H_M\left(\sqrt{b}\, x\right)=(-1)^M e^{b x^2} \frac{d^M}{d\left(\sqrt{b}\, x\right)^M}\left(e^{-b x^2}\right)。$$

14.根据权利要求13所述的方法,其中,该变换函数具有以下形式的升算子:

$$\hat{a}^{\dagger}=\sqrt{\frac{b}{2}}\left(x-b^{-1}\frac{d}{dx}\right)$$

和以下形式的降算子:

$$\hat{a}=\sqrt{\frac{b}{2}}\left(x+b^{-1}\frac{d}{dx}\right)$$

并且在第N区块和第(N+L)区块之间存在一致性,在第N区块和第(N+L)区块之间取出包含区块N+1至N+L-1的内链段(142),此时假定适用

$$\frac{\left(\hat{a}^{\dagger}\right)^{L-1}k_M(x)}{k_{M+L-1}(x)}=\frac{c\,k_M(x)}{(\hat{a})^{L-1}k_{M+L-1}(x)}$$

其中,c是一个常数。

15.根据权利要求1所述的方法,其中,该待存储数据(210)包括标示数字编码文件的内容的数据,其中,待存储数据(210)的提供包括:借助通信接口(214)经由网络(240)从创建数字编码文件的计算机系统(250)中接收所述数据,其中,该方法还包括:

• 借助该通信接口(214)经由网络(240)从问询的计算机系统(220)中接收对区块链结构(100)的当前版本的问询,

• 响应于所接收的问询,借助该通信接口(214)经由网络(240)将扩展的区块链结构(130)发送至问询的计算机系统(220)。

16.根据权利要求1所述的方法,其中,该待存储数据(210)包含交易数据,其中,待存储数据(210)的提供包括借助通信接口(214)经由网络(240)自参与交易执行的计算机系统(250)接收所述数据,其中,该方法还包括:

• 借助该通信接口(214)经由网络(240)自问询的计算机系统(220)接收对区块链结构(100)的当前版本的问询,

• 响应于所接收的问询,借助该通信接口(214)经由网络(240)将扩展的区块链结构(130)发送至问询的计算机系统(220)。

17.根据权利要求1所述的方法,其中,该待存储数据(210)包含装置的状态数据,其中,待存储数据(210)的提供包括:借助通信接口(214)经由网络(240)自借助传感器采集状态数据的计算机系统(250)接收所述数据,其中,该方法还包括:

• 借助该通信接口(214)经由网络(240)自问询的计算机系统(250)接收对区块链结构(100)的当前版本的问询,

• 响应于所接收的问询,借助该通信接口(214)经由网络(240)将扩展的区块链结构(130)发送至问询的计算机系统(250)。

18.根据权利要求1所述的方法,其中,该待存储数据(210)包含标示数字编码文件的处理过程的数据,其中,该区块链结构(100)的提供包括:接收包含区块链结构(100)的待处理文件和从接收文件中读取区块链结构(100),其中,该待存储数据(210)的提供包括:接收文件的处理和数据生成,其中,该扩展的区块链结构(130)的存储包括:添加扩展的区块链结构(130)至处理文件和存储具有扩展的区块链结构(130)的处理文件。

19.根据权利要求18所述的方法,其中,该方法还包括:

• 借助通信接口(214)经由网络(240)自问询的计算机系统(220)接收对处理文件的问询,

• 响应于所接收的问询,借助该通信接口(214)经由网络(240)将具有扩展的区块链结

构(130)的处理文件发送至问询的计算机系统(220)。

20.一种用于在双向链接的区块链结构(100)中防篡改存储数据(210)的电子数据存储系统(200),其中,该数据存储系统包括处理器(202)和带有机读指令(204)的电子存储器(206),其中,通过处理器(202)的机读指令(204)的执行促使该数据存储系统(200)执行以下方法,该方法包括:

• 提供一个双向链接的区块链结构(100),

• 提供待存储数据(210),

• 生成一个用于扩展区块链结构(100)的附加区块(112),该附加区块包含待存储数据(210)并且设置用于与该区块链结构(100)的最后区块(110)双向链接,其中,该区块链结构(100)的最后区块(110)包含存储的数据,

• 计算用于最后区块(110)与附加区块(112)的双向链接的区块相关链接函数(122),其中,该链接函数(122)的计算包括:

o采用存储在最后区块(110)中的数据和待存储在附加区块(112)中的数据(210)来计算所述最后区块和附加区块(110,112)的组合的区块相关校验值,

o将组合的校验值与区块无关的链接过程独立函数进行关联,

• 将该区块相关链接函数(122)添加至最后区块(110),

• 将该区块相关链接函数(122)添加至附加区块(112),

• 存储被扩展了附加区块(112)的区块链结构(130)。

21.一种电信系统,它包括根据权利要求20所述的电子数据存储系统(200)和用于经由网络(240)通信的通信接口(214),其中,该待存储数据(210)的提供包括:借助通信接口(214)经由网络(240)接收数据,其中,所执行的方法还包括:

• 借助该通信接口(214)经由网络(240)自问询的电信系统(220)接收对区块链结构(100)的当前版本的问询,

• 响应于所接收的问询,借助该通信接口(214)经由网络(240)将扩展的区块链结构(130)发送至问询的电信系统(220)。

22.一种电信系统,其包括根据权利要求20所述的电子数据存储系统(200)和用于经由网络(240)通信的通信接口(214),其中,待存储数据(210)包含标示数字编码文件的处理过程的数据,其中,该区块链结构(100)的提供包括:接收包含区块链结构(100)的待处理文件和从所接收的文件中读取该区块链结构(100),其中,该待存储数据(210)的提供包括:接收文件的处理和数据生成,其中,该扩展的区块链结构(130)的存储包括:将扩展的区块链结构(130)添加至处理文件和存储具有扩展的区块链结构(130)的处理文件,其中,所执行的方法还包括:

• 借助该通信接口(214)经由网络(240)自问询的电信系统(220)接收对处理文件的问询,

• 响应于所接收的问询,借助该通信接口(214)经由网络(240)将具有扩展的区块链结构(130)的处理文件发送至问询的电信系统(220)。

采用双向链接的区块链结构在电子存储器中防篡改存储数据的方法、电子数据存储系统和电信系统

技术领域

[0001] 本发明涉及一种用于存储数据的方法和电子数据存储系统。本发明尤其涉及在双向链接的区块链结构中防篡改存储数据的方法和电子数据存储系统。

背景技术

[0002] 改变或甚至有目的地篡改电子存储器中的数字编码数据的可能性是一项技术挑战。

[0003] 从现有技术中知道了区块链结构，即用于数据保险的区块链结构。该区块链结构是单向链接区块链结构。例如相应的区块链结构被用于记录密码货币交易比如比特币支付系统。

[0004] 在此，区块链结构提供布置在区块中的数据组的可扩容名单。在现有技术中，各个区块的完整性通过单向链接在采用呈哈希值形式的单独区块密码校验值情况下被保险。由于每个区块包含在先区块的包括存储于在先区块内的密码校验值在内的密码校验值，故得到区块链接。在此，每个区块包括校验值，其基于所有在先区块的内容。因此难以事后篡改这种区块链，因为为此不是只须篡改一个单独区块，而是要篡改所有的后续区块，因为每个后续区块的校验值尤其基于待篡改的区块。如果待篡改的区块确实被篡改，则其校验值改变。改变的校验值不再匹配于后续区块的校验值，由此可以识别出篡改并且在借助校验值检查时引人注目。

[0005] 但是，已知的区块链结构仅实现单向链接和进而数据保险，因为在链接时总是仅考虑在先区块的数据内容。因此，可以依据链接来检查一个在先区块链结构的一个在先区块是否已被篡改。但无法检查在先区块链结构是否完整。尤其无法检查区块链结构的一部分是否有可能已被缩减。此外，无法检查最后区块是否已被篡改。

[0006] 在区块链结构的检查和保障中，还采用常见的哈希方法。区块链结构的单独区块通过哈希值单向相互关联。为了人们可以检查这种具有单向相互关联的区块的区块链结构是否被篡改，人们不仅需要单独区块的所有信息，还需要其各自的哈希值。此外，这种区块链结构的检查必须以相应区块链结构的第一区块开始并以最后区块结束。

发明内容

[0007] 本发明基于以下任务，提供一种改进的用于防篡改存储数据的方法。

[0008] 本发明所基于的任务分别利用独立权利要求的特征来完成。在从属权利要求中说明了本发明的实施方式。

[0009] 实施方式包括一种用于采用双向链接的区块链结构在电子存储器中防篡改存储数据的方法。该方法包括：

[0010] • 提供一个双向链接的区块链结构，

[0011] • 提供待存储数据，

[0012] • 产生一个附加区块以扩展该区块链结构，该附加区块可包含待存储数据并且设置用于与该区块链结构的最后区块双向链接，其中该区块链结构的最后区块包含存储数据，

[0013] • 计算用于最后区块与附加区块的双向链接的第一区块相关链接函数，其中该链接函数的计算包括：

[0014] o采用存储在最后区块中的数据和待存储在附加区块中的数据计算所述最后区块和附加区块的组合的区块相关校验值，

[0015] o将组合校验值与区块无关的链接过程独立函数关联，

[0016] • 添加第一区块相关链接函数至最后区块，

[0017] • 添加第一区块相关链接函数至附加区块，

[0018] • 存储被扩展了附加区块的区块链结构。

[0019] 实施方式可以具有以下优点，它们允许提供双向链接的区块链，其区块借助区块相关双向链接函数相互链接。所述链接此时允许双向检查区块链结构的真实性或是否篡改。此时该区块链结构并非只能在一个方向上、而是在两个方向上被检查。

[0020] 区块链结构是指形成区块链的数据结构。“区块链”是指整齐有序的数据结构，其包含多个相互链接的数据块。尤其是，区块链是指数据库，其完整性即防事后篡改的保险性通过在各自后随的数据组中存储在先数据组的校验值比如像哈希值得到保障。在此，校验值对应配属于在先数据组的内容并且明确无疑地表征该内容。如果在先数据组的内容被改变，则它不再满足校验特征，由此所述改变变得清楚可见。在已知的区块链结构情况下，比如该区块链的每个区块明确无疑地通过一个哈希值来识别并且关联区块链中的一个包含哈希值的在先区块。

[0021] 关于区块链的例子，参阅https://en.wikipedia.org/wiki/Block_chain_(database)和“掌握比特币”(见第7章区块链，第161页及后页)。区块链概念例如在2008年由中本聪(笔名)撰写的涉及密码货币比特币背景的白皮书中有描述(“比特币:P2P电子现金系统”(https://bitcoin.org/bitcoin.pdf))。在此实施例中，区块链的每个区块在其标头中包含所有在先区块标头的哈希。因此，区块顺序被单一确定并且出现链结构。通过如此实现的单独区块相互链接而做到了在没有同样修改所有后续区块的情况下无法实现事后修改原先区块。

