



(12) 发明专利申请

(10) 申请公布号 CN 112106092 A

(43) 申请公布日 2020.12.18

(21) 申请号 201980032104.1

(22) 申请日 2019.03.14

(30) 优先权数据

62/642,858 2018.03.14 US

(85) PCT国际申请进入国家阶段日

2020.11.12

(86) PCT国际申请的申请数据

PCT/IL2019/050283 2019.03.14

(87) PCT国际申请的公布数据

WO2019/175878 EN 2019.09.19

(71) 申请人 安全事业有限公司

地址 以色列赫维尔埃洛特区

(72) 发明人 哈盖·阿龙 纳达夫·佑兰

大卫·马克·罗森布拉特

(74) 专利代理机构 上海翼胜专利商标事务所

(普通合伙) 31218

代理人 翟羽

(51) Int.Cl.

G06Q 30/00 (2012.01)

G06Q 30/06 (2012.01)

G06Q 10/08 (2012.01)

G06Q 20/40 (2012.01)

G01N 23/22 (2018.01)

H04L 29/06 (2006.01)

H04L 12/24 (2006.01)

G06F 21/60 (2013.01)

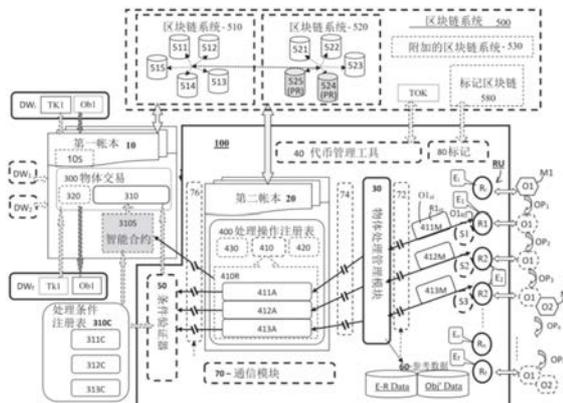
权利要求书6页 说明书29页 附图7页

(54) 发明名称

利用区块链进行供应链管理及完整性验证的系统及方法

(57) 摘要

揭露了用于管理实体物体交易的系统及方法。所述系统可连接到第一分布式账本，所述第一分布式账本适于记录与多方之间的一个或多个实体物体交易相关的多个物体交易。所述系统包含：第二分布式账本，所述第二分布式账本适于记录指示对一个或多个实体物体进行的多个物体处理操作的数据；以及物体处理管理模块，其适于认证对一个或多个实体物体进行的多个处理操作。物体处理管理模块被配置且可操作为用于获取多个处理操作的多个执行参数，对多个处理操作的多个执行参数进行认证并将认证后的多个处理操作记录在第二分布式账本中。从而，系统能够在认证对一个或多个实体物体执行的多个处理操作的多个执行参数满足一个或多个相应的预定条件时，记录与一个或多个实体物体相关联的多个物体交易。



1. 一种用于管理实体物体的交易的系统,其中:
所述系统可连接至一第一分布式账本,所述第一分布式账本适于记录在多方之间与一个或多个实体物体的交易相关联的多个物体交易;
所述系统包含:
一第二分布式账本,其适于记录数据,所述数据指示对所述一个或多个实体物体所实施的多个物体处理操作;以及
一物体处理管理模块,其适于通过实施以下操作来认证对所述一个或多个实体物体所实施的多个处理操作:
获得所述多个处理操作的多个执行参数,
认证所述多个执行参数,以及
将所述多个处理操作的所述多个执行参数记录在所述第二分布式账本中;
从而在对所述一个或多个实体物体所实施的所述多个处理操作的所述执行参数被认证为满足一个或多个各自的预定条件时,使与所述一个或多个实体物体相关联的所述物体交易得以记录。
2. 如权利要求1所述的系统,其中所述第一账本被配置且可操作为记录以下的至少一个:
 - i. 所述一个或多个物体的所有权的交易;以及
 - ii. 与所述一个或多个物体的所有权的变更相关联的代币的交易。
3. 如权利要求1或2所述的系统,其中所述第一分布式账本是能够访问所述第二分布式账本的一智能合约账本,并且适于获得指示对一特定实体物体所实施的至少一处理操作的所述数据,以及在确定所述至少一处理操作符合所述智能合约账本中的用于所述至少一物体的交易的一智能合约所指示的至少一预定条件时,将所述至少一物体的交易记录在所述第一账本中。
4. 如权利要求1或2所述的系统,包含一条件验证器模块,所述条件验证器模块能访问所述第二分布式账本,并适于获得指示对一特定实体物体所实施的至少一个处理操作的所述数据,以及在确定所述至少一处理操作符合至少一预定条件时,将所述至少一物体的交易记录在所述第一账本中。
5. 如权利要求1至4中的任一项所述的系统,可连接至一区块链系统,所述区块链系统被配置且可操作为实现所述第一分布式账本。
6. 如权利要求1至5中的任一项所述的系统,可连接至一区块链系统,所述区块链系统被配置且可操作为实现所述第二分布式账本。
7. 如权利要求1至6中的任一项所述的系统,可连接至一区块链系统,所述区块链系统被配置且可操作为实现所述第一及第二分布式账本。
8. 如权利要求6或7所述的系统,其中所述物体处理管理模块包含所述区块链系统的多个特权节点,所述多个特权节点可操作为在所述第二分布式账本中记录所述多个处理操作的所述多个执行参数。
9. 如权利要求8所述的系统,其中所述区块链系统的多个非特权节点不被允许发起将所述第二分布式账本的数据记录写入至所述区块链中。
10. 如权利要求1至9中的任一项所述的系统,包含可与所述物体处理管理模块或所述

系统的一通信模块连接的一代币管理模块,所述代币管理模块被配置且可操作为在接收到指示一特定区块链系统中的至少一预定代币交易的数据时,通过所述物体处理管理模块对所述多个处理操作进行认证/证实。

11. 如权利要求10所述的系统,其中所述第一及第二账本中的至少一个被实现在所述特定区块链系统中。

12. 如权利要求1至11中的任一项所述的系统,其中所述物体处理管理模块适于认证对所述一个或多个实体物体所实施的所述多个处理操作,其中所述一个或多个实体物体通过一个或多个读取器单元可读的一个或多个标记所标记;所述物体处理管理模块适于通过从至少一读取器单元获得指示一物体的一特定标记的数据来认证所述物体的一处理操作,所述数据通过涉及所述处理操作的所述读取器单元来读取。

13. 如权利要求12所述的系统,其中所述物体处理管理模块适于获得识别所述读取器单元的数据,并通过利用所述物体的所述特定标记来认证所述物体的身份及利用识别所述读取器单元的所述数据来认证拥有所述读取器单元及实施所述处理操作的一实体的身份,来认证所述物体的所述处理操作,从而验证所述处理操作是通过所述实体对所述被认证身份的物体所实施的。

14. 如权利要求13所述的系统,包含以下的至少一个:

i. 通过确定以下两者之间的匹配来认证所述物体的身份:从所述读取器单元获得的所述物体的所述特定标记的数据以及预先存储的指示所述物体的所述特定标记的参考数据:

ii. 通过确定以下数据之间的匹配来认证拥有所述读取器单元的所述实体的身份:识别所述读取器单元的所述数据以及列出所述一个或多个读取器单元的身份的参考数据,其中所述一个或多个读取器单元与拥有所述一个或多个读取器单元的各自的实体相关联。

15. 如权利要求13或14所述的系统,其中认证所述处理操作包含:验证对所述物体实施的所述处理操作是为所述实体授权的。

16. 如权利要求15所述的系统,其中所述第一分布式账本是一智能合约账本,其包含用于所述物体的交易的一智能合约;其中所述智能合约指示了执行针对所述物体的交易所要实施的特定一个或多个各自的处理操作的多个预定执行条件;且其中证实所述多个处理操作包含:确定所述多个处理操作是通过由所述多个执行条件所指示的所述各自的实体来实施的,且确定所述多个处理操作符合所述预定执行条件的条件。

17. 如权利要求12至16中任一项所述的系统,其中所述物体处理管理模块适于授权所述读取器单元以读取所述物体的所述特定标记。

18. 如权利要求17所述的系统,其中所述物体处理管理模块通过将指示读取参数的数据传达给所述读取器单元来授权所述读取器单元以读取所述特定标记,所述读取参数用于读取所述特定标记。

19. 如权利要求18所述的系统,其中所述读取器单元适于操作与所述读取参数相对应的一特定读取方案,从而确定并将指示所述物体的一特定标记的所述数据传送至所述物体处理管理模块。

20. 如权利要求12至19中任一项所述的系统,其中所述多个实体物体通过指示所述多个实体物体的多个物理标记来进行标记,且所述多个物理标记被施加至或嵌入在所述多个实体物体体内。

21. 如权利要求20所述的系统,其中各自的实体物体的所述物理标记分别识别所述多个实体物体。

22. 如权利要求20或21所述的系统,其中各自的实体物体的所述物理标记分别识别所述多个实体物体的类型或批次。

23. 如权利要求20至22中任一项所述的系统,其中所述多个物理标记是可利用所述各自的实体物体的X射线荧光(XRF)分析来识别的多个XRF签名,且其中所述多个读取器单元被配置且可操作为实施多个XRF测量以读取所述多个XRF签名。

24. 如权利要求23所述的系统,其中所述多个读取器单元被配置且可操作为通过用伽马射线的X射线照射所述多个物体的至少一部分并检测指示所述多个物体的所述多个XRF签名的X射线-荧光响应,来实施所述多个XRF测量。

25. 如权利要求24所述的系统,适于处理所述多个物体的所述多个XRF签名以分别确定所述多个标记。

26. 如权利要求25所述的系统,其中所述多个标记是与所述多个物体的材料组成物相关联的所述多个物体的多个本质标记,因此与所述多个物体是不可分离的。

27. 如权利要求10至20中任一项所述的系统,其中所述处理操作可以包含以下的任意一个:

- (i) 所述物体的拥有权的改变;
- (ii) 所述物体的输送/存储;
- (iii) 所述物体与另一个物体的组装。

28. 如权利要求1至27中任一项所述的系统,其与一智能合约或一处理条件注册表相关联,所述智能合约或所述处理条件注册表包含用于实施所述物体的所述交易的所述多个处理操作的至少一预定条件。

29. 如权利要求28所述的系统,其中用于实施所述处理操作的所述至少一预定条件包含至少一数据,所述至少一数据指示被指定为将要拥有所述物体的一特定实体用于执行所述各自的处理操作。

