



(12)发明专利申请

(10)申请公布号 CN 110431558 A

(43)申请公布日 2019.11.08

(21)申请号 201780088974.1

(22)申请日 2017.12.18

(30)优先权数据

17153037.1 2017.01.25 EP

(85)PCT国际申请进入国家阶段日

2019.09.25

(86)PCT国际申请的申请数据

PCT/EP2017/083390 2017.12.18

(87)PCT国际申请的公布数据

W02018/137856 DE 2018.08.02

(71)申请人 西门子公司

地址 德国慕尼黑

(72)发明人 R.法尔克

(74)专利代理机构 中国专利代理(香港)有限公司 72001

代理人 臧永杰 刘春元

(51)Int.Cl.

G06F 21/64(2006.01)

H04L 9/06(2006.01)

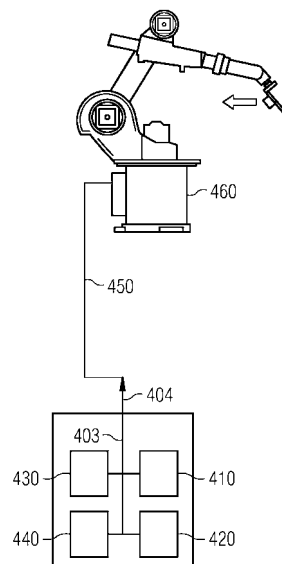
权利要求书3页 说明书14页 附图5页

(54)发明名称

以计算机支持的方式创建和执行控制功能的方法和装置

(57)摘要

本发明实现一种用于以计算机支持的方式创建和执行控制功能的方法。所述控制功能在此可以尤其是针对特定的技术系统、例如自动化系统来实现并且尤其是通过区块链以密码学方式受保护。因此,根据本发明的方法尤其是针对特定的技术系统、例如自动化系统而言适合。



1. 一种用于以计算机支持的方式创建自动化系统的控制功能的方法,所述方法具有以下方法步骤:

- 提供 (110) 所述控制功能的第一控制动作;
- 将所述第一控制动作存储 (120) 在第一交易数据组中;
- 通过产生区块链的第一链节来创建 (130) 所述第一控制功能,其中
- 所述第一链节包括第一交易数据组;
- 借助第一检验和来保护区块链的第一链节的和/或第一链节的之前链节的完整性。

2. 根据权利要求1所述的方法,其中附加地将控制动作交易存储在所述第一交易数据组中。

3. 根据权利要求2所述的方法,其中通过所述控制动作交易来预给定用于所述控制功能和/或所述第一控制动作的安全关键的保护功能。

4. 根据权利要求2或3所述的方法,其中通过所述控制动作交易来预给定用于所述区块链的所述第一交易数据组的路径。

5. 根据权利要求2至4之一所述的方法,其中

- 通过所述控制动作交易来预给定所述第一链节的第一数目的之前链节和/或所述第一链节的第二数目的之后链节,并且
- 通过所述控制动作交易来预给定:所述第一数目的之前链节和/或所述第二数目的之后链节的完整性被确认。

6. 根据上述权利要求之一所述的方法,其中附加地将用于状态断言交易的第一传感器值和/或其他传感器值存储在所述第一交易数据组中。

7. 根据上述权利要求之一所述的方法,其中通过所述控制动作交易来预给定第三数目的区块链节点,所述第三数目的区块链节点成功地执行和/或确认自身的所属的控制动作交易和/或状态断言交易。

8. 用于以计算机支持的方式执行控制功能的方法,其中所述方法具有以下方法步骤:

- 提供 (210) 区块链的第一链节,其中所述第一链节包括第一交易数据组和第一检验和;
- 借助所述第一检验和来检验 (220) 所述区块链的所述第一链节和/或所述第一链节的之前链节的完整性,其中如果成功地确定出所述完整性,则附加地执行以下方法步骤:
 - 从所述第一交易数据组加载 (230) 所述控制功能的第一控制动作;
 - 通过执行所述第一控制动作来执行 (240) 所述控制功能,其中所述执行通过自动化系统来实施。

9. 根据权利要求8所述的方法,其中:

- 通过所述第一交易数据组附加地提供控制动作交易;
- 所述控制动作交易被成功地执行和/或确认,以便允许执行所述控制功能。

10. 根据权利要求9所述的方法,其中通过所述控制动作交易来预给定用于所述控制功能和/或所述第一控制动作的安全关键的保护功能。

11. 根据权利要求9或10所述的方法,其中通过所述控制动作交易来预给定用于所述区块链的所述第一交易数据组的路径。

12. 根据权利要求9至11之一所述的方法,其中

- 通过所述控制动作交易来预给定所述第一链节的第一数目的之前链节和/或所述第一链节的第二数目的之后链节,并且

- 通过所述控制动作交易来预给定:所述第一数目的之前链节和/或所述第二数目的之后链节的完整性被确认。

13. 根据权利要求9至12之一所述的方法,其中

- 附加地通过所述第一交易数据组来提供用于状态断言交易的第一传感器值和/或其他传感器值,

- 所述状态断言交易被确认和/或成功地执行,以便允许执行所述控制功能。

14. 根据权利要求9至13之一所述的方法,其中通过所述控制动作交易来预给定第三数目的区块链节点,所述第三数目的区块链节点成功地执行和/或确认自身的所属的控制动作交易和/或状态断言交易。

15. 根据上述权利要求之一所述的方法,其中如果:

- 所述第一链节的完整性没有被确认;和/或

- 所述控制动作交易没有被确认和/或实施;

- 所述状态断言交易没有被确认和/或实施,

则提供控制信号。

16. 用于以计算机支持的方式创建自动化系统的控制功能的创建装置,所述创建装置具有:

- 第一提供模块(310),用于提供所述控制功能的第一控制动作;

- 第一存储器模块(320),用于在第一交易数据组中存储所述第一控制动作;

- 第一创建模块(330),用于通过产生区块链的第一链节来创建所述第一控制功能,

- 其中所述第一链节包括所述第一交易数据组,

- 所述区块链的所述第一链节和/或所述第一链节的之前链节的完整性借助第一检验和来被保护。

17. 用于自动化系统的控制设备,所述控制设备具有:

- 第一接收模块(410),用于接收区块链的第一链节,其中所述第一链节包括第一交易数据组和第一检验和;

- 第一检验模块(420),用于借助所述第一检验和来检验所述区块链的所述第一链节和/或所述第一链节的之前链节的完整性;

- 第一加载模块(430),用于在成功地确定出完整性的情况下从所述第一交易数据组加载所述控制功能的第一控制动作;

- 第一执行模块(440),尤其是处理器,用于在成功地确定出完整性的情况下通过执行所述第一控制动作来执行所述控制功能。

18. 具有用于执行根据权利要求1至7之一所述和/或根据权利要求8至15之一所述的方法的程序指令的计算机程序产品。

19. 具有用于创建设备的程序指令的计算机程序产品,所述计算机程序产品借助所述程序指令来配置用于,创建根据权利要求16所述的创建装置和/或根据权利要求17所述的控制设备。

20. 用于根据权利要求18或19所述的计算机程序产品的提供装置,其中所述提供装置

存储和/或提供所述计算机程序产品。

以计算机支持的方式创建和执行控制功能的方法和装置

技术领域

[0001] 本发明涉及用于以计算机支持的方式创建和执行控制功能的方法和装置。

背景技术

[0002] 区块链(英语Blockchain)或“Distributed Ledger(分布式账本)”的技术当前是广泛讨论的技术。除了分布式支付系统(例如比特币)的应用以外,在金融业中开发了新的应用可能性。尤其是可以在没有中介者或结算机构的情况下由此以防操纵的方式来实现企业之间的交易。这实现:在没有值得信任的中介者的情况下的新的商业模式,其减小交易成本,并且可以灵活地提供新的数字服务,而无需设立为此专门设立的基础设施和信任关系。通过区块链所保护的交易数据组(或者简称交易)通常包括程序代码,该程序代码也可称为所谓的“智能合约”。

发明内容

[0003] 本发明的任务是:提供一种方法和装置,以用于以安全保护的方式创建和执行控制功能。

[0004] 该任务通过在独立权利要求中所说明的特征而得以解决。在从属权利要求中示出本发明的有利扩展方案。

[0005] 按照第一方面,本发明涉及一种用于以计算机支持的方式创建控制功能的方法,该方法具有以下方法步骤:

- 提供控制功能的第一控制动作;
- 将第一控制动作存储在第一交易数据组中;
- 通过产生区块链的第一链节来创建第一控制功能,其中
- 第一链节包括第一交易数据组;
- 借助第一检验和来保护区块链的第一链节的和/或第一链节的之前链节的完整性。

[0006] 只要是在接下来的描述中没有另外说明,术语“实施”、“计算”、“以计算机支持的方式”、“计算”、“确定出”、“生成”、“配置”、“重建”等就优选地涉及改变和/或产生数据和/或将数据转化成其他数据的行动和/或过程和/或处理步骤,其中所述数据尤其是可以作为物理参量来表示或者存在,例如作为电脉冲。尤其是,表述“计算机”应尽可能宽泛地理解,以便尤其是涵盖具有数据处理属性的电子设备。计算机因此可以例如是个人计算机、服务器、有存储器可编程的控制器(SPS)、手持计算机系统、掌上PC设备、移动无线电设备和其他能够以计算机支持的方式处理数据的通信设备,处理器和用于数据处理的其他电子设备。

[0007] “以计算机支持的方式”可以在本发明的上下文中例如理解为如下方法的实施,其中尤其是处理器实施该方法的至少一个方法步骤。

[0008] 处理器可以在本发明的上下文中理解为例如机器或电子电路。处理器可以尤其是主处理器(英文:Central Processing Unit, CPU(中央处理单元))、微处理器或微控制器,例如专用集成电路或电子信号处理器等,其可能与用于存储程序指令的存储器单元相结

合。处理器可以例如也是IC(集成电路,英文:Integrated Circuit)、尤其是FPGA(英文:Field Programmable Gate Array(现场可编程门阵列))或者ASIC(专用集成电路,英文:Application-Specific Integrated Circuit)或者DSP(数字信号处理器,英文:Digital Signal Processor)或者图形处理器GPU(Graphic Processing Unit(图形处理单元))。处理器也可以理解为虚拟化处理器、虚拟机或软CPU。也可例如涉及可编程处理器,其装备有用于执行所提及的按照本发明的方法的配置步骤或者利用配置步骤来这样配置,使得可编程处理器实现所述方法的、组件的、模块的或本发明其他方面的和/或本发明部分方面的按照本发明的特征。

[0009] “存储器单元”或“存储器模块”等等可以在本发明的上下文中理解为例如以工作存储器(英语:Random-Access Memory, RAM(随机存取存储器))形式的易失性存储器或永久性存储器,例如硬盘或数据载体。

[0010] “模块”可以在本发明的上下文中例如理解为处理器和/或用于存储程序指令的存储单元。例如,处理器专门被设立用于,如此执行程序指令,以便处理器执行功能,用于实施或实现按照本发明的方法或按照本发明的方法的步骤。

[0011] “检验和”在本发明的上下文中例如理解为密码检验和或密码散列或散列值,其尤其已经借助密码散列函数通过数据组/交易来构成或计算。检验和可以尤其是散列树的(多个)散列值或(多个)检验和。此外,其可以尤其也理解为数字签名或密码消息认证码。

[0012] “第一检验和”在本发明的上下文中可以理解为如下检验和,所述检验和尤其是已通过区块链的第一链节的之前链节/前任链节的和/或第一链节的(例如第一交易数据组的)交易或第一链节来构成。附加地或可替代地,第一检验和可以尤其也通过所述之前链节/前任链节的交易(例如前任链节的第一交易数据组)构成。第一检验和可以在此尤其是也借助散列树、例如Merkle树来实现,其中第一检验和尤其是Merkle树的根检验和。尤其是,交易数据组和/或交易借助来自Merkle树的其他检验和来确保,其中所述其他检验和尤其是Merkle树中的叶。第一检验和可以因此例如确保所述交易,其方式为由所述其他检验和来构成根检验和。第一检验和可以尤其是可以也到达第一链节之后的链节中,以便将所述之后链节例如与自身的之前链节(例如第一链节)链接并且尤其是因此使得区块链的完整性是可检验的。

[0013] “提供”在本发明的上下文中可以例如理解为在存储器模块上或者由存储器模块来加载或存储例如第一交易数据组和/或控制动作交易和/或状态断言交易。

[0014] “工作量证明证据”可以在本发明的上下文中例如理解为计算密集的任务的解决,所述任务尤其是与第一交易数据组的内容/链节内容相关地待解决。这种计算密集的任务例如也被称为加密难题。

[0015] “链节”在本发明的上下文中可以例如理解为区块链的区块,所述区块链尤其是作为数据结构来实现。

[0016] “区块链的第一链节的之前链节”在本发明的上下文中可以例如仅理解为区块链的如下链节,该链节尤其是直接在该第一链节前面。可替代地,“区块链的第一链节的之前链节”在本发明的上下文中尤其也可以例如理解为该区块链的如下所有链节,这些链节在第一链节之前。由此,第一检验和可以例如尤其是仅通过直接在第一链节前方的链节或通过所有在第一链节之前的链节来构成。

[0017] “交易数据组”可以在本发明的上下文中例如理解为区块链(英文Blockchain)的链节的交易的数据或者区块链的如下链节的多个交易。交易数据组可以例如包括如下交易,所述交易例如包括如下程序代码,该程序代码尤其是实现智能合约。“交易数据组”可以在本发明的上下文中例如也理解为区块链的链节的交易(例如控制功能或第一控制动作)和/或控制动作交易和/或状态断言交易和/或由所提及的交易组成的组合。

[0018] “控制功能”可以在本发明的上下文中例如理解为尤其是用于自动化系统的一个或多个控制动作。

[0019] “控制动作”可以在本发明的上下文中例如理解为控制指令、程序指令、程序代码或者控制指示,其尤其是用于自动化系统。借助控制动作可以例如控制生产机器人的执行器或能量分布网的电流耦合器的执行器。

[0020] “程序代码”可以在本发明的上下文中例如理解为控制指令、程序指令或者控制指示,其尤其是存储在交易中。

[0021] “智能合约”可以在本发明的上下文中例如理解为可执行的程序代码。

[0022] “控制动作交易”(英文:Control Action Transaction, CAT)或“状态断言交易”(英文:State Assertion Transaction, SAT)可以在本发明的上下文中例如理解为区块链的链节的交易。这种交易可以例如包括如下程序代码,所述程序代码尤其是实现智能合约。控制动作交易可以例如限定能够计算的要求,所述要求尤其是可借助工作量证明证据来实现。尤其是,在控制动作交易已成功地被执行或确认的情况下,才可以例如执行该控制动作和/或控制功能。状态断言交易可以例如包括以第一传感器值的形式能够测量的物理值,其尤其是能够借助传感器来检测。传感器值可以例如是传感器原始数据或者经预处理的传感器原始数据。尤其是,还在执行控制动作和/或控制功能之前再次检测相同物理参量的相应的第二传感器值。控制动作和/或控制功能尤其是只有在第二传感器值与第一传感器值一致的情况下才被执行。为了确定出一致性,可以尤其是预给定如下阈值,第二传感器值尤其是应达到所述阈值。在此情况下,尤其是也能够接受直至预给定的大小/容差范围的偏差/误差。

[0023] “区块链的路径”在本发明的上下文中例如可以理解为区块链中的链节相对于该区块链的其他链节的位置。例如,区块链可以包含分支(例如期望的或不期望的分支),从而尤其是除了之前链节和之后链节以外也存在区块链的分路径中的并行链节,该分路径尤其是已通过分支而产生。

[0024] “区块链节点”、“节点”、“区块链的节点”等可以在本发明的上下文中例如理解为如下设备(例如现场设备)、计算机或参与者,其利用区块链来实施操作(Operation)。这种节点可以例如执行区块链或其链节的交易或者以新交易来将新的链节引入到该区块链中。

[0025] 该方法如下地是有利的,因为尤其是使得能够基于区块链来检验交易、例如控制动作或控制功能。因此,可以例如实现(特定)技术系统的经确保的基于云的或者经确保的分布式的控制或监控功能。尤其是,能够实现可信赖的、以防操纵的方式的控制功能,其优选地并不取决于特定的硬件或网络架构。由此可以尤其是实现在没有中央控制计算机情况下的分布式的控制系统。其例如也通过区块链(英文:Blockchain)的隐含的密码机制相对于有意的操纵来受保护。由此,尤其是保证控制功能性的高完整性保护。尤其是可以实现以防操纵的方式的安全性保护功能(英文:safety protection function),其中尤其是进行