[0022] 区块链的安全性例如可被如此提高，其被公布或者公众可获得，因此允许将现有区块链拷贝与其它公布的或可获得的同一区块链拷贝比较。

[0023] 数据校验值是对应于相应数据的值，其如此单一表征数据，即数据的完整性可以依据校验标记值被检查。呈校验和形式的校验值提供了例如一个值，其从原始数据来算出并且配置用于识别数据中的至少一个位缺陷。根据用于校验和的计算规则有多复杂，可以识别出超过一个的缺陷或者也可以修正。已知的校验值或者说校验和例如可以基于数据值的加和、横额、奇偶校验位、数据加权均值的计算或者更复杂的计算方法，比如像循环冗余检验或采用哈希函数。

[0024] 组合的区块相关校验值是这样的校验值，其不仅取决于第一区块的数据、也取决于第二区块的数据。根据实施方式，它在此可以是如下校验值，其在采用待考虑数据的关联的情况下来计算。根据其它实施方式，它可以是下述校验值，其被称为多个校验值的关联，

例如第一区块的数据的第一校验值与第二区块的数据的第二校验值的关联。这样的关联例如可以是算术关联如加、减、乘和/或除。

[0025] 在单向链接区块链结构的情况下，校验值在采用该区块链结构的一个区块情况下被计算并且被添加至与该区块单向链接的附加区块。依据添加区块的校验值，该区块的完整性或与添加区块单向链接的相应区块的数据的完整性可被检查。为此，例如在采用相应区块的数据情况下来复核该校验值并且将其与由添加区块提供的校验值比较。如果两个校验值一致，则该区块的完整性或与添加区块单向链接的相应区块的数据的完整性得以保证。

[0026] 在根据实施方式的双向链接的区块链结构情况下，校验值不仅在采用区块链结构的最后区块的数据情况下、也在采用要与该区块双向链接的附加区块的数据情况下被计算。依据添加区块的这种组合校验值，可根据添加区块的数据检查该区块完整性或与该添加区块双向链接的相应区块的数据完整性。为此，例如在采用相应区块的数据和添加区块的数据情况下复核包含该校验值的区块相关链接函数并且将其与由添加区块提供的区块相关链接函数比较。如果两个链接函数一致，则该区块的完整性或与添加区块双向链接的相应区块的数据的完整性就像附加区块完整性或附加区块数据完整性那样得以保持。如果双向链接函数不仅被添加至附加区块、也被添加至与附加区块双向链接的区块，则也可以基于要被添加至区块链结构的相应区块的双向链接函数进行完整性检查。换言之，在两个区块双向链接时，可以不仅基于存储在两个区块中第一个中的双向链接函数进行完整性检查，也可基于存储在两个区块中第二个中的双向链接函数进行完整性检查。

[0027] 依据与添加区块双向链接的最后区块的加入区块相关双向链接函数计算中的组合校验值，可以不同于已知的单向链接区块链结构地也识别出区块链结构是否被缩减。因为校验值在已知的单向链接区块链结构情况下总是仅包含关于在先区块的信息，故基于这种校验值无法识别出是否存在后续区块。因此，也无法识别出后续区块在篡改过程中是否被改变、替换或去除。与此相比，双向链接函数的组合校验值根据实施方式分别包含关于两个相互链接的区块的信息。此外，该链接函数被分别添加至两个相应区块中的每一个。如果添加区块在篡改过程中被改变、替代或去除，则这可以依据与添加区块双向链接的区块的链接函数来识别。

[0028] 根据实施方式，该区块链结构的每个内区块、即除了第一区块和最后区块外的所有区块包括至少两个区块相关链接函数，因为每个内区块通过不同的链接函数与一个在先区块和一个后续区块链接。不同于已知的仅基于哈希值的区块链结构链接方法，在这里没有添加单值至区块，而是添加与至少一个不是针对链接所确定的变量相关的函数。如果一个区块包含多个区块相关链接函数，则它们可以相互关联。因此，从各个连接的相互关联的链接函数的范围内得到一个共用的合成链接函数，其完整包含各个连接的所有参与其中的链接函数的信息。相应的关联可以是例如算术关联如加、减、乘和/或除。

[0029] 根据实施方式，在计算校验值时被考虑进来的数据包含相应区块数据的真实子集。根据其它实施方式，在计算校验值时被考虑进来的数据包含相应区块的所有数据。根据实施方式，被考虑用于计算组合的区块相关校验值的区块链结构的最后区块的数据包含最后区块与区块链结构的倒数第二区块的区块相关链接函数。根据实施方式，最后区块的数据(这些数据在组合的区块相关校验值的计算中被考虑进来)不包含：“最后区块与倒数第

二区块的链接”的链接函数。

[0030] 根据实施方式，区块链结构的最后区块还包括最后区块与区块链结构的倒数第二区块的双向链接的第二区块相关链接函数，其中，将第一区块相关链接函数添加至最后区块包括将第一区块相关链接函数与第二区块相关链接函数关联。

[0031] 根据实施方式，区块链结构的每个内区块、即除了第一区块和最后区块外的所有区块包含至少两个区块相关链接函数，因为每个所述内区块通过不同的链接函数与一个在先区块和一个后续区块链接。不同于已知的仅基于哈希值的区块链结构链接方法，在这里未将单值添加至区块，而是添加与至少一个并非针对链接被确定的变量相关的函数。如果一个区块包含多个区块相关链接函数，则它们可以相互关联。因此从各个连接的相互关联的链接函数的范围内得到一个共用的合成链接函数，其完整包含各个连接的所有参与其中的链接函数的信息。相应关联例如可以是算术关联如加、减、乘和/或除。

[0032] 根据实施方式，“区块无关链接过程独立函数”是：包含许多区块无关链接过程独立函数的函数集中的一个函数，其中，该函数集的每个函数分别配属有一个序数，并且该函数集的这些函数按照以第一序数开始的方式(该第一序数对应于在链结构的第一区块与第二区块之间的双向链接区块链结构的第一双向链接)，根据预定的缔合规范设置用于以升序分别单独对应配属于双向链接区块链结构的两个区块的双向链接并且被用来计算与相应两个区块相关的链接函数。

[0033] 实施方式还可以具有以下优点，通过组合校验值与一个区块无关链接过程独立函数的关联，可以实现借助更复杂、安全的链接函数的安全的链接方法。在此，区块无关链接过程独立函数是指具有至少一个变量的数学函数。该函数就针对每个链接过程、即对于区块链结构的两个区块之间的每个双向连接采用不同的函数而言是链接过程独立的。根据实施方式，所有链接过程独立函数此时包含相同的变量。根据实施方式，该链接过程独立函数从同一个综合函数或泛函推导出，从而合成链接过程独立函数形成一个函数集。根据实施方式，该函数集的函数根据预定的缔合规范对应配属于区块链结构的连接。根据实施方式，函数集的函数根据区块链结构的连接顺序被规整。基于这种规整，可以单一确定哪个链接过程独立函数被用于哪个链接过程。根据实施方式，在区块链结构的区块之间的双向链接因此不仅与两个要相互链接的区块的数据内容相关，也与区块链结构内的区块之间的相应连接的优先次序、即在区块链结构内的区块位置相关。

[0034] 根据实施方式，区块无关链接过程独立函数包含第M阶的多项式，其中，M是形成对应配属于该函数的序数的自然数。

[0035] 根据实施方式，区块无关链接过程独立函数包含第M阶多项式与指数函数的关联，其中，指数函数的指数包含大于等于2阶的多项式。相应的关联例如可以是乘。

[0036] 实施方式可以具有以下优点，区块无关链接过程独立函数的序数在采用多项式阶数情况下被确定。它提供了链接函数与在形成区块链结构时的单独链接过程的清晰对应配属关系。例如，多项式阶数可以与序数相等。因此，带有序数1的区块链结构第一连接对应于第1阶多项式或者包含第一阶多项式的链接函数。根据其它实施方式，序数可以作为多项式阶数减去预定数字来确定。在此情况下，它例如是数字10，因此带有序数1的区块链结构第一连接对应配属于第11阶多项式或包含第11阶多项式的链接函数。根据实施方式，关于区块链结构的单独连接的缔合规范还确定了多项式系数具有哪个值。相应的规范可以通过共

用的综合函数来确定。

[0037] 根据实施方式，对于被用来形成区块相关链接函数、确切说是区块无关链接过程独立函数的共用综合函数，规定了升算子和降算子，它们能以一阶或多阶升降任何链接过程独立函数。将这种升算子或降算子用到区块无关链接过程独立函数因此导致了更高阶或更低阶的区块无关链接过程独立函数，在这里，原始函数还有最终函数都被共用综合函数涵盖。

[0038] 基于多项式的区块无关链接过程独立函数的使用还可以有以下优点，相应的多项式能相互变换。通过求导运算，可以将第M阶多项式变换为第(M-1)阶多项式。另外，第M阶多项式可以通过乘以相应变量例如x被变换为第(M+1)阶多项式。根据实施方式，变换函数包含相应变量即第一阶多项式例如x和求导算子例如$\frac{d}{dx}$的组合。以下，将第M阶函数如第M阶多项式变换为第(M+1)阶函数的变换函数被称为升算子，并且将第M阶函数如第M阶多项式变换为第(M-1)阶函数的变换函数被称为降算子。

[0039] 根据实施方式，升算子和降算子可以将第M阶多项式变换为第(M+P)阶或第(M-P)阶多项式，其中P表示大于等于2的自然数。根据实施方式，变换函数在此情况下包含相应变量的第P次幂即第一阶多项式如x^P和该阶数P的求导算子例如$\frac{d^P}{dx^P}$的组合。

[0040] 根据实施方式，最后区块和附加区块的组合的区块相关校验值的计算包括使用哈希函数到存储在最后区块中的数据和待存储在附加区块中的数据。实施方式可以具有以下优点，使用哈希值以形成组合校验值提供了一种简单可靠的方法用于给相互链接的区块的数据配属单一校验值。

[0041] 根据实施方式，在区块链结构的区块中的数据分别以正方形(TxT)矩阵结构来存储，其中，T是大于等于2的自然数。另外，最后区块和附加区块的组合的区块相关校验值的计算包括：

[0042] o计算第一矩阵结构的每列的和，其由存储在最后区块中的数据和待存储在附加区块中的数据的两个矩阵结构提供，

[0043] o计算第二矩阵结构的每行的和，其由存储在最后区块中的数据和待存储在附加区块中的数据的两个矩阵结构提供，

[0044] o计算由第i列的和与第i行的和构成的组合和，其中i是自然数且从1变为T，

[0045] o通过组合和的相互关联形成组合的区块相关校验值。

[0046] 实施方式可以具有以下优点，通过用于两个要相互链接的区块的不同的加和规则，例如一方面是各个列的求和且另一方面是各个行的求和，最终的组合校验值不仅包含关于要相互链接的区块的数据的信息，也包含关于其顺序的信息。如果两个区块的顺序被交换，则例如对于过去在先的区块不是进行按列的求和、而是按行的求和，而对于过去在后但现在在先的区块进行按列的而不是按行的求和。