30. 如权利要求28或29所述的系统,其中关于所述智能合约中的所述处理操作所指定的所述至少一预定条件包含以下的一个或多个:

- (i) 实施所述处理操作所需的多个环境/周围条件;
- (ii) 实施所述处理操作的多个位置条件;
- (iii) 识别所述另一个物体作为所述处理操作的一先决条件。

31. 如权利要求30所述的系统,其中所述物体处理管理模块可连接至一个或多个传感器系统,所述一个或多个传感器系统被配置且可操作为测量关于所述多个处理操作的所述至少一预定条件的多个执行条件,并相应地将所述操作处理的所述多个执行参数传达至所述物体处理管理模块。

32. 如权利要求31所述的系统,其中所述物体处理管理模块可连接到至少一读取器单元,所述至少一读取器单元适于通过读取所述物体的所述特定标记来识别所述物体;且其中所述一个或多个传感器系统与所述至少一读取器单元相关联,并且适于传达与所述各自的处理操作的所述多个执行参数相关联的所述多个处理操作的所述多个执行条件。

33. 如权利要求31或32所述的系统,其中所述一个或多个传感器系统中的一传感器系

统包含至少一传感器及一读出实用程序,所述读出实用程序用于传达通过所述传感器所测量的多个执行参数的数据。

34.如权利要求31至33中任一项所述的系统,其中所述一个或多个传感器系统中的一传感器系统包含至少一传感器,所述至少一传感器包含以下的至少一个:温度传感器、湿度传感器、光传感器、位置传感器(例如,GPS)、以及惯性传感器。

35.一种用于管理多个实体物体的多个交易的方法,包含:对一物体所要执行的一个或多个处理操作中的每个处理操作实施以下操作,以在一第一分布式帐本中注册所述物体的一物体交易:

-确定所述处理操作中的已测量的多个执行参数,借以确定所述已测量的多个执行参数包含通过指定给执行所述处理操作的一实体的一读取器读取所述物体的一标记/签名;

-认证所述已测量的多个执行参数,以确定指示所述物体基于通过所述读取器所读取的所述标记/签名而被所述处理操作所执行的数据,以及识别基于关于所述读取器的数据执行所述处理操作的所述实体;以及

-利用所述已认证的多个执行参数来证实所述处理操作在一第二分布式账本中的注册,所述第二分布式账本呈现已认证的处理操作的一分布式账本;

从而在将所述一个或多个处理操作的每一者在所述第二账本中注册为已认证的处理操作后,使所述物体交易在所述第一分布式账本中的注册得以证实。

36.如权利要求35所述的方法,还包含:验证所述处理操作中的所述已认证的多个执行参数满足所述物体交易所需的多个预定条件,所述多个预定条件指示用于执行所述处理操作的至少一被指定实体及被指定为所述处理操作的对象和被指定物体的身份或类型;所述验证包含:确定作为所述处理操作的实际对象的所述物体以及所述被指定物体之间的一匹配;以及确定作为执行所述处理操作的实际实体的所述实体以及所述被指定实体之间的一匹配。

37.如权利要求36所述的方法,其中所述确定至少一处理操作的所述已测量的多个执行参数还包含:从与所述读取器相关联的一传感器测量附加的传感器数据;且所述验证还包含:确定所述传感器数据与所述多个预定条件所包含的多个附加执行条件之间的一匹配。

38.如权利要求36或37所述的方法,其中证实所述处理操作在所述第二账本中的所述注册包含:对所述处理操作的所述已测量的多个执行参数的所述验证。

39.如权利要求36至38中任一项所述的方法,其中证实所述物体交易在所述第一账本中的所述注册包含:对每个所述一个或多个处理操作中的每一个已测量的执行参数的所述验证。

40.如权利要求36至39中任一项所述的方法,其中所述第一账本是包含执行所述物体交易的一智能合约的一智能合约账本;所述智能合约包含多个子交易,其中所述多个子交易中的一个或多个与所述一个或多个处理操作相关联,并且适于访问所述第二账本以及实施验证所述一个或多个处理操作的所述已认证的多个执行参数满足所述物体交易所需的所述多个预定条件。

41.如权利要求35至40中任一项所述的方法,其中所述第一及第二账本在一个或多个区块链系统上实现。

42. 如权利要求35至41中任一项所述的方法,其中所述物体具有可识别的XRF签名/标记,以及所述读取包含检测所述物体的所述多个XRF签名,从而使所述物体的身份或类型或批次得以确定。

43. 如权利要求42所述的方法,其中所述XRF签名/标记对所述物体是本质的以及与所述物体的一个或多个部分的材料组成物相关联,因此与所述物体不可分离。

44. 一种物体签名读取器,与一个或多个区块链系统进行数据通信以证实在所述一个或多个区块链系统的第一分布式账本中的多个物体交易,所述物体签名读取器包含:

一签名/标记读取模块,其被配置且可操作为读取一实体物体上的一标记/签名以确定指示所述标记的数据;

一识别模块,其携带唯一地识别所述物体签名读取器的读取器身分证明(ID)数据;

一网络通信模块,其使所述物体签名读取器得以进行数据通信以访问指示一个或多个实体物体的多个标记/签名以及拥有与所述读取器身分证明数据相关联的所述签名读取器的一实体的参考数据,并且使所述物体签名读取器与所述一个或多个区块链系统得以通信;

一物体处理管理模块,其可连接至所述签名/标记读取模块及所述通信模块,以及被配置且可操作为:

(i) 通过执行以下操作来认证对所述实体物体所实施的至少一处理操作的多个执行参数:

○通过确定以下两者之间的匹配来认证所述实体物体的身份或类型或批次:从所述读取模块获得的所述实体物体的所述标记/签名的数据以及所述参考数据中的所述一个或多个实体物体的所述多个标记/签名;

○通过确定以下两者之间的匹配来认证拥有所述物体签名读取器的所述实体的身份:识别所述物体签名读取器的所述读取器身分证明数据以及列在所述参考数据中的所述实体的身份;

从而认证所述处理操作;以及

(ii) 操作所述网络通信模块以访问所述一个或多个区块链系统,以及证实所述已认证的处理操作在所述一个或多个区块链系统中的第二分布式账本中的注册。

从而在证实了与所述物体交易相关联的已认证的处理操作在所述第二账本中的注册后,使与所述实体物体相关联的一物体交易得以在所述第一账本中记录。

45. 如权利要求44所述的物体签名读取器,其中所述物体处理管理模块被配置且可操作为通过向所述读取模块单元提供指示用于读取所述标记/签名的多个读取参数的数据,来授权所述读取模块读取所述实体物体的所述标记/签名;其中所述读取模块适于操作与所述多个读取参数相对应的一特定读取方案,从而确定指示所述标记的所述数据。

46. 如权利要求44或45所述的物体签名读取器,包含一条件验证器模块,其适于获得指示所述处理操作的多个预定条件的所述数据,以及在验证所述已认证的处理操作的所述多个执行参数符合所述多个预定条件时,使所述已认证的处理操作在所述第二分布式账本中的所述注册得以证实。

47. 如权利要求44至46中任一项所述的物体签名读取器,包含一代币管理模块,其可连接至所述物体处理管理模块或所述网络通信模块,以及被配置且可操作为使所述处理操作

得以对所述一个或多个区块链系统中的至少一预定代币交易进行认证/证实。

48. 如权利要求44至47中的任一项所述的物体签名读取器,其中所述实体物体的签名/标记是嵌入在所述实体物体中的一本质XRF签名;

其中所述读取模块包含一XRF测量模块,其被配置且可操作为实施所述实体物体的XRF测量以读取所述XRF签名/标记;以及

其中所述读取模块被配置且可操作为通过用X射线或伽马射线照射所述物体的至少一部分以及检测指示所述XRF签名/标记的X射线-荧光响应,来实施所述XRF测量。

49. 如权利要求44至48中任一项所述的物体签名读取器,其中所述参考数据的所述至少一部分通过所述一个或多个区块链系统以去中心化的分布式方式进行存储。

50. 如权利要求44至49中的任一项所述的物体签名读取器,包含一个或多个传感器,其被配置且可操作为测量在执行所述至少一个处理时出现的一个或多个执行条件,从而使在可允许的多个执行条件下所执行的所述处理操作得以验证。

51. 如权利要求44至50中任一项所述的物体签名读取器,包含如权利要求1至34中任一项所述的系统。

利用区块链进行供应链管理及完整性验证的系统及方法

技术领域

[0001] 本发明属于供应链管理领域,更具体地涉及多个分布式账本上的多个供应链的管理。

背景技术

[0002] 物体的X射线荧光(X-ray fluorescence)签名及/或标记(在本文中通常称为标记)有利于一种用于对各种实体物体(physical object)及/或这类实体物体的类型或批次(batch)/批量(lot)进行标记以及认证的健全且可靠的技术,同时通过实际措施(例如,不破坏实体物体)来防止/消除对此类实体物体的伪造。基于添加到物体上及/或最初固有地存在于物体中的XRF标记/签名来标记及/或认证各种类型的物体的技术是多用途且健全的,以及可用于识别以及认证各种类型的物体以及材料。

[0003] 举例来说,共同转让给本申请的受让人的PCT专利申请公开案W0 2016/157185揭露了一种用于对用XRF标记进行标记的物体进行认证的方法及系统。所述方法包含,提供响应于施加到物体的X射线或伽马射线辐射而从物体来的X射线信号的检测部分的波长光谱轮廓(wavelength spectral profile),以及对X射线信号的检测部分的波长光谱轮廓进行滤波以抑制(suppress)来自波长光谱轮廓的趋势(trend)和周期性成分(periodic components),所述趋势和周期性分量与X射线信号与X射线信号部分中的噪声(noise)及杂波(clutter)的至少一个相关联,从而获得具有改善的信噪比(signal to noise ratio)及/或信号杂波比(signal to clutter ratio)的已滤波轮廓,而与所述物体所包含的材料相关联的已滤波轮廓的光谱波峰可以具有更高的准确性和可靠性来被识别。对所述物体的认证是通过处理已滤波轮廓以识别满足预定条件的所述已滤波轮廓中的一个或多个波峰来进行,由此已识别的波峰的波长指示物体中所包含的材料的特征。

[0004] 共同转让给本申请的受让人的PCT专利申请公开案W0 2017/134660揭露了一种用于通过X射线荧光(XRF)分析来验证物体(例如,金属物体)的真实性的防伪标记技术。