冗余的计算和检验(例如工作量证明证据)。尤其是也能够设想,例如使用在没有工作量证明证据情况下的经接入监察的区块链实现方案。在此尤其是也进行如下检验,所述检验例如根据发生在过去的交易的智能合约来验证交易的可靠性。

[0026] 在该方法的第一实施方式中,附加地在第一交易数据组中存储控制动作交易。

[0027] 该方法例如如下地是有利的,以便尤其是通过控制动作交易来实现尤其是自动化设施的以防操纵方式的记录(例如黑盒子记录器、司法记录器(Juridical Recorder))。由此可以尤其是放弃附加的监控硬件。

[0028] 尤其是,通过控制动作交易来引入附加的安全性机制,因为例如只有在控制动作交易已经被确认和/或成功执行的情况下才执行控制功能和/或控制动作。

[0029] 在该方法的另一实施方式中,通过控制动作交易来预给定用于控制功能和/或第一控制动作的安全关键的保护功能。在此,安全关键的保护功能例如理解为关于功能上的安全性(Safety)的功能。这尤其是如下地是有利的:例如能够可信赖地并且以防操纵的方式借助区块链来实现安全关键的保护功能。由此,可以尤其是放弃特别针对功能上的安全性所设计的硬件计算机实现方案、诸如多信道计算机或其可以至少更少耗费地被设计。因此尤其是可能:例如通过多信道或冗余的(例如三个计算机架构其中的两个)计算节点/节点来实现区块链功能性。在此可以尤其是在一种变型方案中例如仅使用多信道计算机。在另一变型方案中,例如不仅使用多信道的计算机而且也使用简单的单信道计算机,其共同地实现区块链。

[0030] 该方法例如如下地是有利的,以便限定安全性要求,所述安全性要求尤其是在执行控制功能和/或控制动作之前必须被确认和/或成功地执行。这可以例如由此来实现,其方式为,控制动作交易要求或预给定确定的工作量证明证据。

[0031] 在该方法的另一实施方式中,通过控制动作交易来预给定用于区块链的第一交易数据组的路径。

[0032] 该方法例如如下地是有利的,以便实现:使区块链满足确定的要求。因此可以例如要求:区块链由预给定数目的链节组成,对于该区块链并不存在分支或者仅允许区块链的确定数目的分支。由此,可以尤其是阻止:在通过区块链中的不允许的分支而对区块链可能的操纵情况下执行控制功能和/或控制动作。也可以例如要求:区块链是没有分支的并且因此尤其是不存在分路径。

[0033] 在该方法的另一实施方式中,通过控制动作交易来预给定第一链节的第一数目的之前链节和/或第一链节的第二数目的之后链节,其中通过控制动作交易来预给定:第一数目的之前链节和/或第二数目的之后链节的完整性被确认。

[0034] 该方法例如如下地是有利的,以便实现高安全性,其方式为,在允许执行控制动作和/或控制功能之前,尤其是多个链节的完整性必须被确认。

[0035] 在该方法的另一实施方式中,附加地将用于状态断言交易的第一传感器值和/或其他传感器值存储在第一交易数据组中。

[0036] 该方法例如如下地是有利的,以便实现高安全性,其方式为,尤其是考虑能够测量的物理参量。物理参量可以例如是特定技术系统的(例如自动化系统的)测量值,诸如电气路线的电压水平、运行温度、压力、力等等。尤其是在允许执行控制功能和/或控制动作之前,所述参量必须例如重新地或者独立地测量(例如作为第二传感器值或者第二传感器的

传感器值)并且在与第一传感器值的比较中必须与其优选地一致,其中尤其是测量精确度和/或直至预给定容差值的偏差被接受。这种控制逻辑可以尤其是在此作为区块链的智能合约或者区块链的交易的智能合约来实现。

[0037] 在该方法的另一实施方式中,通过控制动作交易来预给定第三数目的区块链节点,这些区块链节点成功地执行和/或确认自身的所属的控制动作交易和/或状态断言交易。

[0038] 该方法例如如下地是有利的,以便实现高安全性,其方式为,在允许执行控制功能和/或控制动作之前,尤其是多个链节的完整性必须被确认。

[0039] 按照本发明的另一方面,本发明涉及一种用于以计算机支持的方式执行控制功能的方法,该方法具有以下方法步骤:

- 提供区块链的第一链节,其中该第一链节包括第一交易数据组和第一检验和;
- 借助第一检验和来检验区块链的第一链节和/或第一链节的之前链节的完整性,其中如果成功确定出该完整性,则附加地执行以下方法步骤:
 - 从第一交易数据组加载控制功能的第一控制动作;
 - 通过执行第一控制动作来执行控制功能,其中所述执行尤其是通过自动化系统来实施。

[0040] 该方法如下地是有利的,因为尤其是使得能够基于区块链来检验交易、例如控制动作或控制功能。因此,可以例如实现技术系统的经确保的、基于云的或者经确保的分布式的控制或监控功能。尤其是,能够实现可信赖的、以防操纵的方式的控制功能,其优选地并不取决于特定的硬件或网络架构。由此可以尤其是实现在没有中央控制计算机情况下的分布式的控制系统。其例如也通过区块链的隐含的密码机制相对于有意的操纵来受保护。由此,尤其是保证控制功能性的高完整性保护。尤其是可以实现以防操纵的方式的安全性保护功能(英文:safety protection function),其中尤其是进行冗余的计算和检验。

[0041] 在该方法的另一实施方式中,通过第一交易数据组附加地提供控制动作交易,其中该控制动作交易被成功地执行和/或确认,以便允许执行控制功能。

[0042] 在该方法的另一实施方式中,通过控制动作交易来预给定用于控制功能的和/或第一控制动作的安全关键的保护功能。

[0043] 在该方法的另一实施方式中,通过控制动作交易来预给定用于区块链的第一交易数据组的路径。

[0044] 在该方法的另一实施方式中,通过控制动作交易来预给定第一链节的第一数目的之前链节和/或第一链节的第二数目的之后链节,其中通过控制动作交易来预给定:第一数目的之前链节和/或第二数目的之后链节的完整性被确认。

[0045] 在该方法的另一实施方式中,通过第一交易数据组来附加地提供用于状态断言交易的其他传感器值和/或第一传感器值,其中所述状态断言交易被确认和/或成功地执行,以便允许执行控制功能。

[0046] 在该方法的另一实施方式中,通过控制动作交易来预给定第三数目的区块链节点,这些区块链节点成功执行和/或确认其所属的控制动作交易和/或状态断言交易。

[0047] 在该方法的另一实施方式中,如果:

- 第一链节的完整性没有被确认;和/或

- 控制动作交易没有被确认和/或实施；
 - 状态断言交易没有被确认和/或实施，
- 则提供控制信号。

[0048] 该方法例如如下地是有利的，以便借助控制信号来发送差错报告(Fehlermeldung)给管理员。借助该控制信号可以例如也使特定技术系统(例如自动化系统)处于安全状态，以便尤其是防止进一步的操纵。

[0049] 按照另一方面，本发明涉及一种用于以计算机支持的方式来创建控制功能的创建装置，该创建装置具有：

- 第一提供模块，用于提供控制功能的第一控制动作；
- 第一存储器模块，用于在第一交易数据组中存储第一控制动作；
- 第一创建模块，用于通过产生区块链的第一链节来创建第一控制功能，其中
- 该第一链节包括第一交易数据组，
- 区块链的第一链节和/或第一链节的之前链节的完整性借助第一检验和来被保护。

[0050] 在该创建装置的另一实施方式中，该创建装置包括至少一个其他模块或多个其他模块，用于实施按照本发明的方法(或其实施方式)，以用于以计算机支持的方式创建控制功能。

[0051] 按照另一方面，本发明涉及一种控制设备，所述控制设备用于以计算机支持的方式来创建控制功能，所述控制设备具有：

- 第一接收模块，用于接收区块链的第一链节，其中该第一链节包括第一交易数据组和第一检验和；
- 第一检验模块，用于借助第一检验和来检验区块链的第一链节和/或第一链节的之前链节的完整性；
- 第一加载模块，用于在成功地确定出完整性的情况下从第一交易数据组加载控制功能的第一控制动作；
- 第一执行模块，尤其是处理器，用于在成功地确定出完整性的情况下通过执行第一控制动作来执行控制功能。