[0047] 根据实施方式，待相互链接的区块也可以具有大小不同的矩阵结构。例如，一个区块的数据存储在一个(VxW)矩阵结构中，而另一区块的数据存储在一个(XxY)矩阵结构中，其中，V、W、X、Y是大于等于2的自然数。在此情况下，可以为了组合校验值的形成而确定数字V、W、X或Y中的哪个数最大，行的数量V或X或列的数量W或Y。如果行数和列数相同，则不需要

附加方法步骤。如果列数和/或行数对于两个矩阵结构是不同的，则矩阵结构分别被扩展如此多的行和/或列，即所有的列数和行数与之前确定的最大数相同。此时，所有补充的矩阵单元配属有一个固定的通配值如0值。结果，人们因此获得两个同尺寸的方形矩阵结构，用于方形(TxT)矩阵结构的前述方法可被用于上述方形矩阵结构。

[0048] 根据实施方式，组合和的相互关联包含组合和的成行排列。实施方式可以具有以下优点，它们提供简单和明确的用于形成组合校验值的方法。

[0049] 根据实施方式，双向链接区块链结构的前后相继的区块分别被双向相互链接，其中两个双向相互链接的区块分别都包括共用区块相关链接函数，其中共用区块相关链接函数分别包括存储在两个前后相继区块中的数据的组合的区块相关校验值。

[0050] 根据实施方式，该区块链结构被缩短的区块链结构替代，其中缩短的区块链结构被缩短了区块链结构的至少一个内链段，其中该内链段包括至少一个区块。

[0051] 实施方式可以具有以下优点，通过缩短该区块链结构例如可以节省存储位。此外，可以依据在其间取出链段的链接函数来确定有多少区块包含相应的段。如果例如取出L个区块，则L次使用升算子至在取出区块之前的区块链结构最后区块的链接过程独立链接函数必然导致在取出区块后的区块链结构第一区块的链接过程独立函数。同样情况相似地适用于L次使用降算子至在取出区块后的第一区块的链接过程独立函数。

[0052] 实施方式还可以具有以下优点，通过缩短区块链结构例如可以取出含有安全敏感数据的区块，以保护其免于未准许的访问。链接过程独立函数的使用允许确定取出了多少区块。此外，组合的区块相关校验值的使用允许随后检查取出区块的真实性或完整性。如果取出区块随后或附加地被提供，则可以依据链接函数来检查它实际上是否是取出区块。另外，可以在只提供取出区块时依据链接过程独立函数确定，所述区块从区块链结构的哪个区域中被取出。另外，如果从中推导出链接过程独立函数的共用综合函数是区块链独立选择的，则可以依据该链接函数来确定取出区块属于哪个区块链结构。共用综合函数因此是相应区块链结构的一种“指纹”，其与存储在区块链结构中的数据无关。这种可能性尤其可能在存储在区块链结构的区块中的数据被加密时是有利的。

[0053] 如果一个内链段被取出，则对于区块链结构的在其间取出相应内链段的两个区块因所述取出而分别缺少一个后随区块或在先区块，该区块因双向链接而包含相同的区块相关链接函数。根据实施方式，缩短的区块链结构的在其间取出内链段的这两个区块用一个组合的双向链接函数来链接，组合的双向链接函数包含所取出的内链段的区块的所有区块相关链接函数的组合。

[0054] 实施方式可具有以下优点，区块链结构可被缩短，但未损失与取出区块的链接相关的区块相关信息。内链段的区块的区块相关链接函数的组合例如可以是关联，比如算术关联。这种算术关联例如可以包括加、减、乘和/或除。区块相关链接函数分别与将其链接的区块数据内容或者被单一配属于该区块的数据内容相关。作为内链段的区块的所有区块相关链接函数的组合，将在内链段取出后留下的两个无直接链接的区块相互链接的组合的双向链接函数因此包含关于所有在相应区块之间取出的内链段区块的所有数据内容的信息。

[0055] 根据实施方式，该方法还包括：

[0056] • 提供区块无关变换函数，其配置用于将区块相关链接函数的区块无关链接过程独立函数相互变换，

[0057] • 检查缩短的区块链结构是否一致，其中该缩短的区块链结构的在其间取出内链段的两个紧邻区块的区块相关链接函数的区块无关链接过程独立函数在使用变换函数情况下被相互变换并且变换结果被检查是否一致。

[0058] 实施方式可以具有以下优点，提供以下可能，从区块链结构中取出安全关键信息，但余下的缩短的区块链结构还仍可被同时检查。

[0059] 根据实施方式，区块无关变换函数被配置用于将区块相关链接函数的区块无关链接过程独立函数分别作为降算子根据升序变换为下一较高的区块无关链接过程独立函数和/或作为降算子根据升序分别将区块相关链接函数的区块无关链接过程独立函数变换为下一较低的区块无关链接过程独立函数。

[0060] 实施方式可以具有以下优点，在使用升算子和降算子情况下提供一种高效的检查方法。

[0061] 根据实施方式，区块相关链接函数kM(x)具有如下形式：

[0062] kM(x)＝g(DN,DN+1)fM(x)

[0063] 其中，g(DN,DN+1)表示区块链结构的第N和第(N+1)区块的组合的区块相关校验值，D_N表示存储在第N区块中的数据，D_{N+1}表示待存储在第(N+1)区块中的数据，其中，区块无关链接过程独立函数fM(x)具有如下形式：

[0064] $$f_M(x)=c\,H_M\left(\sqrt{b}\,x\right)e^{-\frac{1}{2}b\,x^2},$$

[0065] 其中，M表示自然数，其单一地对应配属于独立链接过程，其中b和c分别表示一个固定参数，x表示一个变量，其中$H_M\left(\sqrt{b}\,x\right)$表示以下形式的厄米特多项式：

[0066] $$H_M\left(\sqrt{b}\,x\right)=(-1)^M e^{b\,x^2}\frac{d^M}{d\left(\sqrt{b}\,x\right)^M}\left(e^{-b\,x^2}\right)。$$

[0067] 实施方式可以具有以下优点，通过使用包含厄米特多项式的区块相关链接函数，可以提供高效的检查方法。

[0068] 根据实施方式，变换函数包含以下形式的升算子：

[0069] $$\hat{a}^{\dagger}=\sqrt{\frac{b}{2}}\left(x-b^{-1}\frac{d}{dx}\right)$$

[0070] 和以下形式的降算子：

[0071] $$\hat{a}=\sqrt{\frac{b}{2}}\left(x+b^{-1}\frac{d}{dx}\right).$$

[0072] 另外，在以下条件下存在在其间取出包含区块N+1至N+L-1的链段第N区块与第(N+L)区块之间的一致性，即

[0073] $$\frac{\left(\hat{a}^{\dagger}\right)^{L-1}k_M(x)}{k_{M+L-1}(x)}=\frac{c\,k_M(x)}{(\hat{a})^{L-1}\,k_{M+L-1}(x)}$$

[0074] 其中c是常数。

[0075] 根据实施方式，区块无关链接过程独立函数fM(x)例如是：

[0076] $$f_M(x)=\left(\frac{b}{\pi}\right)^{\frac{1}{4}}\frac{1}{\sqrt{2^M\,M!}}\,H_M\left(\sqrt{b}\,x\right)e^{-\frac{1}{2}b\,x^2}.$$

[0077] 在此情况下适用的是$\hat{a}^\dagger\,f_M(x)=\sqrt{M+1}\;f_{M+1}(x)$和$\hat{a}\,f_M(x)=\sqrt{M}\;f_{M-1}(x)$。

[0078] 如果例如在区块N和区块N+3之间取出两个区块N+1和N+2，则剩余区块N如之前一样包括区块N和区块N+1之间双向连接的区块相关双向链接函数kM(x)＝g(DN,DN+1)fM(x)。剩余区块N+3与之前一样包括区块相关双向链接函数kM+2(x)＝g(DN+2,DN+3)fM+2(x)。

[0079] 如果组合校验值与x无关，则适用以下变换规则：

[0080] $$\hat{a}^\dagger\,g(D_N,D_{N+1})=g(D_N,D_{N+1})\,\hat{a}^\dagger,$$

[0081] $$\hat{a}\,g(D_N,D_{N+1})=g(D_N,D_{N+1})\,\hat{a}。$$

[0082] 根据实施方式的不同，组合校验值g(DN,DN+1)可以作为相应数据的两个校验值的关联即g(DN,DN+1)＝g(DN)°g(DN+1)或者作为相应数据本身的关联的校验值存在，即g(DN,DN+1)＝g(DN°DN+1)。

[0083] 对于两次使用升算子到kM(x)，适用的是：

[0084] $$\left(\hat{a}^\dagger\right)^2 k_M(x)=g(D_N,D_{N+1})\left(\hat{a}^\dagger\right)^2 f_M(x)=g(D_N,D_{N+1})\sqrt{M+1}\,\sqrt{M+2}\,f_{M+2}(x)$$

[0085] 对于两次使用降算子到kM+2(x)，适用的是：

[0086] $$(\hat{a})^2\,k_{M+2}(x)=g(D_{N+2},D_{N+3})\,(\hat{a})^2\,f_{M+2}(x)=g(D_{N+2},D_{N+3})\sqrt{M+2}\,\sqrt{M+1}\,f_M(x)。$$

[0087] 为此适用的是：

[0088] $$\frac{k_{M+2}(x)}{\left(\hat{a}^\dagger\right)^2 k_M(x)}=\frac{g(D_{N+2},D_{N+3})}{g(D_N,D_{N+1})\;\sqrt{M+1}\,\sqrt{M+2}}=\frac{d_{M+2}}{\sqrt{M+1}\,\sqrt{M+2}},$$

[0089] 此时，dM+2＝g(DN+2,DN+3)/g(DN,DN+1)并且

[0090] $$\frac{k_M(x)}{(\hat{a})^2\,k_{M+2}(x)}=\frac{g(D_N,D_{N+1})}{g(D_{N+2},D_{N+3})\,\sqrt{M+2}\,\sqrt{M+1}}=\frac{{d_{M+2}}^{-1}}{\sqrt{M+1}\,\sqrt{M+2}}。$$

[0091] 由此得出：

[0092] $$\frac{\sqrt{M+1}\,\sqrt{M+2}\,k_{M+2}(x)}{\left(\hat{a}^\dagger\right)^2 k_M(x)}\;\frac{\sqrt{M+1}\,\sqrt{M+2}\;k_M(x)}{(\hat{a})^2\,k_{M+2}(x)}=1。$$