[0005] 共同转让给本申请的受让人的PCT专利申请公开案W0 2017/175219揭露了一种用于验证电子系统的组件(例如,部件或装置)的兼容性的方法以及系统。在特定实施例中,所述方法包含:使用XRF激发辐射照射假定与电子系统相关联的第一及第二组件,以及检测响应于所述辐射而从第一及第二组件所发出的指示第一及第二XRF签名的一个或多个的XRF响应信号。然后,对第一及第二XRF签名进行处理以确定它们是否分别与第一及第二组件上的第一及第二XRF标记的组合物相关联,并且基于第一及第二XRF签名/标记之间的对应关系(correspondence)确定/验证第一及第二组件与电子系统的兼容性。特定实施例还揭露了电子系统,其包含至少第一及第二电子组件/装置,所述第一及第二电子组件/装置分别具有使组件的兼容性得以验证的第一以及第二XRF标记的组合物。特定实施例揭露了用于基于第一及第二电子组件的第一及第二XRF签名/标记之间的对应关系来对第一及第二组件(例如,装置)进行配对的技术。特定实施例揭露了各种用于校准施加于电子组件的不同基板材料的XRF标记的XRF测量校准技术。

[0006] 共同转让给本申请的受让人的PCT专利申请公开案W0 2018/055625揭露了一种用于检测食品的不当使用及误用的方法,以及提供了一种使用XRF可识别的标记来对用于人或动物的产品进行标记的方法。所述方法包含在产品的至少一区域上形成可通过XRF识别的至少一种FDA级别材料的图案,所述图案可选地为人裸眼至少部分不可见以及具有预定的可识别特征,其中所述产品为选自食品、治疗剂以及化妆品。

[0007] 共同转让给本申请受让人的PCT专利申请公开案W0 2018/042427揭露了一种根据宝石的天然ID及/或在宝石中产生的预定标记,并且基于宝石对预定初始辐射的辐射响应的独特特征来鉴定宝石的方法及系统。

[0008] 共同转让给本申请受让人的PCT专利申请公开案W0 2018/069917揭露了用于生产透明元件的聚合物材料及XRF可识别标记的配方以及母料(masterbatches),所述透明元件包含用于各种工业用途的聚合物及至少一可识别标记。

[0009] 用于实现对实体物体的XRF标记(例如,签名)进行准确且可靠的读取的各种技术包含例如上述W0 2016/157185中所描述的技术。用于所述主题的XRF读取器可以通过例如共同转让给本申请受让人的PCT专利申请公开案W0 2017/221246中公开的一种新颖的XRF分析仪来实现。所述XRF分析仪通过调制/改变激发光束在不同物体上的强度并测量其二次辐射(secondary radiation),能够同时识别多个物体的标记组合物的存在。XRF分析仪包含辐射发射器组件,其适于发射具有空间强度分布的至少一X射线或伽马射线激发辐射束以同时辐照(irradiating)所述多个物体;辐射检测器,其用于响应于X射线或伽马射线辐射(radiation)对物体的辐照(irradiation)而检测来自多个物体的二次辐射X射线信号,并提供指示在多个物体上所检测到的数据X射线信号的空间强度分布的数据;以及与检测器通信的信号读取处理器,所述处理器适于接收及处理所检测到的响应X射线信号以验证包含在所述多个物体中的每个物体的至少一表面的标记组成物的存在。共同转让给本申请受让人的PCT专利申请公开案W0 2018/051353还揭露了一种用于控制X射线荧光(XRF)系统的操作的控制系统及方法,所述X射线荧光系统用于检测样品所携带的至少一材料,例如,样品所携带的至少一标记物。所述控制系统包含:用于接收包含关于所述至少种材料/标记物的与材料/标记物相关的输入数据的数据输入实用程序;以及数据处理器及分析仪实用程序。数据处理器及分析器实用程序被配置且可操作成:用于分析输入数据并确定XRF系统的最佳几何特性,以优化所述XRF系统的操作条件来最大化到达样品的预定区域且被所述区域的一定体积吸收的初始X射线辐射量,以及最大化从所述区域发射抵达XRF系统的检测器的二次辐射的部分;以及用于向XRF系统生成能够调整XRF系统的几何特性的操作数据。

[0010] 在虚拟域中,区块链技术提供了一种健全且安全的方式来以分布式方式存储/注册数据记录,同时实际上消除了伪造或以其他方式未经许可更改数据的可能性。区块链技术是基于节点网络,每个节点维护着组织于依照时间顺序增长的数据区块的记录的账本的副本。通常,区块链类型的数据记录利用分布式计算系统提供注册表(例如,公共),并配置为实现数据安全,防止黑客及不必要的更改。区块链的架构及设计可确保数字数据记录不会被破坏或复制(亦即,不能使用大于一次),因此可以用作虚拟资产。区块链中所记录的数据通常是指这类的虚拟资产的所有权链,称为加密货币或代币(也称为虚拟货币)。

[0011] 举例来说,PCT专利申请公开案W0 2018/064645揭露了一种分布式制造平台及相关技术,可将设计人员、制造商(例如,3D打印机所有者及其他传统制造商),运输员、及其他

实体连接起来,并简化了制造及供应新旧产品的过程。分布式帐本或区块链可用于记录交易、执行智能合约、以及执行其他操作以增加供应链的透明度和完整性。启用了区块链的包装可用于追踪从制造经过运输到递交的包装的动向及状况。

[0012] 美国专利申请公开案2019/012861讨论一种包含至少管理物品(article)的所有权的服务器的供应链系统。此物品(article)是一个实际的物体(object)。容器设有锁。锁被配置为至少通过电子程序而开启。所述容器能够物理上地(physically)存储物品(article)。当接收到开启锁的开启请求时,处理器或电路中的至少一者确定发出了开启请求的用户与具有物品所有权的用户是否匹配。当发出了开启请求的用户与具有物品所有权的用户匹配时,锁被开启以允许物品从容器中移出。服务器被通知锁已被开启。

发明内容

[0013] 各种类型的物体可以基于物体固有的及/或附加的/嵌入的XRF标记/签名容易地被识别或是特征化。这些物体可以包含例如:金属物体、聚合物,食品、宝石、电子组件/系统、以及各种其他物体/材料。从上述技术中可以理解,可以通过简单的处理以及以节省成本的方式(例如,通过将XRF响应材料嵌入及/或特征化在物体中/上)来实现将固有的XRF标记/签名附加或特征化至物体。

[0014] 本发明提供了一种将用于在虚拟域中进行注册交易的区块链技术的健全性和安全性与XRF技术的健全性、防伪安全性和多功能性相链接的新颖方法,所述XRF技术对各种类型的物体的XRF标记/签名进行标记/特征化,以及基于此类的XRF标记对各种物体及/或它们的类型/批量进行识别。

[0015] 实际上,本发明的技术基本上不限于实体物体的标记/签名的XRF类型。然而,精通通过专门利用此类物体的多用途XRF标记/签名对实体物体所实施的处理操作的组合识别、追踪及认证的新颖组合,以及将这类的认证处理记录在区块链账上的人员将会容易理解,根据本发明的如下所述的内容提供了一种用于管理实体物体的虚拟交易,并同时防止防伪的健全及安全的方法。

[0016] 为此,本发明的技术还可以通过直接链结于实体物体本身(而不是与实体物体相关联的包装/标签)的完整/独立物体签名读取器以及对实体物体所执行的处理操作的执行条件,与可用于以去中心化的方式(例如,不使用任何干预/集中式(centralized)服务/服务器或模块)追踪及注册这类的物体的去中心化(decentralized)区块链系统来实现。因此,可以在不需要介入的第三方干预的情况下安全地获得对在规定的实体对象上所执行的处理操作的认证以及对在规定的实体对象上所执行的处理操作的验证。

[0017] 为此,在部分实施例中,本发明提供了促进涉及实体物体及/或产品的点对点(peer to peer)(例如,企业对企业)交易的区块链及代币系统。

[0018] 本发明的技术可以实现以提供用于在虚拟货币及实体物体/产品之间交换的分布式、开放和安全的电子商务平台。由本发明的系统所使用/并入的(一个或多个)区块链或其部分区块链可以利用用于获得共识的机制(例如,工作量证明(proof-of-work)或权益证明(proof-of-stack))形成去中心化的、非许可制(permissionless)网络,或是形成仅被授权方被允许参与作为网络中的节点的许可制(permissioned)系统。在另一选择中,尽管非授权当事方/实体可以作为节点加入到区块链中,但是一个或多个当事方可以具有特权且比

区块链的其他成员具有更大的权限。例如,具有特权的当事方可能有权利对交易进行证实,或者有权力向区块链添加新节点。从以下描述中将容易理解,有利地在部分例子中,本发明的系统可以被实现为区块链的具有特权的当事方。本发明的系统尤其基于对各种类型的商品、产品及/或包装进行物理标记的能力,并为其提供安全且实际上不可伪造的物理签名(physical signature)。本发明的系统的整体架构使得能够在两个或多个虚拟货币账户之间并且涉及实体物体/产品的情况下实现交易及智能合约(亦即,一旦设置了其条款就会自动强行实施或执行的协议)。

[0019] 区块链系统可以在节点网络上实现(例如在服务器网络上运行)。区块链系统用于/促进存储及管理与被标记的有形/实体物体的所有权及/或拥有权(一物体的所有者可能不同于持有或拥有所述物体的当事方)有关的信息。不运行节点的区块链系统成员可以通过数字钱包或区块链应用程序与区块链系统进行相互作用,通过数字钱包或区块链应用程序所述区块链系统成员可以读取区块链中的数据以及进行记录在区块链中的资产的交易(例如,转移所有权)。区块链系统可以是去中心化及开放式的非许可制系统,也可以是仅被授权方可以成为区块链网络成员的许可制系统。区块链系统可以包含原生加密货币(native cryptocurrency)或代币。也就是所交易的虚拟货币以及其所有权历史记录在区块链系统中。

[0020] 本发明的技术提供了用于实现涉及虚拟资产及所有权记录在区块链系统上的被标记的有形物体(以下称为被标记物体)的交易及智能合约。记录被标记物体的所有权或转移被标记物体的所有权的操作可能需要通过读取单元读取被标记物体上的标记(认证物体)。为了读取标记,读取单元可能需要可以通过本发明的系统所执行的参考数据存储,或者一个或多个区块链系统中的分散存储。在部分实施方式中,可访问本发明用于认证实体物体或实体的技术所使用的读取器单元的层面及/或可访问相关参考数据的层面可能需要通过在区块链系统中预选交易的多个代币(例如,作为授权或支付)给予授权,所述代币从交易中的一个或多个当事方传至一遇选的数字钱包。