[0052] 在该控制设备的另一实施方式中，该控制设备包括至少一个其他模块或多个其他模块，用于实施按照本发明的方法(或其实施方式)以用于以计算机支持的方式来执行控制功能。

[0053] 此外，要求保护一种具有用于实施所提到的按照本发明的方法的程序指令的计算机程序产品，其中借助计算机程序产品能够实施按照本发明的方法其中各一个、所有按照本发明的方法或者按照本发明的方法的组合。

[0054] 附加地，要求保护具有用于配置创建设备、例如3D打印机、计算机系统或对于创建处理器和/或设备而言适合的制造机器的程序指令的计算机程序产品的变型方案，其中所述创建设备以所述程序指令这样配置，使得所提到的按照本发明的创建装置和/或控制设备被创建。

[0055] 此外，要求保护一种提供装置，其用于存储和/或提供计算机程序产品。提供装置例如是数据载体，该数据载体存储和/或提供计算机程序产品。可替代地和/或附加地，所述提供装置例如是网络服务、计算机系统、服务器系统、尤其是分布式的计算机系统、基于云

的计算机系统和/或虚拟计算机系统,其优选地以数据流的形式存储和/或提供计算机程序产品。

[0056] 这种提供例如作为以程序数据块和/或指令数据块的形式下载、优选作为文件、尤其是作为下载文件或作为完整计算机程序产品的数据流、尤其是作为下载数据流来进行。但是这种提供可以例如也作为部分下载来进行,其由多个部分组成并且尤其是通过点对点网络来下载或者作为数据流被提供。这种计算机程序产品例如在使用以数据载体形式的提供装置的情况下被读入到系统中并且执行程序指令,从而使按照本发明的方法在计算机上执行或者这样配置创建设备,使得其创建按照本发明的创建装置和/或控制设备。

附图说明

[0057] 本发明的上述特性、特征和优点以及如何实现其的方式和方法将结合以下实施例的描述而变得更加清楚和明显,其中所述实施例与附图相结合地进一步被阐述。在此,在示意图中:

图1 作为按照本发明的用于以计算机支持的方式来创建控制功能的方法的流程图来示出本发明的第一实施例;

图2 作为按照本发明的用于以计算机支持的方式来执行控制功能的方法的流程图来示出本发明的第二实施例;

图3 示出作为创建装置的本发明的第三实施例;

图4 示出作为控制设备的本发明的第四实施例;

图5 示出作为系统的本发明的第五实施例;

图6 示出作为区块链的本发明的第六实施例;

图7示出具有状态断言交易的本发明的第七实施例;

图8 示出作为控制动作交易的本发明的第八实施例;

图9 示出作为对状态断言交易和控制动作交易的组合的本发明的第九实施例。

[0058] 在附图中,只要是没有另外说明,相同功能的元件就配备有相同的附图标记。

具体实施方式

[0059] 只要是没有另外说明或者已经说明,接下来的实施例就具有至少一个处理器和/或存储器单元,以便实施或执行该方法。

[0060] 尤其是对于(相关的)本领域技术人员而言在了解所述一个/多个方法权利要求的情况下所有在现有技术中常见的用于实现产品的可能性或者用于实施的可能性当然是已知的,从而尤其是不需要在说明书中的单独公开。尤其是,这种常规的并且对于本领域技术人员而言已知的实现变型方案仅仅通过硬件(组件)或仅仅通过软件(组件)来实现。可替代地和/或附加地,本领域技术人员可以在其专业能力的范畴内尽量地选择由硬件(组件)和软件(组件)组成的任意的按照本发明的组合,以便实施按照本发明的实现变型方案。

[0061] 尤其是在按照本发明的作用的一部分优选地仅仅通过专用硬件(例如以ASIC或FPGA的形式的处理器)而引起和/或另一部分通过(以处理器和/或存储器支持的)软件而引起,由硬件(组件)和软件(组件)组成的按照本发明的组合于是可以出现。

[0062] 尤其是,鉴于大数目的不同实现可能性而不可能并且对于本发明的理解也并非目

的明显或必要的是：列举所有这些实现可能性。就此而论，尤其是所有接下来的实施例应该仅示例性地示出一些方式：按照本发明的教导的这样的实现方案尤其是看起来如何。

[0063] 因此，各个实施例的特征尤其是并不限于相应的实施例，而是一般而言尤其涉及本发明。相应地，优选地，一个实施例的特征可以也作用于另一实施例的特征，尤其是无需在相应的实施例中详尽提及这点。

[0064] 图1作为按照本发明的用于以计算机支持的方式来创建控制功能的方法的流程图来示出本发明的第一实施例。

[0065] 该方法优选地以计算机支持的方式来实现。

[0066] 详细地，在这种实施例中实现用于以计算机支持的方式来创建控制功能的方法。该方法可以例如被用于创建用于特定的技术系统、诸如自动化系统的控制功能。

[0067] 该方法包括第一方法步骤110，用于提供控制功能的第一控制动作。所述控制功能可以例如相对于该控制动作而言附加地包括其他控制动作。控制动作可以例如控制自动化系统的机器人的执行器的运动。控制动作例如指示执行器来以围绕预给定的轴线的预给定的角度旋转或者以预给定的距离沿着预给定的方向来实施运动。

[0068] 该方法包括第二方法步骤120，用于将第一控制动作存储在所述第一交易数据组中。由此，可以尤其是将控制功能和/或第一控制动作保存到第一交易数据组中。

[0069] 该方法包括第三方法步骤130，用于通过产生区块链的第一链节来创建第一控制功能，其中该第一链节包括第一交易数据组（尤其是包括控制功能和/或第一控制动作在内），并且区块链的第一链节（包括第一交易数据组在内）和/或第一链节的之前链节的完整性借助第一检验和来保护。第一检验和可以例如被附加到第一链节上和/或作为之前区块的检验和在所述第一链节之后的链节中被插入。

[0070] 第一链节因此例如被插入到区块链中。可替代地或附加地，第二检验和通过第一链节的和/或直接在第一链节之前的链节的和/或在第一链节之前的链节（例如所有的或者所选的链节）的第一交易数据组（例如交易动作）来形成。可替代地或附加地，第三检验和通过每个交易或第一交易数据组的每个交易来构成。这些第二检验和和/或第三检验和可以例如是散列树、例如Merkle树的检验和和/或叶。从散列树的、例如用于Merkle树而已知的这些检验和和/或叶计算根检验和，其中根检验和能够用作第一检验和。

[0071] 以这种方式，可以诸如从比特币已知、尤其是替代相应链节的交易/第一交易数据组而仅将相应的检验和（例如第一检验和和/或第二检验和和/或第三检验和）保存到区块链的链节中。由此，尤其是实现节省存储。

[0072] 交易自身和/或第一交易数据组可以在此分别附加地借助第四检验和来保护。这种第四检验和可以例如被实现为数字签名，其中交易的创建者尤其是拥有优选地仅对于他而言已知的用于创建数字签名的私钥和提供用于检验数字签名的匹配的公钥。公钥的提供可以例如在相同的交易中进行，所述交易已经通过创建者来签名或者以另一方式使得该公钥可访问，以便对数字签名或者通过该数字签名所保护的交易鉴于其真实性来检验。这可以例如通过区块链的新的链节的第一交易数据组/单独的交易来进行，其包括该公钥。

[0073] 图2作为按照本发明的用于以计算机支持的方式来执行控制功能的方法的流程图来示出本发明的第二实施例。

[0074] 该方法优选地以计算机支持的方式来实现。

[0075] 详细地,在该实施例中实现用于以计算机支持的方式执行控制功能的方法。该方法可以例如被用于执行用于特定技术系统的、诸如自动化系统的控制功能。

[0076] 该方法包括第一方法步骤210,用于提供区块链的第一链节,其中该第一链节包括第一交易数据组合和第一检验和。所述提供可以例如由此来进行:使区块链的第一链节通过网络连接被传输到自动化系统并且通过控制设备来处理。

[0077] 该方法包括第二方法步骤220,用于借助第一检验和来检验区块链的第一链节的和/或第一链节的之前链节的完整性。为此,控制设备可以例如通过第一链节的第一交易数据组来构成第五检验和。如果第一检验和与第五检验和一致,则因此可以确认第一交易数据组的完整性。这可以以相同的方式也对于之前的链节来执行,以便检验第一交易数据组的完整性。