[0093] 对于在第N区块和第(N+L)区块之间取出L-1区块的一般化情况，伴随kM+L-1(x)＝g(DN+L-1,DN+L)fM+L-1(x)而得到：

[0094] $$\left(\hat{a}^\dagger\right)^{L-1}k_M(x)=g(D_N,D_{N+L})\left(\hat{a}^\dagger\right)^{L-1}f_M(x)=g(D_N,D_{N+L})\sqrt{\frac{(M+L-1)!}{M!}}\,f_{M+L-1}(x)$$

[0095] 和

[0096] $$(\hat{a})^{L-1}\, k_{M+L-1}(x)=g(D_{N+L-1},D_{N+L})\,(\hat{a})^{L-1}\, f_{M+L-1}(x)=g(D_{N+L})\sqrt{\frac{(M+L-1)!}{M!}}\, f_M(x),$$

[0097] 由此得出：

[0098] $$\frac{k_{M+L-1}(x)}{(\hat{a}^{\dagger})^{L-1}\, k_M(x)}=\sqrt{\frac{M!}{(M+L-1)!}}\,\frac{g(D_{N+L-1},D_{N+L})}{g(D_N,D_{N+L})}=\sqrt{\frac{M!}{(M+L-1)!}}\, d_{M+L-1}$$

[0099] 和

[0100] $$\frac{k_M(x)}{(\hat{a})^{L-1}\, k_{M+L-1}(x)}=\sqrt{\frac{M!}{(M+L-1)!}}\,\frac{g(D_{N+L-1},D_{N+L})}{g(D_{N+L-1},D_{N+L})}=\sqrt{\frac{M!}{(M+L-1)!}}\, d_{M+L-1}{}^{-1}$$

[0101] 此时，dM+2＝g(DN+L-1,DN+L)/g(DN+L-1,DN+L)或者

[0102] $$\left[\sqrt{\frac{(M+L-1)!}{M!}}\,\frac{k_{M+L-1}(x)}{(\hat{a}^{\dagger})^{L-1}\, k_M(x)}\right]\left[\sqrt{\frac{(M+L-1)!}{M!}}\,\frac{k_M(x)}{(\hat{a})^{L-1}\, k_{M+L-1}(x)}\right]=1。$$

[0103] 实施方式可以具有以下优点，通过使用相应的升算子和相应的降算子，提供用于相互变换不同阶的链接过程独立函数的高效的变换方法。如果已经知道取出区块的数量，则可以检查剩余区块的一致性。另一方面，可以通过逐步提升升算子和/或降算子的使用来确定取出区块的数量。一旦满足在先限定的一致性标准，则升算子和/或降算子的使用次数对应于取出区块的数量。

[0104] 根据实施方式，待存储数据包含标示数字编码文件内容的数据，其中待存储数据的提供包括借助通信接口经由网络自创建数字编码文件的计算机系统接收数据，其中该方法还包括：

[0105] • 借助通信接口经由网络自问询的计算机系统接收对区块链结构的当前版本的问询，

[0106] • 响应于收到的问询，借助通信接口经由网络将扩展的区块链结构发送至问询的计算机系统。

[0107] 实施方式可以具有以下优点，依据录入在区块链结构中的数据可以检查数字编码文件的完整性。对于现有的数字编码文件，标示该文件内容的数据可被计算。例如可以计算数字编码文件内容的哈希值。该数据可以与区块链结构相比较：如果区块链结构包括相应的数据，则数字编码文件的完整性被确认并且被认定为是真实的。如果区块链结构不包含相应数据，则数字编码文件的完整性被否认。区块链结构此时可以带来以下优点，在仅包含数字编码文件的哈希值时，其大小可被保持紧凑。此外，无法依据数字编码文件的哈希值推断相应文件的内容，由此提高安全性。最后，区块链结构的当前版本例如可以经由网络被下载到便携式移动电信设备，并且只在没有网络通信可用时(即便携式移动电信设备处于离线模式时)，才被用于检查数字编码文件。

[0108] “文件”尤其是指消息通知、文本、证件、证书或身份证、有价文件或安全文件且尤其是权利文件、尤其是纸质和/或塑料质文件例如像电子身份证尤其是护照、个人身份证、

签证、驾驶证、行驶证、车辆出厂证、健康卡或者公司证或者其它ID证件、芯片卡、支付手段尤其是钞票、银行卡或信用卡、发票或其它资格证。尤其是，该文件可以是机读旅行证件，例如像国际民用航空组织(ICAO)和/或BSI标准化的文件。证件是以文本形式或字符形式的说明，其固化一定的事实情况或实情。另外，证件可以证实证件的签发者。

[0109] 数字编码文件是指用于电子数据处理的数据构造，其包含数字编码数据。在此情况下，它尤其可以是任何文件格式的电子文件，比如像文本文件、表格文件、声频文件、图形文件和/或视频文件。根据实施方式，该电子文件是可执行的或不可执行的。数字编码文件例如可以是如下文件，其通过具有实体文件体的文件的数字化、即将实体文件体所含数据转换为二进制码而以文件形式编制或转为文件形式。尤其是这种文件的有效性与固定对应的文件体的存在与否无关。

[0110] 根据实施方式，可以例如创建数字编码文件，做法是在计算机上生成具有相应文件的数据的文件。另外，虚拟文件例如也可以通过实体文件体比如纸质文件的扫描录入或去色来创建。

[0111] 根据实施方式，待存储数据包含交易数据，其中待存储数据的提供包括借助通信接口经由网络自参与交易执行的计算机系统接收数据，其中该方法还包括：

[0112] • 借助通信接口经由网络自问询的计算机系统接收对区块链结构的当前版本的问询，

[0113] • 响应于收到的问询，借助该通信接口经由网络将扩展的区块链结构发送至问询的计算机系统。

[0114] 实施方式可以具有以下优点，依据录入在区块链结构中的数据可以记录交易。所述交易例如可以是经典货币的密码货币交易、销售、货运、所有权转让或物和/或数字编码文件的转交。

[0115] 根据实施方式，待存储数据包含装置的状态数据，其中待存储数据的提供包括借助通信接口经由网络自用传感器测知状态数据的计算机系统接收数据，其中该方法还包括：

[0116] • 借助通信接口经由网络自问询的计算机系统接收对区块链结构的当前版本的问询，

[0117] • 响应于收到的问询，借助通信接口经由网络将扩展的区块链结构发送至问询的计算机系统。

[0118] 实施方式可以具有以下优点，依据录入在区块链结构中的状态数据可以记录下装置的状态和/或状态历史。这种装置例如可以是生产装置、计算机系统部件、锁具、访问控制装置或车辆。“车辆”在此是指移动交通工具。这种交通工具例如可以用于运输货物(货运)、设备(机器或辅助手段)或人员(客运)。车辆尤其也包括机动化交通工具。车辆例如可以是陆上运输工具、水面运输工具和/或空中运输工具。陆上运输工具例如可以是:汽车，比如像轿车、公共汽车或载货汽车、机动两轮车比如像摩托车、小型摩托车、电动滑轮车或电动自行车、农用拖拉机、叉车、高尔夫移动小车、吊车。另外，陆上运输工具也可以是有轨车辆。水面运输工具例如可以是船或艇。另外，空中运输工具例如可以是飞机或直升机。车辆也尤其是指汽车。

[0119] “传感器”在此是指用于获得测量数据的元件。测量数据是如下数据，其定性或定

量展现被测物的物理性能或化学性能，例如像热量、温度、湿度、压力、声场强度、电磁场强、亮度、加速度、位置变化、pH值、离子强度、电化学势和/或其物质特性。测量数据借助物理作用或化学作用来测知并且被转换为可进一步电子处理的电信号。此外，测量数据、状态和/或状态变化可以由电子设备或因使用者使用而被展现。

[0120] 状态数据也可以根据实施方式包含关于由装置执行的功能的数据。例如因此可以记录下由生产装置执行的制造过程和/或加工过程。另外，例如可以记录访问控制装置的动作，其中所记录的数据可能包含关于谁在何时通过访问控制装置获得过对保险区域的访问的信息。

[0121] 根据实施方式，待存储数据包含标示数字编码文件的处理过程的数据，其中区块链结构的提供包括包含区块链结构的待处理文件的接收和从接收文件中读取区块链结构，在这里，“待存储数据的提供”包括：接收文件的处理和数据生成，其中，“扩展的区块链结构的存储”包括：添加扩展的区块链结构至经过处理的文件；和存储带有扩展的区块链结构的经过处理的文件。

[0122] 实施方式可具有以下优点，依据录入区块链结构中的数据，可记录数字编码文件的处理过程。例如可记录谁在何时访问文件和在文件上是否作出改动或何种改动。另外，例如可以记录下文件复制过程并且将扩展的区块链结构添加至创建的拷贝。在此情况下，区块链结构包括创建拷贝的来源历史。

[0123] 根据实施方式，该方法还包括：

[0124] • 借助通信接口经由网络自问询的计算机系统接收对经过处理的文件的问询，

[0125] • 响应于接收到的问询，借助通信接口经由网络将包含扩展的区块链结构的经过处理的文件发送至问询的计算机系统。

[0126] 实施方式可以具有以下优点，依据该区块链结构可以完成和/或复查经过处理的文件的处理历史和/或来源历史。

[0127] 所述文件可尤其是消息通知比如呈网页、与网页链接的或集成到网页中的文件或帖子。网页或者说网络文件、互联网页或网页是指通过互联网提供的文件，其例如由网络服务器提供并可利用用户计算机系统的浏览器在说明统一资源定位符(URL)情况下被调用。例如它是HTML文件。帖子在此是指在互联网平台比如像社交媒体平台、网络论坛或博客上的单独稿件。

[0128] 实施方式包括一种用于在双向链接区块链结构中防篡改存储数据的电子数据存储系统。该数据存储系统包括处理器和带有机读指令的电子存储器，其中由处理器执行机读指令促使该数据存储系统执行下述方法，其包括：

[0129] • 提供双向链接的区块链结构，

[0130] • 提供待存储数据，

[0131] • 生成用于扩展区块链结构的附加区块，附加区块包含待存储数据并且设置用于与区块链结构的最后区块双向链接，其中该区块链结构的最后区块包含存储数据，

[0132] • 计算用于最后区块与附加区块双向链接的区块相关链接函数，其中该链接函数的计算包括：

[0133] o采用存储在最后区块中的数据和待存储在附加区块中的数据计算最后区块和附加区块的组合的区块相关校验值，

[0134] o将组合校验值与区块无关链接过程独立函数关联，

[0135] •添加区块相关链接函数至最后区块，

[0136] •添加区块相关链接函数至附加区块，

[0137] •存储被扩充了附加区块的区块链结构。

[0138] 根据实施方式，该电子数据存储系统配置用于执行所述用于防篡改存储数据的方法的前述实施方式中的一个或多个。

[0139] 根据实施方式，电子数据存储系统包括文件系统。文件系统提供在数据存储器上的档案管理。数据比如数字编码文件可以作为文件被存储在数据存储器上。另外，所述文件可被读取、改变或删除。