[0021] 在本发明的另一方面,区块链系统可以记录被标记物体的所有权(例如,在第一账本中)以及拥有被标记物体的当事方(例如,在另一账本中)。容易理解的是,不同的账本可以通过相同的区块链系统(例如,通过相同的区块链)或是不同的区块链系统来进行注册。系统可以随着或是不随着所有权的转移,促进涉及物体的拥有权改变的交易。将物体的拥有权从一方转移到另一方的交易可能需要转移与包含所有权转移或包含两者的转移在内的代币数量不同的代币。另外,对于不同的交易,在读取器使用方面的要求可能会有所不同。例如,一种类型的交易(例如,涉及所有权转移的交易)可能需要读取物体上的标记,而不同类型的交易(例如,仅拥有权的转移)可能不需要。

[0022] 为此,根据本发明的一广泛方面,提供了一种用于管理实体物体的交易的系统。系统可连接到适于记录与双方之间的一个或多个实体物体的交易相关联的物体交易的第一分布式帐本。系统包含适于记录指示对一个或多个实体物体所实施的物体处理操作的数据的第二分布式帐本;以及适于验证对一个或多个实体物体所实施的处理操作进行认证的物体处理管理模块。物体处理管理模块被配置且可操作用于获得所述处理操作的执行参数,认证处理操作的执行参数,以及将已认证的处理操作(例如,处理操作的已认证的执行参数)记录在第二分布式帐本中。系统从而在对一个或多个实体物体所实施的处理操作的执

行参数被认证为满足一个或多个各自的预定条件时,使得与所述一个或多个实体物体相关联的物体交易得以记录。

[0023] 在部分实施例中,第一分类账被配置且可操作用于记录以下的至少一个:(i) 一个或多个物体的所有权的交易;以及(ii) 与所述一个或多个物体的所有权变更的相关联的代币(token)的交易。

[0024] 在部分实施例中,第一分布式账本是能够访问第二分布式账本的智能合约账本,并且适于获得指示对特定实体物体所实施的至少一处理操作的所述数据,以及在确定至少一处理操作符合智能合约账本中的用于所述至少一物体的交易的一智能合约所指示的至少一预定条件时,将至少一物体的交易记录在第一账本中。

[0025] 在部分实施例中,系统包含条件验证器模块,其能访问第二分布式账本并适于获得指示对特定实体物体所实施的至少一处理操作的所述数据,以及在确定至少一处理操作符合至少一预定条件时,将至少一物体的交易记录在第一账本中。

[0026] 在部分实施例中,系统可连接至被配置且可操作为实现第一分布式账本的区块链系统。替代地或附加地,在部分实施例中,系统可连接至被配置且可操作为实现第二分布式账本的区块链系统。在部分实施例中,区块链系统被配置且可操作为实现第一分布式账本及第二分布式账本。在部分实施方式中,物体处理管理模块包含区块链系统的多个特权节点以及可操作为在第二分布式账本中记录处理操作的执行参数。在这方面,区块链系统的多个非特权节点不被允许发起将第二分布式账本的数据记录写入至区块链中。

[0027] 在部分实施例中,系统包含可与物体处理管理模块或系统的通信模块连接的代币管理模块,所述代币管理模块被配置且可操作为在接收到指示特定区块链系统中的至少一预定代币交易的数据时,通过物体处理管理模块对所述处理操作进行认证/证实。

[0028] 在部分实施例中,物体处理管理模块适于认证对一个或多个实体物体所实施的处理操作,其中所述一个或多个实体物体通过一个或多个读取器单元(在下文中也可互换地称为“物体签名读取器”)可读的一个或多个标记所标记。物体处理管理模块适于通过从至少一读取器单元获得指示物体的特定标记的数据来认证实体物体的处理操作,所述数据通过涉及处理操作的读取器单元来读取。在部分实施方式中,物体处理管理模块适于获得识别读取器单元的数据,并通过利用物体的特定标记来认证物体的身份及利用识别读取器单元的数据来认证拥有读取器单元及实施处理操作的实体的身份,来认证实体物体的处理操作,从而验证处理操作是通过实体对被认证身份的物体所实施的。为此,物体处理管理模块可以被配置且可操作为实施以下操作:

[0029] i. 通过确定以下两者之间的匹配来认证所述物体的身份:从所述读取器单元获得的物体的所述特定标记的数据以及预先存储的指示所述物体的所述特定标记的参考数据:

[0030] ii. 通过确定以下数据之间的匹配来认证拥有读取器单元的实体的身份:识别所述读取器单元的所述数据以及列出所述一个或多个读取器单元的身份的参考数据,其中所述一个或多个读取器单元与拥有所述一个或多个读取器单元的各自的实体相关联。

[0031] 根据部分实施例,处理操作的认证还包含验证对所述物体实施的处理操作是为所述实体授权的。

[0032] 在部分实施例中,第一分布式账本是包含用于实体物体的交易的智能合约的智能合约账本。智能合约可以指示对实体物体的物体交易所要实施的特定一个或多个各自的处

理操作的预定执行条件；且其中证实多个处理操作可包含：确定处理操作是通过由执行条件（在下文中也称为“被指定的实体”）所指示的各自的实体来实施的，且确定处理操作符合预定执行条件的条件。

[0033] 根据部分实施例，物体处理管理模块还适于授权读取器单元（例如，及/或读取器单元的“标记/签名读取模块”）读取物体的特定标记。为此，物体处理管理模块可以通过与读取器单元（例如，与读取器单元的标记/签名读取模块）进行通信以向读取器单元提供指示用于读取特定标记的读取参数的数据，来授权读取器单元以读取特定标记。继而，读取器单元（例如，标记/签名读取模块）适于操作与读取参数相对应的特定读取方案，从而确定并将指示物体的特定标记的数据传送至物体处理管理模块。

[0034] 在部分实施例中，物理标记是可利用各自的实体物体的X射线荧光分析来识别的多个X射线荧光（XRF）签名。读取器单元（例如，读取器单元的标记/签名读取模块）被配置且可操作为实施XRF测量以读取XRF签名。例如，读取器单元被配置且可操作为通过用X射线或伽马射线照射所述多个物体的至少一部分并检测指示实体物体的XRF签名的X射线-荧光响应，来实施XRF测量。在部分实施方式中，读取器单元（例如，读取器单元的标记/签名读取模块）被配置且可操作为对实体物体的XRF签名进行处理以分别确定实体物体的标记/签名。为此，标记/签名可以是与物体的材料组成物相关联的实体物体的本质（elemental）标记，因此与所述物体是不可分离的。

[0035] 根据本发明的部分实施例，涉及实体物体的物体交易的处理操作可以包含以下的任何一个：

[0036] (i) 物体的所有权的改变；

[0037] (ii) 物体的输送/存储；

[0038] (iii) 物体与另一个物体的组装。

[0039] 为此，在部分实施例中，系统可以与所述第一账本中的智能合约或处理条件注册表相关联，所述智能合约或所述处理条件注册表包含用于实施物体的交易的处理操作的至少一预定条件。用于处理操作的至少一预定条件可例如包含指示被指定为将要拥有物体的特定实体用以执行各自的处理操作的的数据、及/或作为处理操作的对象的身分及/或物体的类型/批次。此外，在部分例子中，预定条件可包含以下的一个或多个：

[0040] -实施处理操作所需的多个环境/周围条件；

[0041] -实施处理操作的位置条件；

[0042] -识别另一个物体作为处理操作的先决条件。

[0043] 在部分实施例中，物体处理管理模块可连接至一个或多个传感器系统，所述一个或多个传感器系统被配置且可操作为测量关于处理操作的至少一预定条件的执行条件，并相应地将操作处理的执行参数传达至物体处理管理模块。例如，物体处理管理模块可连接到适于通过读取物体的特定标记来识别物体的至少一读取器单元。所述一个或多个传感器系统与所述至少一读取器单元相关联（例如，包含在其中），并且适于传达与各自的处理操作的执行参数相关联的处理操作的执行条件。传感器系统可包含例如至少一传感器及用于传达利用传感器所测量的执行参数数据的读出实用程序，所述至少一传感器可例如是：温度传感器、湿度传感器、湿度传感器、光传感器、位置传感器（例如，GPS）、惯性传感器、以及计时器/计时传感器。

[0044] 根据本发明的另一广泛方面,提供了一种用于管理实体物体的交易的方法。所述方法包含对实体物体所要执行的一个或多个处理操作中的每个处理操作实施以下操作,以在第一分布式帐本中注册实体物体的物体交易:

[0045] -确定处理操作中的已测量的执行参数,借以确定已测量的执行参数包含通过指定给执行处理操作的实体的读取器读取物体的标记/签名;

[0046] -认证已测量的执行参数,以确定指示实体物体基于通过读取器所读取的标记/签名而被所述处理操作所执行的数据,以及识别基于关于读取器的数据执行处理操作的实体;以及

[0047] -利用已认证的执行参数来证实处理操作在第二分布式账本中的注册,所述第二分布式账本从而呈现已认证的处理操作的分布式账本;

[0048] 所述方法从而在将一个或多个处理操作的每一者在第二账本中注册为已认证的处理操作后,使物体交易在第一分布式账本中的注册得以证实。

[0049] 在部分实施例中,所述方法还包含:验证所述处理操作中的已认证的执行参数满足所述物体交易所需的预定条件,所述预定条件指示用于执行所述处理操作的至少一被指定实体及被指定为所述处理操作的对象的可指定物体的身份或类型;所述验证包含:确定作为处理操作的实际对象的所述物体以及被指定物体之间的匹配;以及确定作为执行处理操作的实际实体的所述实体以及被指定实体之间的匹配。

[0050] 根据部分实施例,确定至少一处理操作的已测量的执行参数还包含:从与读取器单元相关联的传感器测量附加的传感器数据;且所述验证还包含:确定传感器数据与预定条件所包含的附加执行条件之间的匹配。

[0051] 在部分实施例中,证实处理操作在第二账本中的注册包含:对处理操作的已测量的执行参数的验证。

[0052] 为此,在部分实施例中,证实物体交易在第一账本中的注册可包含:对一个或多个处理操作的每个处理操作的每个已测量的执行参数的验证。

[0053] 如上所述的,第一账本可以是包含执行所述物体交易的一智能合约的一智能合约账本。在部分实施例中,智能合约包含多个子交易,其中多个子交易中的一个或多个(例如,其可选性地可以以计算机可执行的码/脚本的形式通过第一帐本来执行)与一个或多个处理操作相关联,并且适于访问第二账本以及实施上述的验证一个或多个处理操作的已认证的执行参数满足物体交易所需的预定条件。