[0078] 如果在该方法的中间步骤225中对于第一交易数据组成功地确定出完整性,则附加地执行以下方法步骤:

该方法包括第三方法步骤230,用于在已成功地确定出完整性的情况下从第一交易数据组加载控制功能的第一控制动作。该控制设备对此例如读出第一交易数据组并且将第一控制动作加载到其工作存储器中。

[0079] 该方法包括第四方法步骤240(在已经成功地确定出完整性的情况下)用于通过第一控制动作的执行来执行控制功能,其中该执行尤其是通过自动化系统来实施。该控制设备例如为此而与第一控制动作相应地操控自动化系统的执行器。

[0080] 如果在中间步骤225中并没有成功地确定出对于第一交易数据组的完整性,则可以例如在第五方法步骤中250中提供控制信号,以便例如将控制设备引入安全状态。

[0081] 尤其是,可以将任意信息作为(例如第一交易数据组的)交易/交易数据结构来编码。这种交易可以尤其是被存放在区块链(英文:Blockchain)中。例如通过交易所存放的信息并不能事后地被操纵,并且其可以优选地通过第三方(例如节点)来评估和检验。在此,尤其是不需要中央基础设施。这种区块链因此优选地表示分散式的、以防操纵方式的数据库。

[0082] 换言之,在图1和图2中实现按照本发明的用于创建和执行控制功能的方法。控制功能可以在此尤其是针对特定技术系统、例如自动化系统来实现并且尤其是通过区块链来以密码学的方式受保护。尤其是,因此使按照本发明的方法对于特定技术系统、例如自动化系统而言是适合的。

[0083] 在此,控制动作尤其是与当前在区块链中经确认的链节和所包含的交易相应地被实施。这尤其具有优点:使用区块链的保护,以便实现安全关键的关键控制功能的可信赖性。尤其是,安全关键的保护功能通过区块链交易的智能合约来限定。这种交易可以尤其是也被称为控制动作交易,因为其操控例如执行器的动作。

[0084] 在一种变型方案中,在交易处于经确认的路径中(也即还不存在区块链的分路径)的情况下,控制动作交易才能够被实施。

[0085] 在另一变型方案中,如果存在在包括所述控制动作交易的链节之后的、区块链的能够预给定的数目的经确认的链节,则通过该控制动作交易所限定的动作才被执行。

[0086] 在另一变型方案中,在控制动作交易多次地被确认的情况下,该控制动作交易才于是作为有效的而适用。在此情况下,在交易作为有效而被接受并且由执行器来执行之前,必须优选地通过不同区块链节点来检验该交易。换言之,链节必须尤其是(例如利用不同的

难题解或工作量证明证据)通过多个节点来确认,以便将其认可为有效的。

[0087] 控制设备与区块链的最新的经确认的链节的控制动作交易相应地执行控制功能。

[0088] 在另一变型方案中,节点监控:实际上在区块链中存在最新的经确认的链节。否则,尤其是(例如通过控制信号)激活故障安全模式(Fail-Safe-Mode)。也即,尤其是监控:该区块链系统是否还是活跃的(liveliness monitoring(存在性监控))。

[0089] 在另一变型方案中,物理系统、例如特定技术系统、例如自动化系统的状态可以通过传感器或现场设备以所连接的传感器来确认。通过这些传感器所检测传感器值在状态断言交易中优选地通过值得信任的来源和/或节点被插入到区块链中。在此,尤其是进一步可能的是,由物理的、实际的传感器的原始数据所推导出的经检验的数据(例如借助智能合约)被确定。因此,可以例如确定状态值,该状态值根据多个冗余的传感器的测量值来确定,这些传感器分别将状态断言交易设置到区块链中。具体地,这可以例如由此来实现:将具有交易数据组或状态断言交易的链节插入到区块链中。可以例如于是借助智能合约来进行检验,该智能合约同样地已经被插入到区块链中或者作为交易被插入到区块链的链节中。这可以例如由此来进行:构成经推导出的、经检验的值(例如三个中的两个的多数决)。可以因此尤其是在区块链之内进行以防操纵方式的传感器数据处理(数据融合(Data Fusion))。

[0090] 尤其是可以因此实现以下控制功能。

[0091] 例如,可以利用按照本发明的方法在信号所和/或火车安全系统中来实现以下应用情境:交易尤其显示出铁路自动化系统的当前状态(例如道岔位置、行驶信号、计轴器、轨道空闲报告、障碍报告)。尤其是通过区块链或被存放在交易/交易数据组中的智能合约来确保:仅容许的交易通过区块链来被确认。只有在智能合约被履行的情况下,状态转换、例如道岔位置的改变或者行驶信号的信号示象的改变才作为控制动作交易通过区块链被确认。在此,尤其也可以检验:所述交易通过火车安全系统的多个节点、例如验证节点来被确认为容许的。

[0092] 在另一变型方案中,信号所自身作为区块链来实现。

[0093] 在另一变型方案中,仅仅监控信号所的运行。为此,控制通信可以例如通过单向网关从控制网络无反馈地被输出耦合。替代于仅记录数据以便使其在意外事故事件中可供使用的例如常规的黑盒子记录器或司法记录器,其可以在区块链中立刻鉴于可靠性被检验。由此可以针对于信号所/火车安全系统实现独立的监控系统。

[0094] 例如,可以利用按照本发明的方法也实现自动化系统的保护电路。与上述(信号所和/或火车安全系统)相似地可以在例如借助光幕来对机器人的保护监控情况下,如果并不最新地通过控制动作交易确认存在运行安全的状态,则将机器人转换到故障安全模式。

[0095] 例如,可以利用按照本发明的方法来实现诊断功能、例如差错报告,作为交易。也可以尤其是取决于交易地探测需要的维护工作(predictive maintenance(预见性维护))并且可以必要时自动地产生维护票据(Wartungs-Ticket)。

[0096] 在另一变型方案中,从项目数据(组件、自动化逻辑)出发,针对控制功能/第一控制动作来生成用于区块链的相应智能合约,其实现控制逻辑。

[0097] 图3示出作为用于以计算机支持的方式创建用于自动化系统的控制功能的创建装置的本发明的第三实施例。

[0098] 该装置包括通过第一总线303相互通信连接的第一提供模块310、第一存储器模块

320、第一创建模块330和可选的第一通信接口304。

[0099] 该装置可以例如附加地还包括一个其他组件或多个其他组件,诸如处理器、存储器单元、输入设备,尤其是计算机键盘或计算机鼠标,和显示设备(例如监视器)。处理器可以例如包括多个其他处理器,其中例如所述其他处理器分别实现模块其中一个或多个。可替代地,处理器尤其是实现实施例的所有模块。所述一个或多个其他组件可以例如同样地通过第一总线303相互通信连接。

[0100] 处理器可以例如是ASIC,其已经应用特定地针对该实施例的(和/或其他实施例的)所有模块的或相应模块的功能来实现,其中程序组件或程序指令尤其是作为集成电路来实现。处理器可以例如也是FPGA,其尤其是借助程序指令这样来配置,使得FPGA实现该实施例(和/或其他实施例)的所有模块或相应模块的功能。

[0101] 第一提供模块310设立用于提供控制功能的第一控制动作。

[0102] 第一提供模块310可以例如借助处理器、存储器单元和第一程序组件来被实施或实现,其中例如通过执行第一程序组件的程序指令这样配置处理器,或者通过程序指令这样配置处理器,使得提供控制功能的第一控制动作。

[0103] 该第一存储器模块320被设立用于在第一交易数据组中存储第一控制动作。

[0104] 第一存储器模块320可以例如借助处理器、存储器单元和第二程序组件来实施或实现,其中例如通过执行第二程序组件的程序指令来这样配置处理器或者通过程序指令来这样配置处理器,使得存储第一控制动作。

[0105] 第一创建模块330用于通过产生区块链的第一链节来创建第一控制功能,其中第一链节包括第一交易数据组并且区块链的第一链节的和/或第一链节的之前链节的完整性借助第一检验和来保护。

[0106] 该第一创建模块330可以例如借助处理器、存储器单元和第三程序组件来实施或实现,其中例如通过执行第三程序组件的程序指令来这样配置处理器或者通过程序指令来这样配置处理器,使得创建控制功能。