[0140] 根据实施方式，电子数据存储系统包括数据库。数据库或数据库系统表示电子数据管理系统。数据库系统允许高效、无矛盾且长期地存储大数据集并且以不同的按需显示形式提供所需子集给使用者和应用程序。该数据库系统例如包括数据库管理系统和狭义上的数据库或数据基础。数据库管理系统提供用于管理数据基础的数据的管理软件。管理软件在内部规整数据的结构化存储并且控制数据库的所有读写访问。数据基础包含待管理数据集。数据比如数字编码文件在此情况下例如作为数据基础的一部分被存储。

[0141] 存储器例如可以包括可更换式存储器，即用于计算机系统的非固定安装的、可更换的和/或便携的数据载体。可更换式存储器例如包括蓝光光碟、CD、软盘、DVD、HD-DVD、磁带、MO/MOD、固态驱动器(SSD)、存储卡、U盘或可更换式硬盘。

[0142] 实施方式包括一种电信系统，其包含前述的电子数据存储系统和用于经由网络通信的通信接口，其中待存储数据的提供包括借助通信接口经由网络接收数据，其中所执行的方法还包括：

[0143] •借助通信接口经由网络自问询的电信系统接收对区块链结构的当前版本的问询，

[0144] •响应于收到的问询，借助通信接口经由网络将扩展的区块链结构发送至问询的电信系统。

[0145] 电信系统例如是配置用于经由网络通信的计算机系统。

[0146] 网络例如可以是局部网尤其是局域网(LAN)、专用网络尤其是内联网或虚拟专用网络(VPN)。例如，该计算机系统可以具有用于连接至WLAN的标准无线电接口。此外，它可以是公众网络例如像互联网。此外，它例如可以是数字蜂窝式移动无线电网络。

[0147] “计算机系统”在此是指如下设备，其借助可编程的计算规范并在采用电子电路情况下处理数据。“程序”或“程序指令”在此不限制地是指任何类型的计算机程序，其包含用于控制计算机功能的机读指令。

[0148] 计算机系统可以包括用于与网络通信的接口，其中，该网络可以是专用网络或公众网络，尤其是互联网或其它的通信网。根据实施方式的不同，所述通信也可以借助移动无线电网络建立。

[0149] 计算机系统例如可以是移动电信设备、尤其是智能手机、便携式计算机例如像笔记本电脑或掌上电脑、个人数字助理等。此外，它例如可以是智能手表或智能眼镜。此外，它可以是固定式计算机系统例如像个人电脑或绑定到客户端-服务器环境的服务器。它尤其可以是带有数据库管理系统的服务器，该数据库管理系统管理包含数据的数据库。

[0150] “存储器”或“数据存储器”在此不仅是指易失电子存储器或数字存储介质，也是指非易失电子存储器或数字存储介质。

[0151] “非易失存储器”在此是指用于长久存储数据的电子存储器。非易失存储器可以作为不可变存储器来配置，其也被称为只读存储器(ROM)，或者是可变存储器，其也被称为非易失存储器(NVM)。尤其是，它在此可以是EEPROM例如闪存EEPROM，简称闪存。非易失存储器的特点是，在供电装置关断后也保持留存存储于其上的数据。

[0152] “易失电子存储器”在此是指用于暂时存储数据的存储器，其特征是，所有数据在供电装置关停后丢失。它在此情况下尤其可以是易失直接存取存储器，其也被称为随机存取存储器(RAM)，或者是处理器的易失工作存储器。

[0153] “处理器”在此且在以下是指用于执行程序指令的逻辑电路。逻辑电路可在一个或多个独立元件、尤其是芯片上实现。“处理器”尤其是指由多个处理器核心和/或多个微处理器构成的微处理器或微处理器系统。

[0154] “接口”或者说“通信接口”在此是指如下接口，可经此收发数据，其中该通信接口能以接触或非接触的方式来配置。通信接口可以是内部接口或者外部接口，其例如借助电缆或以无线方式与对应的设备相连。用于无线通信的通信接口是指配置用于无线收发数据的通信接口。通信例如可以按照RFID标准和/或NFC标准比如像蓝牙来进行。此外，该通信接口可以配置用于经由局域无线电网络通信，例如按照IEEE-802.11族标准和/或Wi-Fi。

[0155] 接口例如可以作为无线电接口来配置，其允许经由数字蜂窝移动无线电网络的通信，其可以按照移动无线电标准例如像GSM、UMTS、LTE、CDMA或其它标准构成。

[0156] 通信一般例如可以经由网络进行。“网络”在此是指具有通信连接的每种传输介质，这种连接允许在至少两个计算机系统之间的通信。网络例如可以是局部网、尤其是局域网(LAN)、专用网尤其是内联网或者虚拟专用网络(VPN)。例如该计算机系统可以具有用于连接至WLAN的标准无线电接口。此外，它可以是公用网络例如像互联网。

[0157] 实施方式包括一种电信系统，其包括前述的电子数据存储系统和用于经由网络通信的通信接口，其中待存储数据包含标示数字编码文件的处理过程的数据，其中区块链结构的提供包括包含该区块链结构的待处理文件的接收和从接收文件中读取区块链结构，其中待存储数据的提供包括接收文件的处理和数据生成，其中扩展的区块链结构的存储包括添加扩展的区块链结构至经过处理的文件和存储包含扩展的区块链结构的经过处理的文件，其中所执行的方法还包括：

[0158] • 借助通信接口经由网络自问询的电信系统接收对经处理的文件的问询，

[0159] • 响应于收到的问询，借助通信接口经由网络将包含扩展的区块链结构的经过处理的文件发送至问询的电信系统。

[0160] 根据实施方式，针对收到发送请求来进行数字编码文件的发送。例如数字编码文件是HTML文件。例如在互联网平台上提供数字编码文件，比如作为网页或者帖子。帖子在此是指在互联网平台比如像社交媒体平台、网络论坛或博客上的单独稿件。另外，该数字编码文件可以被提供用于下载。例如，网页或帖子包括调用数字编码文件的链接。

[0161] 针对比如呈HTTP-GET要求形式的相应请求，数字编码文件被发送至请求的计算机系统。

[0162] 根据可选实施方式，数字编码文件的发送与发送请求无关地进行。例如，该文件以

电邮、即时通信、声音消息、视频消息、图形消息、SMS或者MMS形式被发出，或者被前述的消息类型涵盖。即时通信表示如下通信方法，在此，两个及以上的用户通过数字编码的文本、语言、图形和/或视频消息相互通信。在此，发送者触发消息的传输，即采用所谓的推送法，从而消息尽量直接到达预定接收者。用户此时利用计算机程序通过网络比如像互联网直接地或通过服务器相互通信。

附图说明

[0163] 此外，参照附图来详述本发明的实施方式，其中：

[0164] 图1示出示例性区块链结构的实施方式的示意性框图，

[0165] 图2示出用于创建双向区块链结构的示例性方法的示意性流程图，

[0166] 图3示出用于创建双向区块链结构的示例性方法的示意性流程图，

[0167] 图4示出用于创建组合区块相关校验值的示例性方法的示意性框图，

[0168] 图5示出用于创建组合区块相关校验值的示例性方法的示意性流程图，

[0169] 图6示出用于创建缩短双向区块链结构的示例性方法的示意性流程图，

[0170] 图7示出示例性数据存储系统的实施方式的示意性框图，

[0171] 图8示出示例性电信系统的实施方式的示意性框图。

[0172] 以下实施方式的彼此对应的单元带有相同的附图标记。

具体实施方式

[0173] 图1示出示例性区块链结构100的实施方式，其包括N个区块102、104、106、108、110。区块链结构100应该被扩展一个附加区块112。区块链结构100的区块102、104、106、108、110通过区块相关链接函数被双向相互链接。各个双向连接或链接V_1、V_{M-2}、V_{M-1}由双箭头示意表示。区块链结构100的内区块104、106、108分别包括组合的区块相关链接函数，其是两个区块相关链接函数的关联之结果。两个关联的区块相关链接函数中的第一个例如包括校验值，该校验值取决于相应的内区块的数据以及紧接在前的区块的数据。两个关联的链接函数中的第二个包括例如校验值，该校验值取决于相应内区块的数据和紧接在后的区块的数据。相应的区块相关链接函数、即第一和第二链接函数的关联被集成到各自区块中。

[0174] 用于区块链结构100的最后区块110与附加区块112链接的、即用于产生双向连接V_M的链接函数的校验值不仅包含存储在最后区块110中的数据，也包含待存储在附加区块112中的数据。因此，只要两个区块的数据保持不变，在链接过程中存储在最后区块110和附加区块112中的链接函数只表示两个相应区块的正确的校验值。在例如篡改附加区块112的情况下，最后区块110的校验值和进而在最后区块110与附加区块112之间的连接的相应链接函数不再匹配于附加区块112的数据。依据所述偏差，可以识别出相应的篡改。此外，用于产生双向连接V_M的链接函数包括区块无关链接过程独立函数，其例如取决于M。

[0175] 图2示出用于以区块112扩展图1的区块链100的方法的示意性框图。区块链结构100的区块106、108、110分别包括区块相关链接函数，其由函数曲线示意性示出。区块链结构100中的区块比如像倒数第二区块108和倒数第三区块106分别具有区块相关双向链接函数，其包含与在先区块例如区块108情况下的区块106以及与后续区块例如在区块108情况下的区块110的双向连接的区块相关双向链接函数的关联。相应的区块相关链接函数作为

数学函数被集成到相应区块106、108中。各自的区块相关链接函数分别在采用两个待相互链接的区块的数据情况下生成。另外，包含区块无关链接过程独立函数的相应的链接函数总是与链接过程相关。为此，表示多个链接函数的关联的组合链接函数取决于多个链接或双向连接。

[0176] 为了区块链结构100的最后区块110与附加区块112的双向链接，例如提供泛函112。从该泛函112推导出一个具体的区块无关链接过程独立函数。该函数与两个要相互链接的区块即区块110和区块112的数据的校验值关联。相应的关联例如可以是算术关联比如像加、减、乘和/或除。因此可以从共用的综合函数120中推导出区块相关双向链接函数122，其明确对应于区块110和区块112之间的双向连接，并且还不仅取决于区块110的数据、也取决于区块112的数据。区块相关双向链接函数122为了区块110与区块112的双向链接而不仅被添加至区块110，也被添加至区块112。此时，链接函数122与在区块108和区块110之间双向链接的已经存在于区块110内的链接函数关联。