[0054] 如上所述的,在部分实施例中,实体物体具有可识别的XRF签名/标记,以及所述读取器包含检测物体的XRF签名,从而使物体的身份或类型或批次得以确定。XRF签名/标记对所述物体可以是本质(elemental)的以及与所述物体的一个或多个部分的材料组成物相关联,因此与所述物体不可分离。

[0055] 根据本发明的又一广泛方面,提供了一种物体签名读取器(例如,在上文中又称为“读取器”或“读取器单元”),其可以被配置且可操作用于独立地操作以监控/测量物体的处理操作;认证处理操作,以及可能地验证已认证的处理操作满足预定条件,以及在第二帐本中注册已认证且可能地还已验证的处理操作。物体签名读取器与一个或多个区块链系统进行数据通信且可使在通过一个或多个区块链系统所实现的第一分布式账本中的物体交易得以证实。物体签名读取器包含:(a)签名/标记读取模块,其被配置且可操作为读取实体

物体上的标记/签名以确定指示标记/签名的数据；(b) 识别模块，其携带唯一地识别物体签名读取器的读取器ID数据；(c) 网络通信模块，其使物体签名读取器得以进行数据通信以访问指示一个或多个实体物体的标记/签名以及拥有与读取器ID数据相关联的物体签名读取器的实体的参考数据，并且使物体签名读取器与一个或多个区块链系统得以通信；以及(d) 物体处理管理模块，其可连接至签名/标记读取模块及通信模块。物体处理管理模块可以被配置且可操作为通过实施以下操作来认证对实体物体所实施的至少一处理操作的执行参数：

[0056] -通过确定以下两者之间的匹配来认证所述实体物体的身分或类型或批次：从所述读取模块获得的实体物体的所述标记/签名的数据以及所述参考数据中的一个或多个实体物体的标记/签名；

[0057] -通过确定以下两者之间的匹配来认证拥有物体签名读取器的实体的身份：识别所述物体签名读取器的读取器ID数据以及列在参考数据中的所述实体的身份；

[0058] 从而认证所述处理操作。物体处理管理模块还可以被配置且可操作为操作网络通信模块以访问一个或多个区块链系统，以及证实已认证的处理操作在第二分布式账本中的注册。物体签名读取器从而在证实了与物体交易相关联的已认证的处理操作在第二账本中的注册后，使与实体物体相关联的物体交易得以在第一账本中记录。

[0059] 在部分实施例中，物体签名读取器的物体处理管理模块被配置且可操作为通过向所述读取模块提供指示用于读取标记/签名的读取参数的数据，来授权读取模块读取所述实体物体的标记/签名。读取模块适于操作与读取参数相对应的特定读取方案，从而确定指示所述标记/签名的数据。

[0060] 在部分实施例中，物体签名读取器还包含条件验证器模块，其适于获得指示处理操作的预定条件的数据，以及适于在验证已认证的处理操作的执行参数符合预定条件时，使已认证的处理操作在第二分布式账本中的注册得以证实。

[0061] 在部分实施例中，物体签名读取器包含代币管理模块，其可连接至物体处理管理模块或所述网络通信模块，以及被配置且可操作为在一个或多个区块链系统中出现至少一预定代币交易时，对处理操作进行认证/证实。

[0062] 在部分实施例中，实体物体的签名/标记是嵌入在所述实体物体中的本质XRF签名。读取模块包含XRF测量模块，其被配置且可操作为实施实体物体的XRF测量以读取XRF签名/标记。例如，读取模块可被配置且可操作为通过用X射线或伽马射线照射所述物体的至少一部分以及检测指示所述XRF签名/标记的X射线-荧光响应，来实施XRF测量。

[0063] 在部分实施例中，参考数据的至少一部分通过一个或多个区块链系统以去中心化的分布式方式进行存储，以及物体签名读取器的物体处理管理模块适于访问一个或多个区块链系统以提取参考数据的至少一部分。

附图说明

[0064] 为了更好地理解本文公开的主题并举例说明如何实际地进行实施，现在将仅通过非限制性示例的方式并参考附图来描述实施例，其中：

[0065] 图1是根据本发明一实施例示意性示出的系统100的方块图；

[0066] 图2A是根据本发明的各种实施例详细示出可以实现的具有各种模块的系统100的

方块图；

[0067] 图2B是根据本发明一实施例的方法200的流程图；

[0068] 图2C是根据本发明示意性地示被实现为集成的物体签名读取器系统的系统100的方块图；

[0069] 图3及图4及图6是根据本发明的另外的实施例示意性地示出系统100的方块图；

[0070] 图5是根据本发明又一实施例的方法600的流程图；以及

[0071] 图6是示出根据本发明又一实施例的系统100的方块图。

具体实施方式

[0072] 在图1中示出了用于实现本发明的多个交易及/或多个智能合约的系统100的一实施例，图1为包含区块链系统500、管理模块30及可选的代币(token)管理工具40的所述系统的总体结构的示意图。

[0073] 管理模块30(在下文中也可互换地称为管理系统/模块及/或处理管理模块)与多个读取器单元R1、R2至Rn通信，读取器单元R1、R2至Rn可以读取多个被标记物体上的实体标记(物体的签名)。可选地，多个读取单元也可以与区块链系统500通信来验证物体上的标记已被读取及识别(例如，作为附加的安全层)。

[0074] 区块链系统500与多个数字钱包DW1、DW2至DWn相互作用。所述多个数字钱包可以被实现为在任何类型的计算设备(例如智能手机、PDA、PC及服务器)上运行的软件。所述多个数字钱包也可以在区块链500的多个节点上运行。数字钱包DW1至DWn还可以与管理系统30及代币管理工具40通信。

[0075] 管理系统30与存储了指示多个被标记物体上的标记的信息相关联的参考数据。物体上的标记对于所述物体可以是唯一的(例如，呈现所述物体的多个标识符)，使得所述标记可以用作与特定物体相关联的一签名。或者，标记可以对应于多个物体，例如，属于相同批次的多个物体或多个产品。此外，管理系统30可以存储为了实施对一被标记物体的标记的测量所需要的数据(例如，用于读取多个特定物体的多个标记或多个类型的多个读取方案)。可选地，可以由管理系统30单独访问这种类型的信息，使得一读取单元仅在从管理系统30接收到这数据之后才能够读取一物体的标记。管理系统30也可以与存储了关于多个读取器的其他信息的参考数据相关联。例如，参考数据存储了读取器使用的位置、时间及日期、识别读取器的一序列号(读取器的身份证件(ID))、及识别读取器的ID、及/或操作读取器的人员/实体。

[0076] 根据本发明的各种实施例，通过多个读取单元(以下称为读取器)所读取的物体的/物体上的标记可以是应用于或嵌入到物体中并配置为与所述物体永久且物理地相关联的各种标记方法中的任何一种，例如全息图(hologram)、QR码，紫外线或红外线标记剂(UV、IR taggant)，RFID标签、以及基于X射线衍射(X-ray Diffraction, XRD)或X射线荧光(X-Ray Fluorescence, XRF)分析技术的X射线签名。术语“标记”在本文中应该被广泛地理解为是指被施加、耦合、附加或印刷在物体上的标记/标签，或者是嵌入在物体中的不可分离的标记/签名。同样地，此处使用的“标记”可以指的是物体固有的/本质的标记，例如表示物体特征的签名或是能够识别物体及/或物体的类型及/或物体的来源的本身材料(例如，贵重的石头或钻石通常具有这类的本质标记/签名的特征)；或者指的是添加到/附加到物体的

标记。

[0077] 合适的物体标记可以使用标准或专门配置的读取单元来读取,并且可能需要特定的扫描/读取协议及参数。在一示例中,读取器是可以检测及识别从被标记物体发射的电磁辐射的光谱仪。特别地,读取器可以识别被标记物体响应于初始的电磁辐射对被标记物体的辐照所发射的响应信号。在一较佳示例中,读取器是XRF分析仪(特别是能量色散(energy dispersive) XRF分析仪),其向被标记物体发射X射线或伽马射线辐射,并从而检测从被标记物体来的响应X射线信号。为了读取对XRF敏感的标记(亦即,可以通过XRF分析检测到的标记),读取器应根据多个预定的读取参数来调整。这些参数包含:X射线发射器参数(亦即,X射线发射管的电流及电压)、过滤传入或传出信号的滤波器的类型、以及读取的持续时间(亦即,X射线发射器向物体发射辐射的持续时间)。可设置的附加参数包含X射线发射器、检测器与被标记物体之间的距离及角度,如以引用方式并入本文的国际专利申请案PCT/IL2017/051050中所述。读取物体上的标记所需的参数可以存储在管理系统40上,并且仅提供给有授权对一特定物体进行读取的特定读取器,如以引用方式并入本文的美国临时专利申请案62/503,067中所述。

[0078] 在本发明的系统100的一方面中,物体可以用两种或多种类型的标记来进行标记。其中一种类型的标记可以在从管理系统30接收数据之后被读取,而其中一种或多种类型的标记可以在不需要来自测量系统的信息下由合适的读取器来读取。例如,物体可以被标记为对XRF敏感的标记,其仅在从管理系统接收到数据后才能测量标记(并且在没有合适的读取器下可以是不可见且不可检测的),此外,物体可以用一条形码或QR码进行标记,所述条形码或QR码为可见的且可以通过任意条形码或QR码扫描仪进行读取。

[0079] 在本发明的一态样中,管理系统30本身可以被设计为一区块链系统(在下文中也被称为管理区块链),其中与多个物体上的多个标记有关的数据的许多副本被存储在多个节点中。与标记有关的存储数据(例如,下面显示的参考数据Obj' Data)可以被加密,使得签名及/或与读取单元读取签名的方式有关的数据受到保护。在一示例中,标记管理系统30可以被实现为或包含构成区块链系统500的一部分的一管理区块链。在本案中,管理系统30的多个节点可以具有区块链系统500的多个特权节点的作用以存储及管理受保护的数据,所述数据不会与区块链系统的其余部分共享(例如,与物体上的标记有关的数据)。