[0107] 相应的模块的程序指令的执行可以在此情况下例如借助处理器自身和/或借助初始化组件、例如加载器(英文:Loader)或配置组件来进行。

[0108] 图4 示出作为用于以计算机支持的方式来执行用于自动化系统的控制功能的控制设备的本发明的第三实施例。

[0109] 该装置包括通过第二总线403相互通信连接的第一接收模块410、第一检验模块420、第一加载模块430、第一执行模块440和可选的第二通信接口404。通过第二通信接口,工业机器人460通过第三总线450来与控制设备连接。

[0110] 该装置可以例如附加地还包括一个其他组件或多个其他组件,诸如处理器、存储器单元、输入设备,尤其是计算机键盘或计算机鼠标,和显示设备(例如监视器)。处理器可以例如包括多个其他处理器,其中例如所述其他处理器分别实现模块其中一个或多个。可替代地,处理器尤其是实现该实施例的所有模块。一个/多个其他组件可以例如同样地通过第一总线403相互通信连接。

[0111] 处理器可以例如是ASIC,其已经应用特定地针对该实施例的(和/或其他实施例的)所有模块的或相应模块的功能来实现,其中程序组件或程序指令尤其是作为集成电路来实现。处理器可以例如也是FPGA,其尤其是借助程序指令这样来配置,使得FPGA实现该实

施例(和/或其他实施例)的所有模块或相应模块的功能。

[0112] 该第一接收模块410被设立用于接收区块链的第一链节,其中该第一链节包括第一交易数据组和第一检验和。

[0113] 第一接收模块410可以例如借助处理器、存储器单元、第二通信接口404和第一程序组件来实施或实现,其中例如通过执行第一程序组件的程序指令这样配置处理器或者通过程序指令这样配置处理器,使得由控制设备可接收第一链节。如例如在图3中示出的,该第一链节可以例如由创建设备传送给控制设备。

[0114] 第一检验模块420被设立用于,借助第一检验和来检验区块链的第一链节的和/或第一链节的之前链节的完整性。

[0115] 该第一检验模块420可以例如借助处理器、存储器单元和第二程序组件来实施或实现,其中例如通过执行第二程序组件的程序指令这样配置处理器或者通过程序指令这样配置处理器,使得完整性被检验。

[0116] 第一加载模块430被设立用于,在已经通过第一检验模块420成功地确定出完整性的情况下从第一交易数据组加载控制功能的第一控制动作。

[0117] 该第一加载模块430可以例如借助处理器、存储器单元和第三程序组件来实施或实现,其中例如通过执行第三程序组件的程序指令这样配置处理器或者通过程序指令这样配置处理器,使得在已经通过第一检验模块420成功地确定出完整性的情况下加载第一控制动作。

[0118] 第一执行模块440被设立用于,在已经通过第一检验模块420成功地确定出完整性的情况下通过执行第一控制动作来执行控制功能。

[0119] 第一执行模块440可以例如借助处理器、存储器单元和第四程序组件来实施或实现,其中例如通过执行第四程序组件的程序指令这样配置处理器或者通过程序指令这样配置处理器,使得在已经通过第一检验模块420成功地确定出完整性的情况下执行第一控制动作。

[0120] 相应模块的程序指令的执行可以在此情况下例如借助处理器自身和/或借助初始化组件、例如加载器(英文:Loader)或配置组件来进行。

[0121] 图5示出作为系统的本发明的第五实施例。

[0122] 详细地,图5示出如下系统,其具有多个设备,例如第一现场设备D1、第二现场设备D2、第三现场设备D3、第四现场设备D4和第五现场设备D5、网关GW和多个节点或区块链节点BCC、例如比特币节点或以太坊节点。在一种(未示出)变型方案中,可以将其中各个或所有的区块链节点BCC作为故障安全的计算机、例如作为多信道计算机、诸如锁步双架构(Lockstep dual processor architecture(锁步双处理器架构))、三模块冗余架构(triple modular redundant(三模块冗余), TMR)来设计。第三现场设备D3、第四现场设备D4和第五现场设备D5通过自动化网络510相互链接并且通过该网关来与互联网520连接。该第一现场设备D1和第二现场设备D2、以及区块链节点BCC同样地与互联网520连接并且彼此处于通信连接以及通过网关GW来与现场设备D3-D5处于通信连接。

[0123] 现场设备D1-D5可以具有传感器S和/或执行器A或者与其连接。

[0124] 公钥(英文Public Key)或公钥散列可以尤其分配给每个区块链节点(例如现场设备)、传感器、执行器,利用所述公钥或公钥散列能够在区块链系统之内来标识该区块链节

点、传感器、执行器。由此,可以在区块链的链节中例如借助公钥来对相应交易进行数字签名。因此可以例如将传感器值分配给传感器并且将用于确定执行器的控制命令有针对性地分派给该执行器。附加地,可以使区块链节点、传感器、执行器分别包括机密私钥,以便尤其是对交易/第一交易数据组进行数字签名。

[0125] 现场设备D1-D5可以分别包括控制设备,如在图4中已阐明的那样。区块链节点BCC其中的一个或多个例如包括创建设备,就如其例如在图3中已经阐明的那样。

[0126] 具有创建设备的区块链节点BCC可以例如创建控制功能,就如这在图1中已阐明的那样。这种控制指令例如被传送到第五现场设备D5,作为第一链节。该第五现场设备的控制设备然后对第一链节进行评估并且必要时执行控制功能,就如这在图2中已阐明的那样。

[0127] 图6示出作为区块链的第六实施例。

[0128] 详细地,图6示出区块链的这些链节610、例如第一链节611、第二链节612和第三链节613。

[0129] 这些链节610分别包括多个交易数据组T。一个、多个或所有的交易数据组可以例如是第一交易数据组,就如其在图1中被创建的那样。

[0130] 这些链节610分别还附加包括根据前任链节所构成的第一检验和CRC1、CRC2、CRC3。因此,第一链节611包括其前任链节的第一检验和,第二链节612包括第一链节611的第一检验和,并且第三链节613包括第二链节612的第一检验和。第一检验和优选地分别通过包括交易数据组T在内的总数据结构来构成。这可以如已经在之前实施例中所阐述的那样借助散列树来实现。这些检验和CRC1、CRC2、CRC3可以优选地在使用密码散列函数、诸如SHA-256或SHA-3的情况下来构成。

[0131] 为了形成散列树,这些链节分别关于自身的交易/交易数据组T包括第三检验和(通常同样为根据交易/交易数据组所构成的散列值)。通常,散列树、例如Merkle树或Patricia树被使用,其根散列值/根检验和优选作为第一检验和被存放在相应的链节中或者针对接下来的链节来被提供。

[0132] 链节还可以具有时间戳、数字签名、工作量证明证据。

[0133] 这些链节可以现在被传输给具有控制设备(例如图4中的控制设备)的现场设备并且使得该控制设备来执行所述链节的交易。如果这些交易和这些链节的完整性被认可为有效的,则控制功能因此被执行并且例如使该现场设备的执行器被操控。

[0134] 图7示出具有状态断言交易的本发明的第七实施例。

[0135] 详细地,图7示出第一交易数据组,其实现状态断言交易710。

[0136] 状态断言交易包括多个数据域、诸如用于交易720的标题/标识符、可选的公开的设备密钥730(例如3A76E21876EFA03787FD629A65E9E990...)、公钥730的所使用的算法740(例如ECC)、关于算法的参数说明750(例如曲线:brainpoolP160r1)和智能合约760,其说明传感器值770应如何被评价并且传感器值770必须满足哪些条件,以便使该交易是有效的或者能够成功地执行。附加地,状态断言交易710包括用于该状态断言交易710或第一交易数据组的时间戳780和数字签名790。

[0137] 图7尤其是示出用于状态断言交易710、传感器数据或传感器值的示例,其共同地用及时性信息来确认。及时性信息可以例如作为实时性信息(时间戳780)或计数器值。