[0177] 图3示出用于为双向链接区块链结构扩展一个附加区块的示例性方法的一个实施方式。在步骤400中提供双向链接区块链结构。在步骤402中提供待存储数据。在区块404中生成用于扩展区块链结构的一个附加区块。附加区块包括所述待存储数据并且设置用于与区块链结构的最后区块双向链接。在步骤406中，用于区块链结构的最后区块与附加区块双向链接的区块相关链接函数被计算。为此，一方面，计算组合的区块相关校验值，其不仅包含区块链结构的最后区块的数据，也包含待添加的附加区块的数据。尤其是该校验值可包含用于区块链结构的最后区块与区块链结构的倒数第二区块的双向链接的链接函数。此外，提供区块无关链接过程独立函数。区块无关链接过程独立函数例如可以从泛函推导出。在此选择如下函数，它被明确划归入在区块链结构的最后区块与附加区块之间的链接过程或对应于双向连接。相应的配属例如可以通过链接过程独立函数的相应的序数实现。链接过程独立函数与该校验值关联。相应关联例如能以算术关联的形式进行。例如链接过程独立函数能乘以校验值。在步骤408中，在步骤406中算出的链接函数被添加至区块链结构的最后区块。在步骤410中，链接过程独立函数被添加至附加区块。根据实施方式，步骤408包含在步骤406中算出的链接函数与在区块链结构的最后区块和倒数第二区块之间的双向连接的已存在于最后区块中的链接函数的关联。该相应的关联例如可以是算术关联。例如所述两个链接函数可以相加。

[0178] 图4示出了两个要相互链接的区块110、112的校验值的计算的示意性框图，比如它大致被图3的步骤406涵盖。两个要相互链接的区块110、112的数据例如分别被存储在方形(TxT)矩阵结构160、170中。T例如是自然数T≥2。如果两个区块110、112的矩阵结构160、170具有不同的大小，则一个或两个矩阵结构160、170被如此扩展，得到两个同样大小的方形矩阵结构。为此，例如添加附加的矩阵单元或附加的行和/或列。添加的矩阵单元分别包含一个通配符例如0值。如果例如区块110的矩阵结构少了一列，即例如缺少第T列，则它被补充，在这里，第T列的所有单元$D1_{1T}$至$D1_{TT}$分别被设为0。为了计算组合的区块相关校验值PW，例如对于区块110的矩阵结构160的每列162，相应列162的所有单元的和被计算。对于第i列，此时得到和$\sum_{Si}=\sum_{j=1}^{T} d1_{ji}$。另外，对于区块112的矩阵结构170的每一行172，分别计算相应行172的所有单元的和。对于第i行，此时得到了和$\sum_{Zi}=\sum_{j=1}^{T} d2_{ij}$。在下一步骤中，分别将针

对区块110的矩阵结构160的第i列所计算的和ΣSi加至区块112的矩阵结构170的第i行的和Σ_{Zi}。合成的T和Σ_{11}至Σ_{TT}作为数字被连接在一起，从而得到数序，其形成组合的区块相关校验值：$PW=\Sigma_{11}\Sigma_{22}\cdots\Sigma_{T-1T-1}\Sigma_{TT}$。根据可选实施方式，为了计算组合校验值也可以形成矩阵结构160的行的和与矩阵结构170的列的和。

[0179] 图5示出了根据图4的用于计算组合的区块相关校验值的示例性方法。在步骤500中，对于第一区块的矩阵结构的每列计算相应列的所有单元的和。在步骤502中，对于应该与第一区块双向链接的第二区块的矩阵结构的每行，计算相应行的所有单元的和。在步骤504中，第一区块的矩阵的每列对应配属于第二区块的矩阵的一行。例如，第i列对应于第i行。对于由第一区块的矩阵结构的相应第i列和第二区块的矩阵结构的第i行所造成的每一对，计算一个组合和。在步骤506中，在步骤504中算出的和以数序来排列成行，从而它们形成组合的区块相关校验值。

[0180] 图6示出了示例性的双向链接区块链结构100，其应该被缩短，从而出现缩短的区块链结构150。为此，在区块140和144之间的内链段142被取出。取出的内链段142例如可以是包含安全关键数据。例如，内链段142包含区块链结构100的许多前后相继的区块。在链段142取出之后，区块140、144形成相邻区块。该相邻区块140、144通过其链接函数相互连接。但所述连接是借助包含所述链接函数的区块无关链接过程独立函数的连接。因此，双向连接由虚线的双箭头所示。链接过程独立函数对应于根据预定的配属对照图的单独双向连接或链接，例如根据升序。基于整齐有序的配属，区块链结构还依据链接过程独立函数及其相互关系可被检查一致性，其由同一泛函推导得出。在图6的情况下，例如区块140的链接过程独立函数可以通过三次使用升算子被变换为区块144的链接过程独立函数，或者区块144的链接过程独立函数可以通过三次使用降算子被变换为区块140的链接过程独立函数。

[0181] 根据实施方式，还可以进行区块相关链接函数以在区块140和区块144之间产生双向链接，其不仅取决于区块140的数据、也取决于区块144的数据和段142的所有区块。为此，内链段142的区块的链接函数相互关联，从而生成组合的双向链接函数。组合的双向链接函数取决于内链段142的所有区块的数据以及与内链段142相邻的区块140、144的数据。例如，各个双向链接函数通过例如包含加、减、乘和/或除的算术关联相互关联。在从区块链结构100中取出内链段142之后出现的缩短的区块链结构150的两个区块140和144在采用组合的双向链接函数情况下相互链接。由此，在取出内链段142后形成区块链结构150的松解端的两个区块140和144不仅与链接过程独立函数相关地双向相互连接，也与其数据相关地双向相互连接。为此，例如如此扩展区块140、144的链接函数，即它们完全包含组合的双向链接函数。为此出现了缩短的双向链接区块链结构150，其中的所有区块不仅就其关联顺序而言、也就其数据而言双向相互链接。所出现的区块链结构150此时尤其与之前一样取决于所取出的内链段142。如果所取出的内链段142被提供用于补充缩短的区块链结构150，则可以通过使用区块140、144的扩展的双向链接函数来检查所提供的内链段是否是真实的。如果所提供的内链段是真实的，即与所取出的链段142相同，则缩短的区块链结构可以被补足成为最初完整的区块链结构100。因此，例如可以补充包含安全关键数据的区块，其原先被取出以保护安全关键数据。

[0182] 图7示出了呈计算机系统形式的用于在采用双向链接的区块链结构100情况下在电子存储器206中防篡改存储数据210的示例性数据存储系统200的实施方式的示意性框

图。计算机系统200包括处理器202，其配置用于执行程序指令204。通过程序指令204的执行，处理器202控制计算机系统200，从而它执行用于防篡改存储数据的方法的前述实施方式之一。

[0183] 计算机系统200还包括存储器206，在存储器中存储有用于计算双向链接函数的、即用于计算或推导区块相关组合校验值和区块无关的链接过程独立函数的函数208以及双向链接区块链结构100。存储器206还包含数据210，其在采用双向链接区块链结构100情况下应该被防篡改保护或防篡改存储。例如计算机系统200执行根据图2和图3的方法之一并且生成用于区块链结构100的附加区块，附加区块包含待防篡改存储的数据210并且与区块链结构100的最后区块双向关联。为了附加区块的双向关联，例如采用包含数据210以及来自区块链结构100的数据的函数208来计算组合校验值并与链接过程独立函数关联。

[0184] 最后，计算机系统200包括通信接口214。通信接口214例如可以是用于经由网络通信的网络接口，或者是用于与可更换式数据载体通信的接口。通过通信接口214，例如可以提供数据210和/或区块链结构100。另外，通信接口214可以是用于由用户输入指令和/或输出结果的用户接口。

[0185] 根据实施方式，程序指令204例如可以包含数据库管理系统，其管理存储在存储器206中的区块链结构比如像区块链结构100。

[0186] 图8示出图7的示例性数据存储系统200，其配置成电信系统，它借助通信接口214可经由网络240与其它计算机系统比如像计算机系统220、250通信。例如，数据210由计算机系统250通过网络240来提供。

[0187] 计算机系统250例如包括用于存储数据210的存储器256，该数据应通过计算机系统200被防篡改保护。根据实施方式，数据210是如下数据，其标示数字编码文件。例如数据210是数字编码文件内容的哈希值。根据其它实施方式，数据210是计算机系统250所促成、记录和/或执行的交易的交易数据。根据其它实施方式，数据210是传感器数据，其借助计算机系统250的传感器266来获得。计算机系统250还包括处理器252，该处理器被配置用于执行程序指令254。根据实施方式，计算机系统250也作为电信系统来配置，其借助通信接口264经由网络240可与计算机系统200通信。处理器252执行程序指令254促使计算机系统250例如发送数据210至计算机系统200。数据210经由网络240的转送此时例如可以响应于询问地由计算机系统200促成进行或响应于自身主动由计算机系统250促成进行。

[0188] 图8还示出计算机系统220，其例如也作为电信系统来配置并且可借助通信接口264经由网络240与计算机系统200通信。计算机系统220例如包括含程序指令224的处理器222。处理器222配置用于执行程序指令224，其中在由处理器222执行程序指令224中促使计算机系统220经由网络从计算机系统200问询被扩展了数据210的区块链结构100。响应于问询，计算机系统220例如接收区块链结构100。根据实施方式，计算机系统220可以读取存储在区块链结构100中的数据。计算机系统220例如可以在采用存储在存储器226中的函数208的情况下检查读取数据的完整性。利用函数208，区块链结构100的将区块链结构100的区块双向相互链接的区块相关双向链接函数被复核并且被检查一致性或完整性。读取数据例如是用于证明数字编码文件真实性的数据。相应文件例如自计算机系统250经由网络240被提供给计算机系统220。如果读取数据例如是文件内容的哈希值，则可以依据该数据检验所提供的文件的真实性。例如针对该文件通过计算机系统220计算哈希值。如果计算的哈希值与

读取数据一致，则所提供的文件被认定真实。

[0189] 由计算机系统220接收的区块链结构100尤其也可以被用于以离线模式的检查，即当网络240暂时不可用时。因此，借助区块链结构100被检查其真实性的数据能够例如通过计算机系统220被直接接收或读入而无需网络240。该数据于是可以采用区块链结构100被检查其真实性。