[0080] 区块链系统500可以用作一公共账本,其记录在多方之间的多种类型的可交易项目(在下文中也可互换地称为“物体”或“资产”)的所有权(ownership)(及/或拥有权(possession))及交易数据。如上所述,多方可以通过数字钱包DW1至DWn连接到区块链系统500。这类的数字钱包每一个包含可用于证明一可交易资产/物体或该资产的一部分的所有权的数据(例如,一公钥加密系统中的一私钥)。可交易资产可以是以下的一个或多个:(i) 多个被标记的有形物体或这类物体的一部分;(ii) 由代币管理工具40管理的一代币(token),其可以是与区块链系统500相关联的原生代币(native token)。代币可以表示与服务或实用程序有关的资产。例如,代币可以使代币的拥有者能够使用管理系统30提供的服务或是要求使用管理系统30的服务。在一特定示例中,代币可以是允许访问管理系统30中的数据(例如,对应于一特定物体上的实体标记)的数据(例如,存储在数字钱包中的一个或多个私钥中的一组)。在另一示例中,用户可以使用代币来购买或雇用读取器,或者为要求使用读取器的服务付费。

[0081] 代币管理工具40控制区块链系统500及管理系统30之间的接口,并提供或拒绝对由管理系统30记录的数据或可以由管理系统30获得的数据的访问。另外,在使用读取单元及读取服务可以由管理系统30管理的情况下,代币管理工具40可以控制对读取单元的访问。例如,代币管理工具40可以适于响应于由一代币拥有者(例如是拥有代币的一实体)提供的一请求进行操作,以操作/指示标记管理系统及/或读取单元来验证物体是通过一特定代码进行标记(亦即,代币拥有者支付代币以进行验证)。在另一示例中,代币管理工具40允许自由访问这类的数据,并且仅针对从一用户(亦即,数字钱包)转移一物体的所有权的交易要求代币。每一个服务的代币价格可能取决于所需的特定服务以及其他因素。

[0082] 现在一起参照图2A及2B,其分别是根据本发明的部分实施例的用于管理一个或多个物体{01、02}的物体交易300的系统的方块图100及方法的流程图200。从本揭露内容中可以理解,根据本发明的系统100及方法200特别适合于在多个实体/当事方(例如,从E_i到E_f)之间的实体物体(例如,01)交易的管理,其中物体交易可以在一分布式账本(例如,10)平台(例如,区块链500)上实施/注册Obj1。例如,当注册Obj1从实体E_i的数字钱包DW_i转移到实体E_f的数字钱包DW_f,物体01的交易310在分布式账本10中示出。如图所示,通过将代币TK1从实体E_i的数字钱包DW_i转移到实体E_f的数字钱包DW_f,代币TK1的对应交易(例如,加密货币)也可能被注册在分布式账本10中(例如,与物体交易310相关联)。实际上,通常情况是,实体物体的交易受多个特定处理操作(例如,OP1至OP_n)所限制或决定,所述处理操作通过实体(例如,E_i到E_n)来执行,其可能是人员/公司(例如,沿着在双方E_i及E_i之间的一供应链对物体01进行供应及/或制造/制作及/或包装及/或组装及/或运输及/或存储)。因此,实体物体01的物体交易300和物体代币交易TK1在分布式账本10中的注册Obj1及TK1可以被限制使得物体交易310所需的处理操作OP1至OP_n满足/达到所需的处理条件310C(例如,由被授权的实体及/或在预定的执行条件(例如,令人满意的环境条件/位置等)下对实体物体01执行那些操作)。

[0083] 本发明的系统100和方法200提供了一种新颖技术,用于将用于注册这样的物体交易300的虚拟环境区块链500及帐本10与在这样的物体交易期间物体{例如,01及02}被实际处理时所处的实际/物理环境进行链接的,以及促使容易地对为了这样的物体交易300而对物体{例如,01及02}/在物体上所执行的处理操作的执行条件进行认证,并且可能地自动地验证处理操作是根据物体交易的先决条件被适当地执行的。

[0084] 因此,本发明提供了一种新颖的解决手段,其适于例如监控多个物体的一供应链。

[0085] 就这一点而言,本文使用术语“认证”(authenticate)及类似的术语来表示对多个实际物体{01及02}所进行的鉴定(identification)/认证,或是表示对涉及多个处理操作的实际物体的类型(type)/批量(lot)/批次(batch)进行的鉴定/认证,以及表示对涉及/实施所述多个处理操作的相应的实际实体{E1至E2}进行的鉴定/认证,并且可能地,在部分实施例中,还确定所述多个处理操作执行时所处/所在的一些执行条件(例如,环境/惯性条件及/或位置)。

[0086] 一般而言,认证与多个读取器单元RU的操作以及可能与读取器单元RU相关联的多个附加传感器相关联,而一处理操作的多个执行条件(所涉及的物体及实体的身份,以及通过多个传感器感应的多个可能附加条件)通过认证来测量/确定。为了实现这一点,由多个读取器单元(例如带有或不带有附加传感器411M至413M)所测量的多个执行条件被比较,例

如由读取器单元RU或由物体处理管理模块30将其与参考数据60进行比较,如下所述,并且它们之间的一匹配表示了多个处理条件的真实性,从而产出多个确实的处理条件411A至413A。认证操作本身可以仅由多个读取器单元来执行。

[0087] 本文使用术语“进行证实”(validate)或“证实”(validation)等来表示使用在一区块链系统中作为对区块链中的一交易(已确认的交易)进行存储/注册/记录的一先决条件的一操作。如本领域技术人员将理解的,当请求在区块链系统中注册/存储交易时,所请求的交易是待定的(pending),直到其被“证实”并获得关于所述交易的去中心化共识(在这一点上,应注意到可能没有正式的「待定状态」,所请求的交易通常不会被注册直到区块链中的多个节点完成关于交易验证的去中心化共识)。在进行此类证实下,待定的交易变为有效/被证实的交易,并被注册及存储在区块链中。为此,本文中的术语“待定”交易或交易“请求”用于表示待证实的交易。一般术语“交易”的含义可以指的是“已注册”的交易或“待定”的交易,应根据上下文进行解释。在这方面,应该注意的是,本文所述的第一账本10用于注册多个物体交易300,它们的证实取决于对与所述物体交易中的物体所执行的特定处理操作。为此,这些物体交易300(在本文中通常也称为“交易”)通常保持为待定交易(未注册)的状态,直到与那些交易相关联或所要求的多个处理操作被证实及验证。一物体交易(例如,310)在第二账本20中与各自的交易相关联的所有处理操作OP1至OP3被证实以及验证有效的处理操作OP1至OP3满足交易300的处理条件要求311C至310C后可以进行证实。继而,一特定物体交易310的处理操作OP1至OP3通常在第二账本20中以多个交易(例如,411A至413A)来表示。处理操作OP1至OP3可以被视为第二账本20的多个待定交易,直到其各自的所测量的执行条件411M至413M被系统100认证而产生各自的已认证的执行条件411A至413A为止,以及可选地,在一实施例中,它们还保持待定状态,直到已认证的执行条件411A至413A被验证为与各自的处理操作OP1至OP3的先决处理条件311C至313C匹配为止。然后,至少已认证并且可能还经过验证的处理操作OP1至OP3通过系统100进行证实,并照此被注册在第二账本20中(例如,在所述图中通过注册已认证的执行条件411A至413A来举例说明)。

[0088] 本文使用术语“进行验证”(verify)或“验证”(verification)来表示实际/已认证的多个物体{01及02}、实际/已认证的多个实体{E1至E2}及/或涉及多个处理操作OP1至OP3的多个实际执行条件满足相应的物体交易(例如,310)的多个处理条件OP1至OP3的要求(前提处理条件311C至313C)。为此,对已认证的处理操作411A的验证可以在将已认证的处理操作411A注册在账本20中之前通过系统100来执行,在这种情况下,已认证的处理操作411A实际上呈现已验证的已认证处理操作411A。替代地,对已认证的处理操作的验证可以在将已认证的处理操作411A注册在账本20中之后通过系统100、帐本10中的智能合约及任一其他实体中的一个来执行,在这种情况下,帐本20呈现已认证但不一定已验证的处理操作。如上所述,一物体交易(例如,310)在对其所有处理操作进行验证及认证之后才进行证实。

[0089] 为了实现这一点,系统100可连接到第一分布式账本10,其适于记录在多方{Ei、Ef}之间的与一个或多个实体物体{01、02}的交易相关联的物体交易300(例如,所有权/代币的改变)。系统100包含第二分布式账本20。第二分布式账本20适于记录指示对所述一个或多个实体物体{01、02}的物体交易(例如,310)所执行的物体处理操作{OP1至OPn}(例如,拥有权及/或运输/处理/组装的条件的改变)的数据。通常,只有处理操作的已认证记录存储在第二分布式账本20中,以便第二分布式账本20可以用作与物体的交易300相关联的多

个处理操作 {OP1至OPn} 的多个执行参数的已认证注册表。系统100还包含物体处理管理模块30,其可配置且操作用于通过执行以下操作来认证对一个或多个实体物体 {01、02} 所实施的多个处理操作 {OP1至OPn}: (i) 获取所述多个处理操作 {OP1至OPn} 的多个执行参数 {411M至413M} (例如,确定要执行处理操作 {411M至413M} 的一个或多个条件), (ii) 认证所述多个执行参数 {411M至413M}, 以及 (iii) 将所述多个处理操作 {OP1至OPn} 的所述多个执行参数 {411M至413M} (或只有相应的多个执行参数 {411A至413A}) 记录在第二分布式账本20中。因此,在验证了对一个或多个实体物体 {01、02} 所实施的多个处理操作 {OP1至OPn} 的已认证的多个执行参数满足一个或多个相应的预定条件 {311C至313C} 后,系统100促进了与一个或多个实体物体 {01、02} 相关联的物体交易300 (例如,所有权的改变) 的验证及记录。

[0090] 参考图2B,现在将一并跟图2A所示的模块来描述根据本发明实施例的用于证实物体交易的方法200。

[0091] 在操作210中,提供一特定物体01的一待定期交易310。物体交易310等待确定以在第一账本10中进行注册,且将在对交易300的注册所要求执行的各自的处理操作 (例如,OP1到OP3) 的多个预定条件311C至313C被满足时进行注册。待定期交易310可以例如是一智能合约310S的形式,或者可以在一特定处理条件数据注册表310C中找到预定条件311C至313C。

[0092] 在可选的操作215中,待定期交易310的处理操作OP1至OP3被设置/认为是即将注册在第二账本20中的一待定期交易。例如,假使待定期交易310是智能合约310S,它可以包含智能合约310S的多个子交易 (例如,条件311C至313C), 其由待定期交易310的操作OP1至OP3在第二账本20中的证实及注册所限制。