[0138] 公开的设备密钥730可以例如为此被使用,以便确保传感器值的真实性。例如,只

有确定的传感器已提供了所述传感器值。

[0139] 图8示出具有控制动作交易的本发明的第八实施例。

[0140] 详细地,图8示出如下第一交易数据组,其实现控制动作交易810。

[0141] 控制动作交易810包括多个数据域、诸如用于交易720的标题/标识符、用于标识控制功能的可选的公钥830(例如3A76E21876EFA4711FD629A65E9E990...)、公钥730的所使用的算法740(例如ECC)、关于算法的参数说明750(例如曲线:brainpoolP160r1)和智能合约860,其说明控制动作870(例如第一控制动作)应如何被评价并且必须满足哪些安全性条件,以便使该交易是有效的或者能够成功地执行。附加地,该控制动作交易810包括:尤其是应执行控制动作870的动作目标875、时间戳780和数字签名790,其用于控制动作交易810或第一交易数据组。

[0142] 以这种方式,可以尤其是借助区块链的链节来实现安全保护的控制功能。

[0143] 图9示出作为状态断言交易和控制动作交易的组合的本发明的第九实施例。

[0144] 详细地,图9示出第一交易数据组,其将控制动作交易810与状态断言交易710相结合并且作为组合交易910来实现。

[0145] 组合交易810包括多个数据域、诸如用于交易720的标题/标识符、用于标识控制功能的可选的公钥830(例如3A76E21876EFA4711FD629A65E9E990...)、公钥730的所使用的算法740(例如ECC)、关于算法的参数说明750(例如曲线:brainpoolP160r1)和智能合约960,其说明控制动作870(例如第一控制动作)应如何被评价并且必须满足哪些安全性条件,以便使该交易是有效的或者能够成功地执行。附加地,组合交易包括用于该控制动作交易810或第一交易数据组数字签名790。

[0146] 控制应用的逻辑、例如安全性逻辑和/或控制算法和/或控制功能和/或通过控制动作交易能够作出的规定和/或安全性关键的保护功能在此作为智能合约、例如程序代码被存放在交易中。

[0147] 例如在此情况下,区块链节点、例如包括创建设备(如在图3中示出的)并且尤其是作为区块链控制节点来实现的区块链节点(BCC)根据特定技术系统、例如自动化系统的当前状态来确定交易。其可以按照确定的状态断言交易710并且可选的也根据其他当前控制动作交易810来被实施。控制逻辑和/或检验逻辑和/或要求/规定在此是被存放在智能合约960中的。可替代地或附加地,控制逻辑和/或检验逻辑和/或要求/规定被存放在确定的状态断言交易710的智能合约中和可选的其他当前控制动作交易810中。

[0148] 尽管本发明已详细地通过实施例进一步被示出并且描述,本发明并不通过所公开的示例而受限并且其他的变型方案可以由本领域技术人员由此导出,而并不偏离本发明的保护范围。