[0190] 附图标记列表

[0191] 100 区块链结构

[0192] 102 第一区块

[0193] 104 第二区块

[0194] 106 倒数第三区块

[0195] 108 倒数第二区块

[0196] 110 最后区块

[0197] 112 附加区块

[0198] 120 共用的综合函数

[0199] 122 双向链接函数

[0200] 130 扩展区块链结构

[0201] 140 区块

[0202] 142 内链段

[0203] 144 区块

[0204] 150 缩短的区块链结构

[0205] 160 矩阵结构

[0206] 162 列

[0207] 170 矩阵结构

[0208] 172 行

[0209] 200 计算机系统

[0210] 202 处理器

[0211] 204 程序指令

[0212] 206 存储器

[0213] 208 函数

[0214] 210 数据

[0215] 214 通信接口

[0216] 220 计算机系统

[0217] 222 处理器

[0218] 224 程序指令

[0219] 226 存储器

[0220] 234 通信接口

[0221] 240 网络

[0222] 250 计算机系统

[0223] 252 处理器

[0224] 254 程序指令

[0225] 256 存储器

[0226] 264 通信接口

[0227] 266 传感器

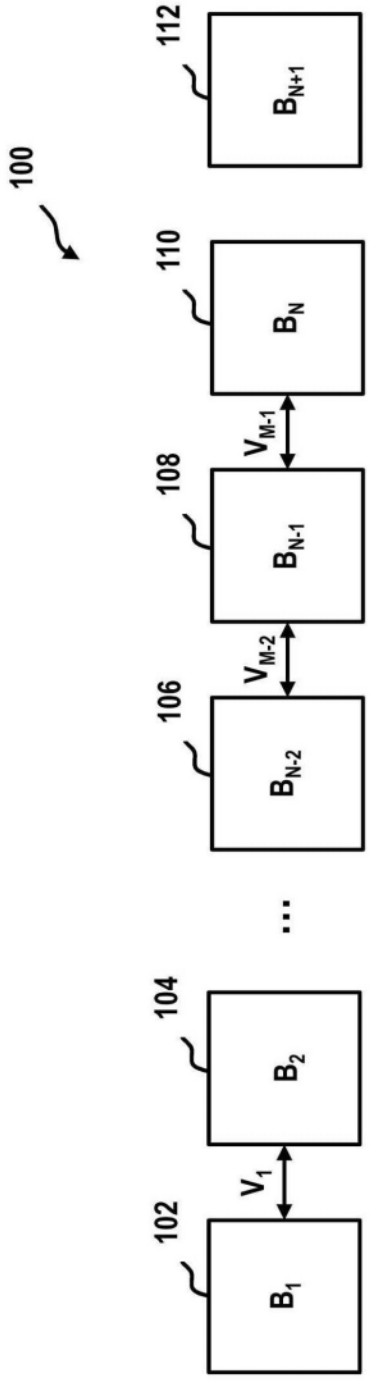


图1

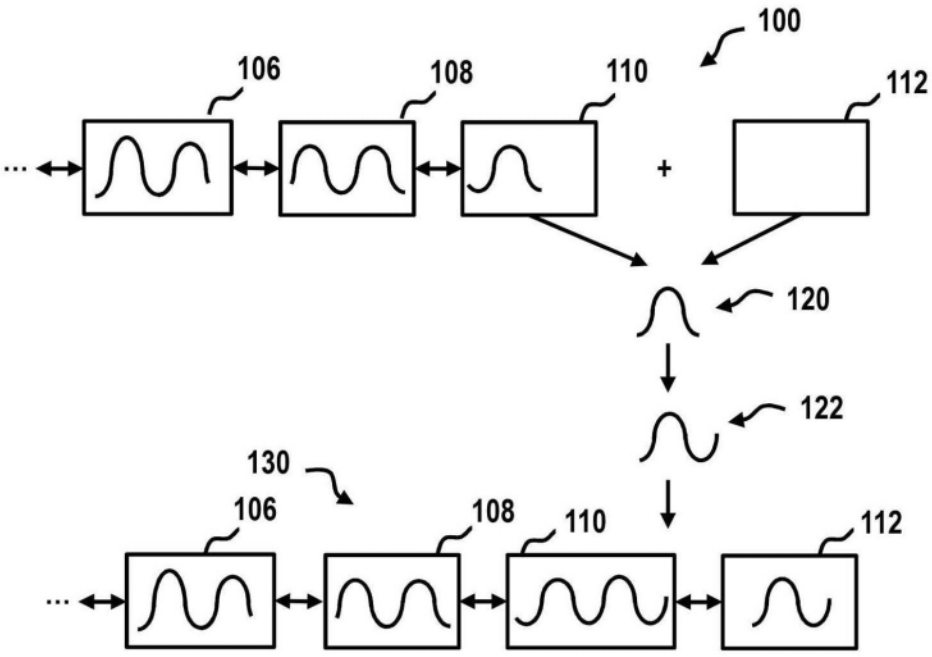

100
106
108
110
112
120
122
130
106
108
110
112

图2

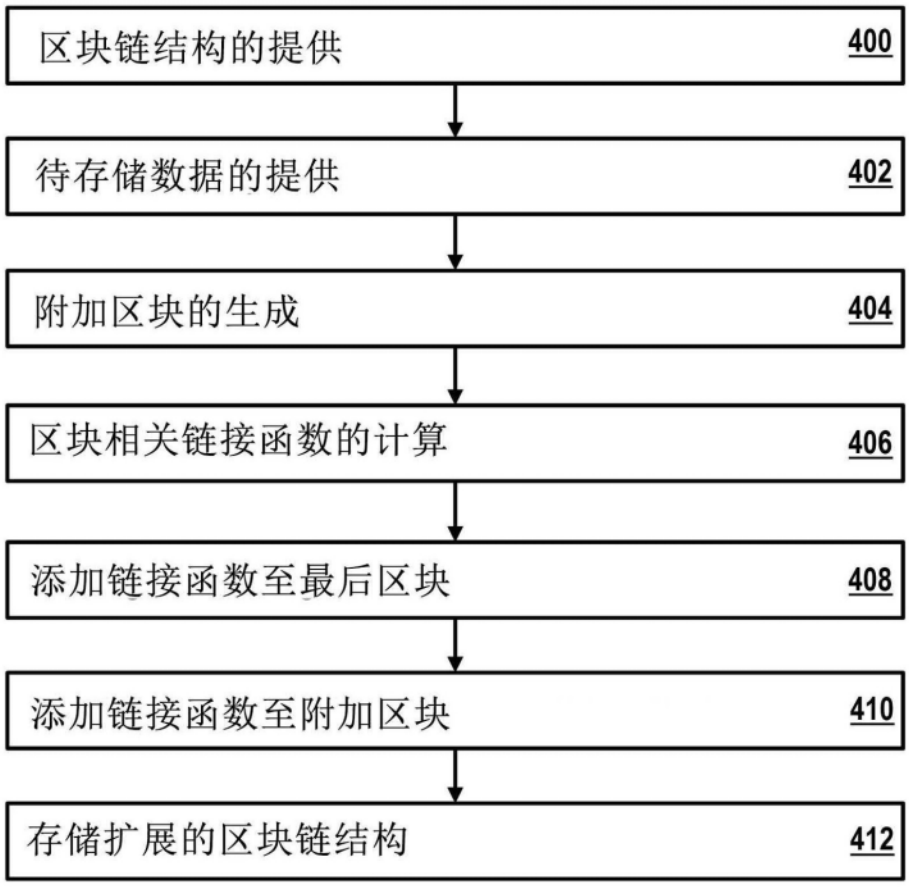

区块链结构的提供
400
待存储数据的提供
402
附加区块的生成
404
区块相关链接函数的计算
406
添加链接函数至最后区块
408
添加链接函数至附加区块
410
存储扩展的区块链结构
412

图3

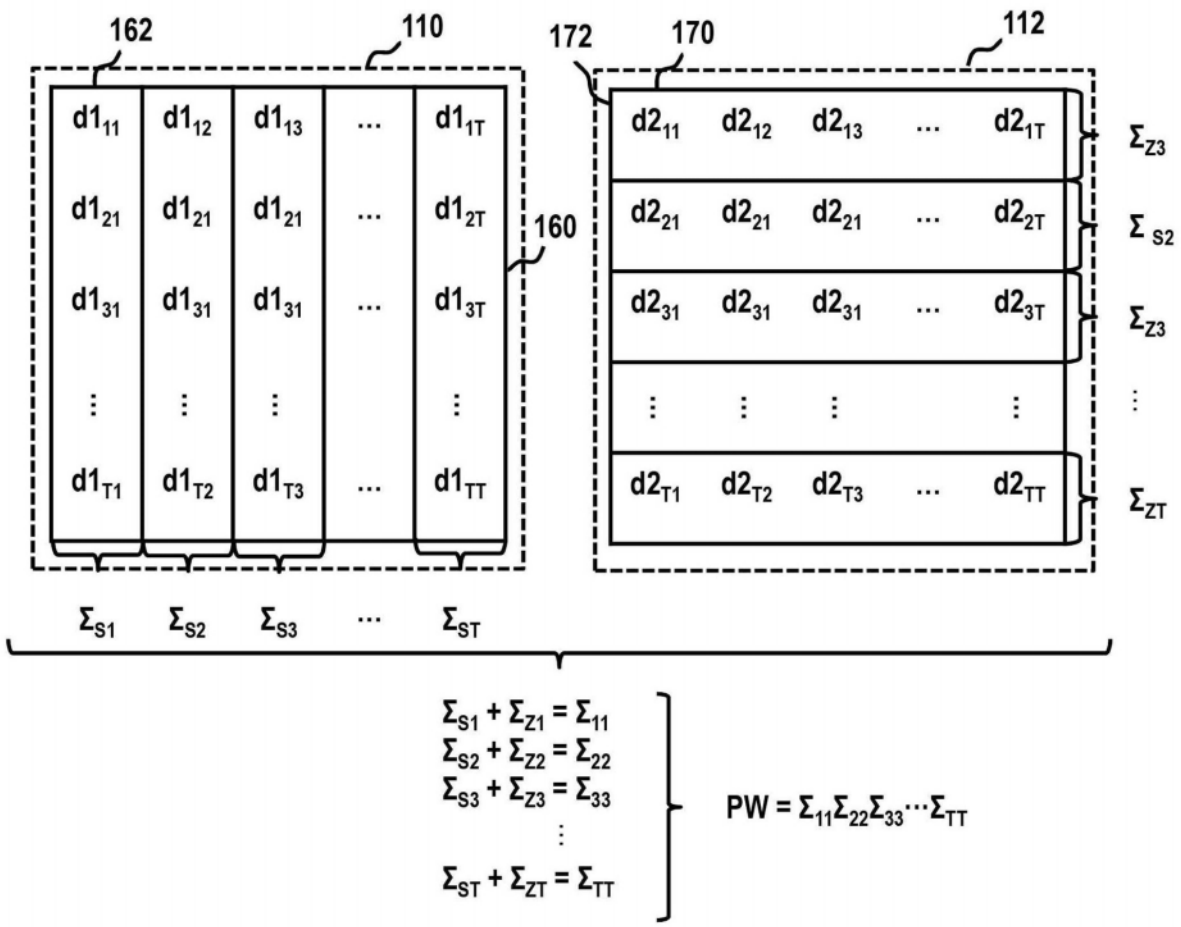

162
110
172
170
112
160
$d1_{11}$ $d1_{12}$ $d1_{13}$ ... $d1_{1T}$
$d1_{21}$ $d1_{21}$ $d1_{21}$ ... $d1_{2T}$
$d1_{31}$ $d1_{31}$ $d1_{31}$ ... $d1_{3T}$
$d1_{T1}$ $d1_{T2}$ $d1_{T3}$ ... $d1_{TT}$
$d2_{11}$ $d2_{12}$ $d2_{13}$ ... $d2_{1T}$
$d2_{21}$ $d2_{21}$ $d2_{21}$ ... $d2_{2T}$
$d2_{31}$ $d2_{31}$ $d2_{31}$ ... $d2_{3T}$
$d2_{T1}$ $d2_{T2}$ $d2_{T3}$ ... $d2_{TT}$
Σ_{Z3}
Σ_{S2}
Σ_{Z3}
Σ_{ZT}
Σ_{S1} Σ_{S2} Σ_{S3} ... Σ_{ST}
$\Sigma_{S1} + \Sigma_{Z1} = \Sigma_{11}$
$\Sigma_{S2} + \Sigma_{Z2} = \Sigma_{22}$
$\Sigma_{S3} + \Sigma_{Z3} = \Sigma_{33}$
$\Sigma_{ST} + \Sigma_{ZT} = \Sigma_{TT}$
$PW = \Sigma_{11}\Sigma_{22}\Sigma_{33}\cdots\Sigma_{TT}$