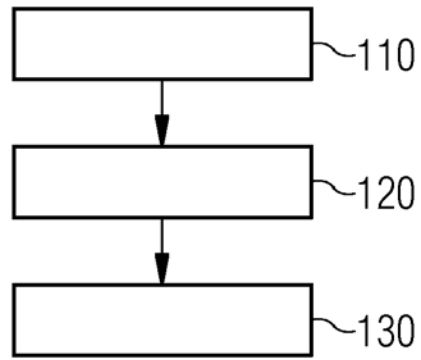


图 1

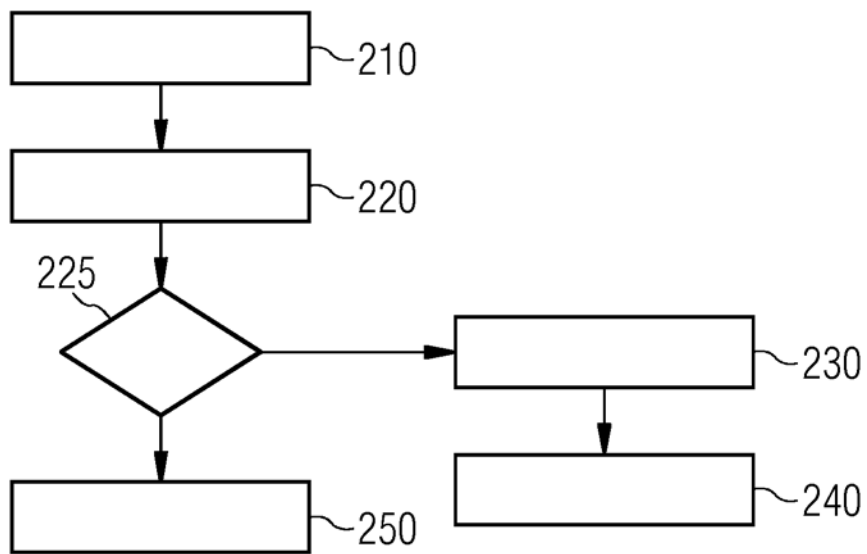


图 2

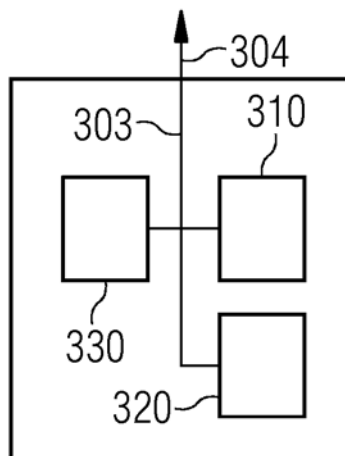


图 3

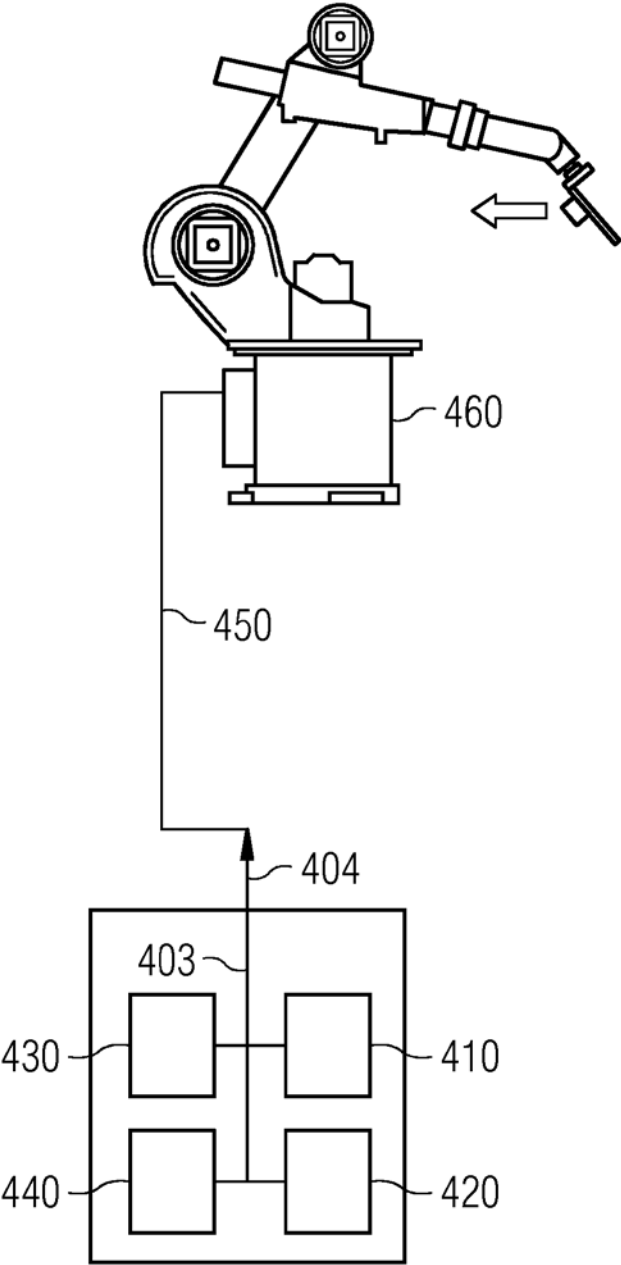


图 4

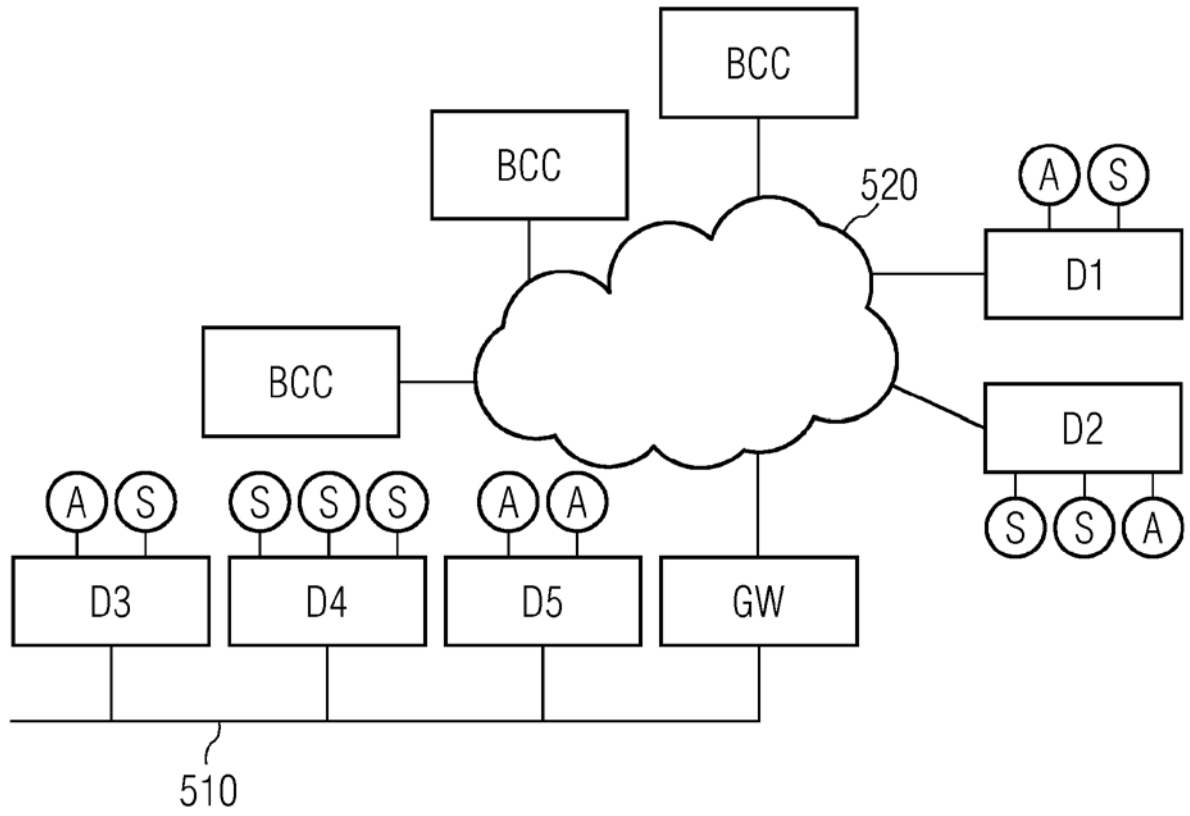


图 5

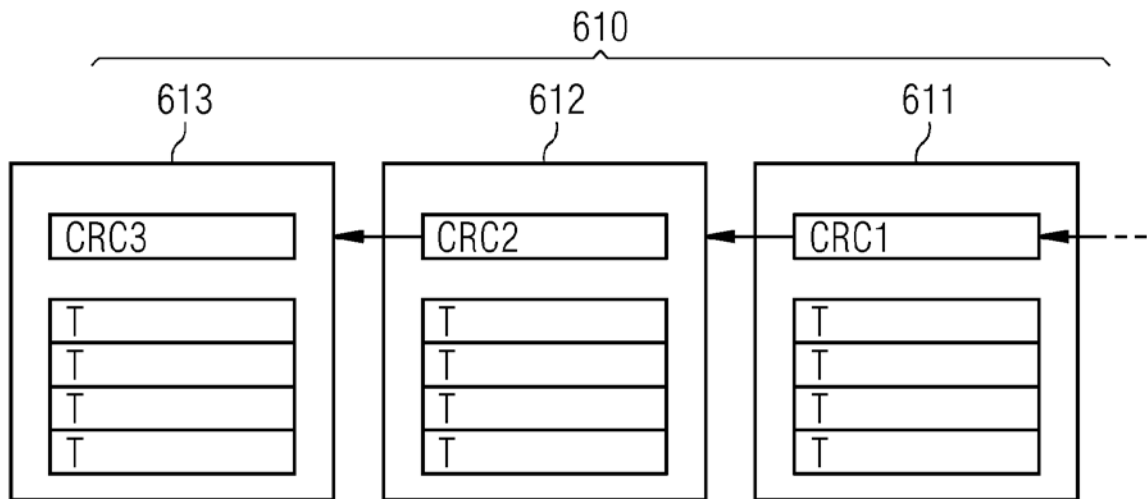


图 6

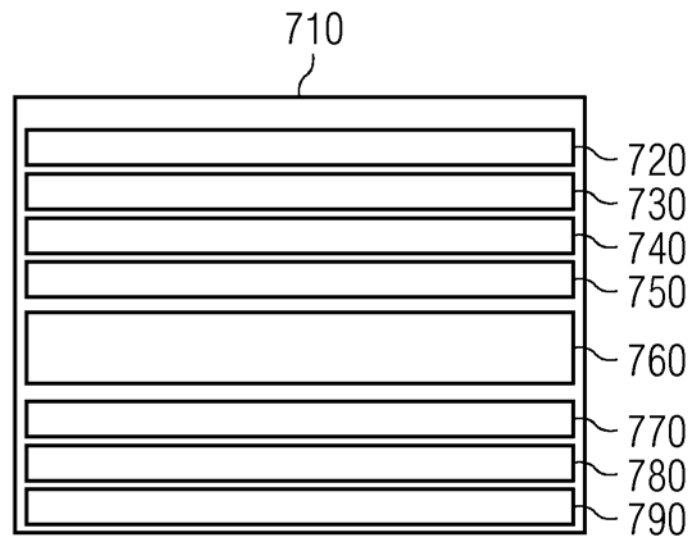


图 7

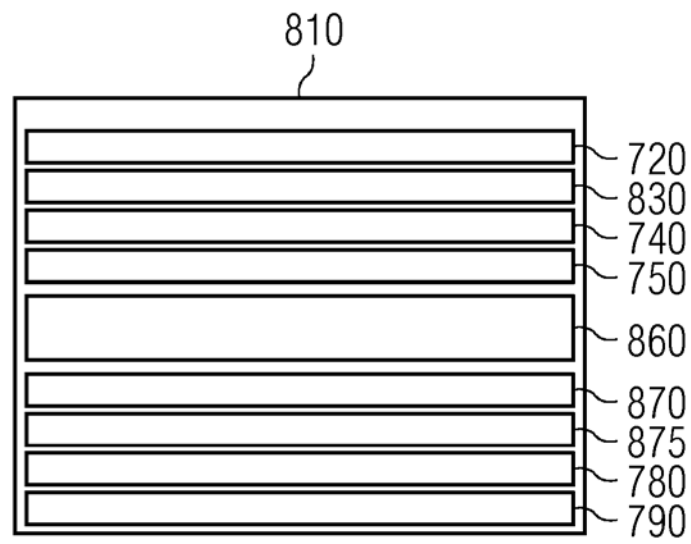


图 8

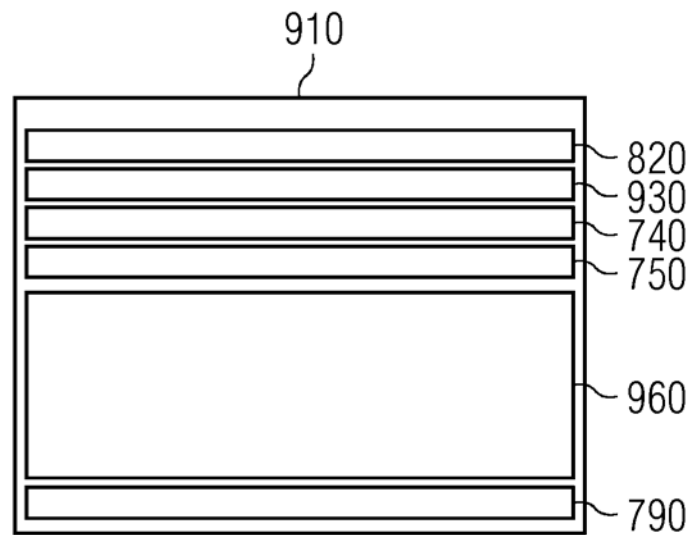


图 9