图4

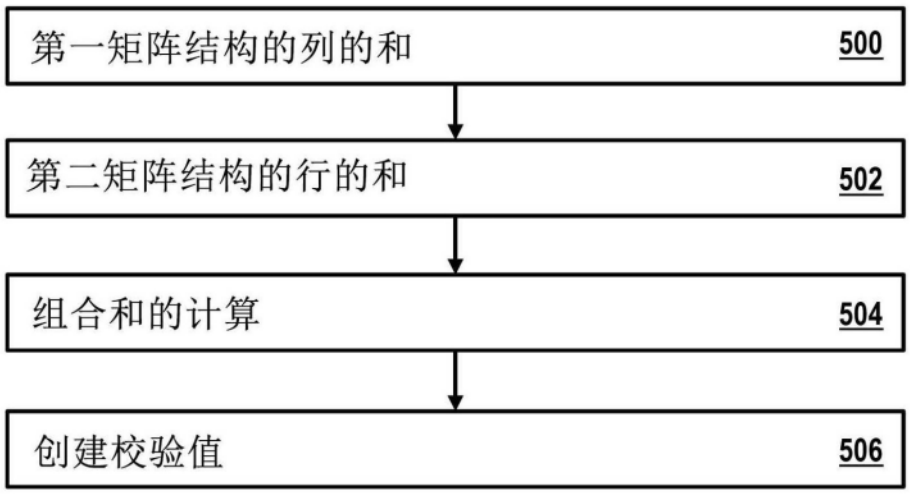

第一矩阵结构的列的和 500
第二矩阵结构的行的和 502
组合和的计算 504
创建校验值 506

图5

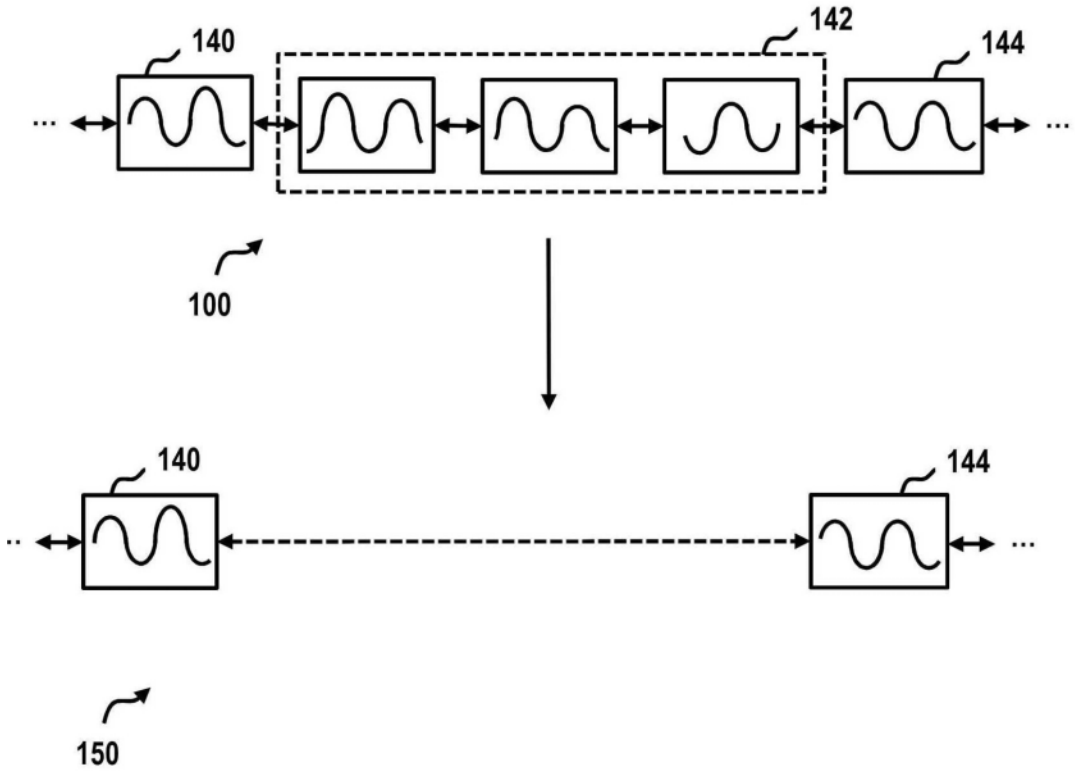

140
142
144
100
140
144
150

图6

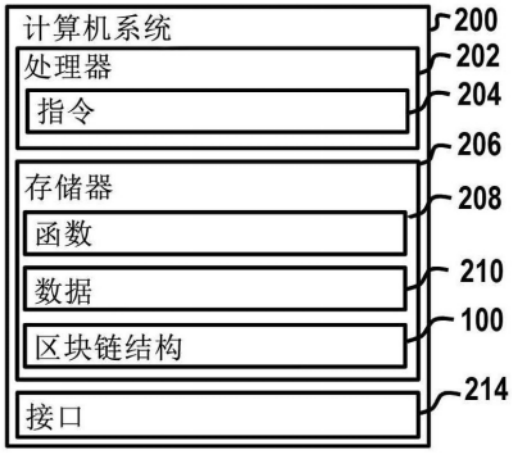

计算机系统
200
处理器
202
指令
204
206
存储器
208
函数
数据
210
区块链结构
100
接口
214

图7

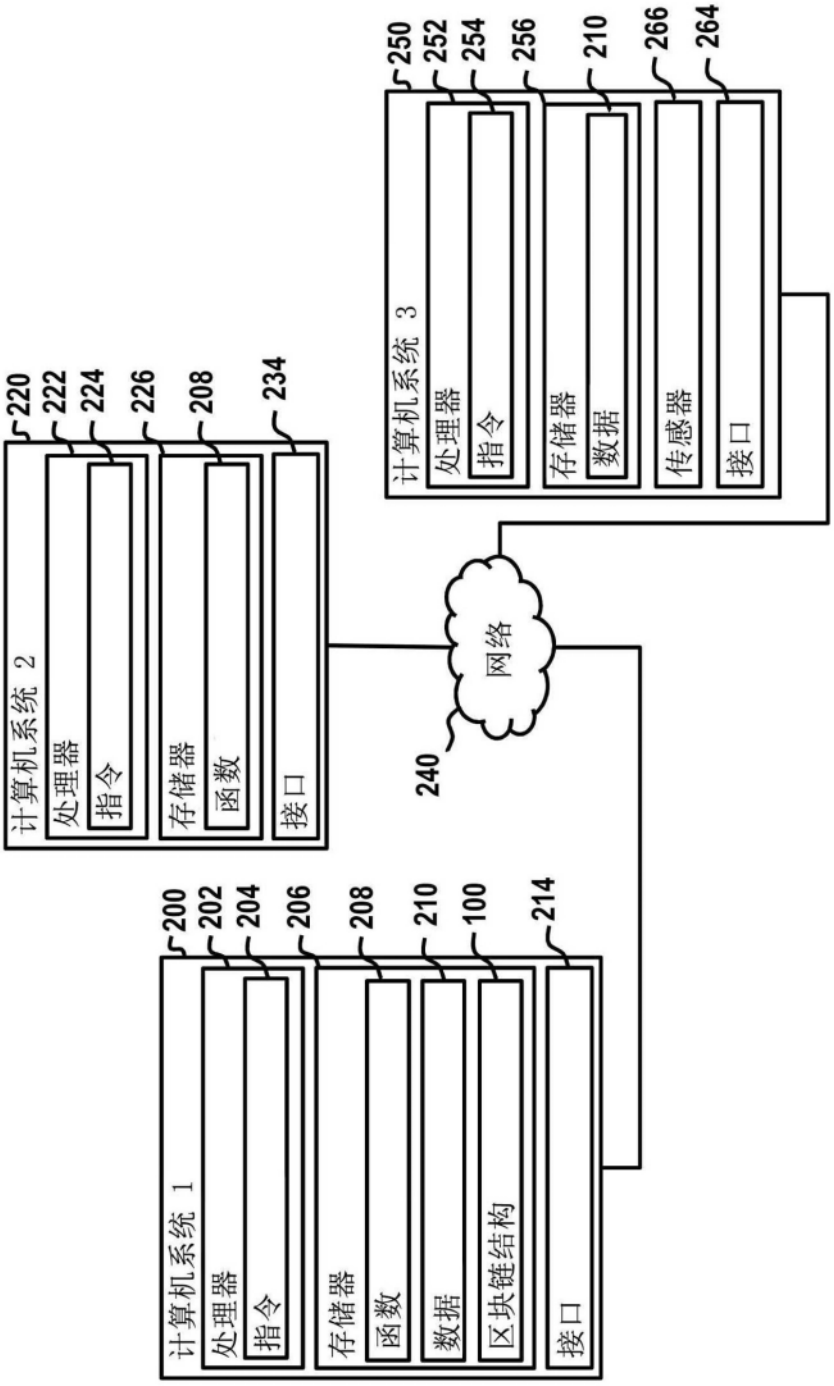

计算机系统 1
处理器
指令
存储器
函数
数据
区块链结构
接口
200
202
204
206
208
210
100
214
计算机系统 2
处理器
指令
存储器
函数
接口
220
222
224
226
208
234
计算机系统 3
处理器
指令
存储器
数据
传感器
接口
250
252
254
256
210
266
264
网络
240

图8