[0093] 操作220通常通过本发明的多个读取器单元RU来执行,读取器单元RU通常利用执行处理操作的实体 (例如,E1至En) 来进行操作,且相应的读取器分配给所述实体。例如,在操作220中,在执行处理操作OP1时,获得已测量的多个执行参数411M,其指示对由处理操作OP1所实施的物体01的标记M1 (例如,签名) 的读取。已测量的多个执行参数411M通过分配给执行处理操作OP1的实体E1的读取器 (例如,R1) 获得/读取,且可能还包含从可与相应的读取器R1相关联的附加传感器S1获得的附加传感器数据。

[0094] 操作230通常通过物体处理管理模块30来执行,且包含对已测量的多个执行参数411M进行认证,以基于已测量的多个执行参数411M来确定由处理操作OP1所实施的物体01的身份以及执行处理操作OP1的实体E1,从而获得已认证的多个执行参数411A。

[0095] 然后,通常由物体处理管理模块40或相应的读取器单元R1执行操作250,以证实处理操作OP1中的已认证的多个执行参数411A在第二账本20中的注册。

[0096] 如操作252中所示,可选地,根据本发明的部分实施例,第二账本20注册了已认证的多个处理操作 (但不一定是已验证的处理操作)。

[0097] 替代地,如可选的操作254所示,第二账本20中的处理操作OP1的证实还包含验证处理操作OP1中的已认证的多个执行参数411A满足/达到相应的处理操作OP1的多个预定条件311C。这可以通过例如如下所述的系统100的条件验证器模块50来执行。在本例中,第二账本20注册了已认证及已验证的多个处理操作。

[0098] 最后,当物体交易310的所有处理操作OP1至OP3都已认证、及已验证或即将被验证

时,可以执行操作260以证实待定物体交易310在第一账本10中的注册。在这方面,操作262可以在第二账本20注册了已认证但不一定经过验证的处理操作的情况(例如,如上所述的操作252)下执行。在这样的情况下,证实物体交易310的注册包含验证待定物体交易310中的所有处理操作OP1至OP3的已认证的执行参数411A至413A已在第二账本20中注册,以及验证那些已认证的执行参数411A至413A都满足物体交易310的各自的预定条件311C至313C。操作262可以例如通过如下所述的系统100的条件验证器模块50来执行。替代地,操作264可以在第二账本20注册了已认证及已验证的处理操作的情况(例如,如上所述的操作254)下执行。在这样的情况下,在操作264中,在所有已验证及已认证的处理操作OP1至OP3已在第二账本20注册时,待定物体交易310被证实已在第一分账本10中注册。这可以例如通过第一账本10中的一智能合约来执行。

[0099] 可选地,在操作240中,上述的操作220、230、250(例如,252或254)或260(例如,262或264)中的一个或多个可以仅在一预定代币交易发生时,通过系统100(例如,账本10)在一特定或多个区块链系统500中执行。这可以由系统100的代币管理工具40执行。

[0100] 根据本发明的各种实施例的方法200的进一步细节及实施方式一并参照系统100叙述如下。本领域技术人员将容易理解如何实施方法200中叙述如下的特征。

[0101] 返回到图2A,在这样的验证已认证的执行参数{411A至413A}满足交易的条件{311C至313C}下,第一账本10可以被配置且可操作于自动记录一物体交易(例如,310)。就这一点而言,物体交易310可以包含例如(i)一个或多个物体(例如,01)的所有权0b1的交易;以及(ii)与一个或多个物体(例如,01)的所有权变更相关联的代币Tk1的交易。

[0102] 例如,第一分布式账本10可以是一智能合约账本10S,其能够访问第二分布式账本20,且适于获得对实体物体01所实施的处理操作(例如,OP1,OP2或OP3)的已认证的执行参数411A、412A或413A的,以及在确定所述至少一处理操作(例如,OP1,OP2或OP3)符合由账本10S中的智能合约310S指示用于所述物体的交易的至少一预定条件{例如,311C、312C或313C}时,将至少一物体01的物体交易记录在第一账本10中。

[0103] 替代地或附加地,系统100可以包含一条件验证器模块50,其适于获得对物体01所实施的处理操作(例如,OP1,OP2或OP3)的已认证的执行参数411A、412A或413A,将已认证的执行参数411A、412A或413A与预定条件(例如,311C、312C或313C)进行验证/比对,以及在确定与此物体交易310相关联的所有处理操作(例如,OP1至OPn)的参数符合其各自的预定条件{例如,311C、312C或313C}时,在第一账本10中记录/验证物体01的物体交易310。

[0104] 分布式账本10及20通常在一个或多个区块链系统500上实现。实现分布式账本10及20的区块链系统可以是相同的(例如,单个)区块链系统500,其以连接的节点/服务器511至515及521至525为示例,其中每个节点/服务器都携带账本10及20的副本。在这方面,应当理解,在部分实施例中,分布式账本10及20的记录可以一起写在同一区块链500的区块中。

[0105] 替代地或另外地,在部分实施例中,实现分布式账本10及20的区块链500分别是不同的区块链510及520,其由区块链510中连接的节点/服务器511至515(实现第一分布式账本10),以及区块链520中连接的节点/服务器521至525(实现第二个分布式账本20)为示例。

[0106] 因此,当账本10及20是在区块链(例如,500或510及520)上实现时,账本10及20是去中心化的分布式账本,其对于记录/交易伪造通常不具有集中化的脆弱性或是具有被减弱的集中化的脆弱性。这使得系统100特别有利于用在实体物体的交易,其可能自然地涉及

许多(未必可信任的实体来处理所述物体的交易例如,在供应链的例子中通常如此),因为没有单一实体独自地负责将数据写入/记录在账本中。在这方面,应当理解,将记录写入账本10及20中的任何一个(与区块链(在下文中通常为500)的区块的写入相关联)可以根据任何适当的区块链技术来实现,且通常包含根据合适的区块链协议/技术(例如,“工作量证明”加“证实”(proof-of-work plus validation)或“权益证明”(proof-of-stake))在各自的区块链的多个节点之间达成去中心化共识。取决于系统100的特定实施方式,实现账本10、20或两者的区块链510、520或500可以各自是一私有或公共的区块链,并可以被配置且可操作为使用相同或不同的区块链协议/技术。

[0107] 应当注意,根据本发明的部分实施例,物体处理管理模块30包含区块链系统500或520的多个特权节点PR(例如,524及525),其可操作(例如,排他地)用于请求在第二分布式账本20内的处理操作(例如,OP1、OP2或OP3)的执行参数(例如,411A、412A或413A)的记录/注册。为此,没有这种特权的所述区块链系统500或520的其它节点(例如,521至523),可能不被允许发起/请求将数据记录写入至区块链500或520中。

[0108] 根据本发明的部分实施例,系统100还包含一代币管理模块40,其被配置且可操作为选择性地启用或防止在第二分布式账本20内写入(例如,发布/注册)。处理操作(例如,OP1、OP2或OP3)的已认证的执行参数(例如,411A、412A或413A),或者在某些情况下,甚至有选择地允许或防止在第二账本20内写入已测量的执行参数(例如,411M、412M或413M)。为此,代币管理模块40可以被配置且可操作为根据接收到指示在与系统100相关联的一个或多个区块链系统500中的一者的一代币TOK的一预定交易的数据TOK,选择性地启用/发起或是阻止任何执行参数(例如,411M或411A A)的写入/发布/注册。代币TOK所要求的预定交易可以是与一特定所要求的实体(E_i及E_f中的或E_i到E_n中的的一预定实体)相关联的一交易,并且可以当作用来授权系统100以实施相应的处理操作(例如,OP1)的各自的测量/认证的一信号。在部分实施方式中,为了启动/发起处理操作OP1的测量/认证而即将被接收的代币TOK的属性,或是它的执行参数(例如,411M或411A A)任一者的注册,可以由智能合约310S或与相应的物体交易310相关联的处理条件注册表310C所包含/指定。因此,在接收到预定的代币TOK时,代币管理模块40可以启动/发起测量/认证及/或相应执行参数(例如,411M或411A A)的注册/记录。

[0109] 为此,系统100通常可以包含一数据/网络通信模块70,其促进区块链系统500(或至少例如实现账本20的520)的与它的通信。代币管理模块40可以连接到数据/网络通信模块70,例如连接到数据/网络通信模块70的至少一组件/开关,例如70、72、74或76,且代币管理模块40被配置且可操作为以由此利用数据/网络通信模块70来启动/发起或是防止对一特定执行参数(例如,411M或411A)的测量/认证及/或注册/记录。替代地或附加地,物体处理管理模块30可以与代币管理模块40连接,并且适于在与一特定执行参数(例如,411M或411A)有关的测量/认证及/或注册/记录中的任何一项活动之前,从代币管理模块40中请求/接收授权指令。

[0110] 为此,物体处理管理模块30适于认证对一个或多个实体物体O₁,O₂所实施的处理操作(例如,OP1、OP2或OP3)。一个或多个实体物体O₁,O₂利用一个或多个标记M₁,M₂来标记,这些标记可通过与系统100相关联或包含在系统100内的一个或多个读取器单元RU(例如,图2A所示分别与实体E_i、E₁、E₂及E_f(例如,人员/公司)相关联的读取器R_i、R₁、R₂及R_f)来读

取。物体处理管理模块30适于通过从至少一个读取器单元(例如,R1)获得指示物体O1的一特定的标记M1的数据,来认证一物体(例如,O1)的处理操作(例如,OP1),所述数据可通过涉及所述处理操作OP1的读取器单元R1来读取。

[0111] 系统100可以包含参考数据注册表60(例如,其可以例如利用一个或多个数据库、云数据存储及/或在区块链500的多个分布式账本中实现),或者可以与参考数据注册表60相关联。参考数据通常包含:

[0112] (a) 实体与读取器参考数据E-R-Data,其存储了将系统的读取器单元R_i、R₁、R₂及R_f与当前拥有这些读取器的各自实体E_i、E₁、E₂及E_f的标识符相关联的数据。因此,系统100(例如,物体处理管理模块30)可以容易地将读取器的标识符R_{1id}(亦即,分配给每个读取器的唯一识别码)与具有/使用相应读取器R₁的实体E₁(人员/公司/部门)的身份相关联,如表1中所示:

E-R-Data		
[0113] 读取器	实体	
R _{1id}	E ₁ 的 ID	

[0114] 表1

[0115] (b) 物体参考数据Obj'-Data存储了识别数据(例如,O_{1id}),其指示了与可利用系统100的读取器单元R_i、R₁、R₂及R_f轻易读取的相应的标记(例如,M1(例如,优选地,本质的XRF标记或其它可能的标记/标签))相关联的各个物体(例如,O1)。因此,系统100(例如,物体处理管理模块30)可以容易地将物体O1读取到(例如,通过任一读取器单元)的标记(例如,M1)与物体的识别(例如,O_{1id})相关联。实际上,在部分实施例,物体参考数据Obj'-Data还存储了与每个/部分物体O1相关联(例如,与每个/部分物体标记的标记M1相关联)的多个特定读取指令O_{IRD}(读取方案/参数),所述读取指令O_{IRD}是为了适当地操作读取器单元R_i、R₁、R₂及R_f中的一个或多个以使用适当的读取方案O_{IRD}并正确地读取物体O1上的相应标记M1所需要的。以这种方式,将读取方案O_{IRD}提供给读取器R₁实际上授权读取器R₁并让读取器R₁能够读取/破译物体的身份O_{1id}。在本例中,给定指示物体O1(或物体类型)为一物体交易310的物体的数据(其数据可以从物体交易300的处理条件注册表310C获得),系统100(例如,物体处理管理模块30)从物体参考数据Obj'-Data中提取与所述物体/物体类型相关联的适当读取方案O_{IRD},并将读取方案O_{IRD}发送/传达给相应的读取器(例如,R1)使得读取器R1能够识别物体O1。例如,如表2中所示:

Obj'-Data		
[0116] 物体/批次/类型的 ID	标记	读取方案
O _{1id}	M1	O _{IRD}

[0117] 表2

[0118] 在这方面,应当注意,在部分实施例,将物体参考数据Obj'-Data也注册在一分

布式账本中(例如,在区块链580中或在另一区块链500中)是有利的。在标记不易/实际上无法伪造的情况下,这一点可能特别重要,(例如XRF本质标记,其为物体材料的固有部分)。这是因为拥有具有标记M1的物体O1的第一实体(例如,Ei)物体O1而言通常可视为是值得信任的。因此,将物体参考数据Obj'-data放置在分布式账本/区块链(例如,580)中,让这类的实体能够先将具有标记M1的物体O1注册在物体参考数据Obj'-data中,使得这个参考数据是去中心化及分散的,并且实际上无法被伪造。实际上,这对于本质标记(诸如XRF标记)而言更为重要,因为这类的本质标记,当它们是物体材料的一部分,在许多情况下并无法实际地从物体中移除。为此,系统10可以可选地包含一标记管理模块80,其被配置且可操作为使得能够利用分布式标记账本580中的物体参考数据Obj'-Data来标记物体的注册。标记管理模块80可以被实现为构成区块链系统500或580的一部分的一管理区块链,以及可以包含所述区块链系统500或580中具有特权对物体参考数据Obj'-Data进行存储及管理的多个特权节点。可选地,物体参考数据Obj'-Data也可以是不能与区块链系统500的其余部分共享的受保护数据。

[0119] 应当理解,在本公开内容中所使用的术语“标记”(marking)应被广义地解释为涉及与物体相关联的任何类型的标记/标签及签名。例如,这些可以是打印在物体上的QR码、附着/耦接至物体的RFID标签、以及XRF标记及签名。对于XRF而言,应该注意的是,部分物体(例如,钻石或其他宝石)可以固有地包含作为物体的固有标记的强烈特征化的XRF签名,且物体上并未被施加任何主动的标记动作。替代地,在人造物体中,可以通过利用任何合适的技术让物体的材料包含一些对XRF有反应的材料组合物/混合物,或是用对XRF有反应的材料组合物/混合物涂覆物体,来诱使XRF签名标记于物体。

[0120] 为此,对感兴趣的一物体O1的一特定标记(它是一附加的标记/代码或标签、或是一固有的本质签名)进行识别、特征化或施加的一实体Ei可以访问分布式标记账本580以及注册具有标记M1且可能具有用于读取标记的合适读取方案OIRd的物体的ID O1id。可选地,在部分实施例中,可以通过标记管理模块80来监督分布式标记账本580,标记管理模块80可以具有将物体标记注册在分布式标记账本580中的特权,以及可以被配置且可操作用于提供这类的注册服务给感兴趣的实体。

[0121] 此外,在部分实施例中,实体与读取器参考数据E-R-Data也可以被注册在分布式账本中。例如,读取器单元(例如,Ri、Ri至Rn及Rf)本身可以被视为物体,其传送至实体Ei、Ei至En及Ef的物体交易或来自实体Ei、Ei至En及Ef的物体交易被注册在账本10中并且通过系统100管理,类似于本文关于物体O1所述的。例如,希望租借一读取器的一实体可以通过一物体交易(例如,注册在账本10或一类似账本(在本例中,它实际上将会存储实体与读取器参考数据E-R-Data)中的320)来这样做。

[0122] 根据本发明的各个实施例,无论参考数据60的存储方式如何,物体处理管理模块30都适于利用参考数据60来认证物体O1的处理操作OP1以验证处理操作OP1是通过所述实体E1实施在被识别的物体O1上。这包含,例如:

[0123] i. 利用物体的所述特定标记M1来认证所述物体O1的身份O1id。更具体地,认证物体O1的身份O1id是通过确定以下数据之间的匹配来进行:从读取器单元R1获得的物体O1的所述特定标记M1的数据,以及预先存储的指示物体O1是利用所述特定标记M1进行标记的参考数据Obj'-Data;以及

[0124] ii. 利用辨别所述读取器单元R1的数据R1_{id}来认证拥有读取器单元R1并实施所述处理操作OP1的实体E1的身份。认证拥有读取器单元R1的实体E1的身份可以通过确定以下数据之间的匹配来进行：识别所述读取器单元的数据R1_{id}，以及列出所述一个或多个读取器单元 {Ri、R1、R2、Rf} 的身份的参考数据E-R-Data，其中所述一个或多个读取器单元 {Ri、R1、R2、Rf} 与拥有所述一个或多个读取器单元 {Ri、R1、R2、Rf} 的各自的实体 {Ei、E1、E2、Ef} 相关联。

[0125] 在部分实施方式中，在操作读取器单元R1之前，物体处理管理模块30适于授权读取器单元R1以读取物体O1的特定标记M1，及/或适于为了此授权读取器单元R1这件事获得/测量一相应的处理操作（例如，OP1）的任何其他执行参数411M。例如，如上所述，在一些实施方式中，物体处理管理模块30通过传送指示用于读取特定标记M1的读取参数O1_{RD}的数据给读取器单元R1，来授权读取器单元R1以读取所述特定标记M1。继而，读取器单元R1可适于操作与读取参数O1_{RD}相对应的一特定读取方案，并从而确定指示物体O1的一特定标记M1的数据，以及将所述数据传送至所述物体处理管理模块30。在本例中，物体身份的认证及验证的步骤可以视为是同时执行的。这是因为，在作为物体交易300对象的被声称物体的身分与正在处理/读取的实际物体不匹配的情况下，正在读取的实际物体O1的不正确的读取参数O1_{RD}可能会从物体交易300的处理条件注册表310C中获得，这可能继而导致对实际物体O1的不正确读取。

[0126] 在本发明的部分实施例中，在对处理操作OP1进行认证之后，接着是验证对所述物体（亦即，O1）实施的处理操作OP_i是为所述实体E_i授权的。

[0127] 例如，第一分布式账本10可以是包含用于物体O1的物体交易310的一智能合约310S的一智能合约账本10S。智能合约310S指示了多个预定条件310C，其包含对物体O1的物体交易310即将要实施的特定一个或多个相应的处理操作 {OP1、OP2、OP3} 的执行条件 {311C、312C、313C}。因此，可以通过确定处理操作 {OP1、OP2、OP3} 是利用由执行条件 {311C、312C、313C} 所指示的相应的实体 {E1、E2、E3} 来实施，以及它们的已认证的执行参数 {411A、412A、413A} 也符合执行条件 {311C、312C、313C}，来实现验证处理操作 {OP1、OP2、OP3}。

[0128] 根据本发明的部分实施例，实体物体 {O1、O2} 由实体标记 {M1、M2} 进行标记，物理标记 {M1、M2} 被施加或嵌入到实体物体 {O1、O2} 中，或者是实体物体 {O1、O2} 本质的/固有的，并指示这些实体物体 {O1、O2} 的身份。为此，各个实体物体 {O1、O2} 的物理标记 {M1、M2} 可以分别识别特定实体物体 {O1、O2}。替代地或附加地，各个实体物体 {O1、O2} 的物理标记 {M1、M2} 分别识别实体物体的类型或批次。在任何这样的例子中，在本文中的标记被视为识别物体，无论是识别特定物体，还是仅为识别物体的类型/批次。

[0129] 在部分实施例中，实体标记 {M1、M2} 是可通过对各个实体物体 {O1、O2} 进行XRF分析来识别的X射线-荧光 (X-Ray-Fluorescence, XRF) 签名。在这类的例子中，读取器单元 {Ri、R1、R2、Rf} 被配置且可操作用于在所述实体标记 {M1、M2} 上实施XRF测量以读取XRF签名。为此，标记 {M1、M2} 可以是与物体的材料成分相关联的物体 {O1、O2} 的本质标记，因此与所述物体 {O1、O2} 是无法分离的。读取器单元 {Ri、R1、R2、Rf} 可以被配置且可操作为通过用伽马射线或是X射线照射所述物体 {O1、O2} 的至少一部分以及检测指示所述物体 {O1、O2} 的XRF签名的X射线-荧光响应来实施XRF测量。系统100（例如，处理管理模块30）可以被配置且可操作为对物体 {O1、O2} 的XRF签名进行处理以分别确定所述标记 {M1、M2}。可以由处理管

理模块30及/或读取器单元RU实现及/或实施以识别XRF签名/标记的技术的示例例如在PCT专利申请公开案WO 2016/157185、WO 2017/221246及WO 2018/051353中详细揭露,它们共同转让给本申请的受让人并以全文引用方式并入本文。为此,在部分实施例中,读取器单元RU或读取器单元RU的至少一读取模块(例如,图2C中的90)及/或处理管理模块30可以根据本发明被配置且操作以实现这些PCT公开案中所述的用于读取及/或测量及/或处理及/或分析物体的XRF签名/标记中的任何一个或多个技术。

[0130] 应当注意的是,处理操作(例如,利用读取器监控),可能包含以下的任何一个或多个:

[0131] (i) OP1-物体01的拥有权的改变。在图2A的示例中,将被识别的物体01的拥有权从实体E_i转移到实体E₁,并且在本示例中,拥有权的改变是通过实体E₁的读取器R₁来进行认证。因此,系统100验证/认证物体01的拥有权从实体E_i到实体E₁的改变。

[0132] (ii) OP2-物体01的输送/存储(例如,在图2A的示例中,物体01随后从实体E_i被输送到实体E₂(通过也获得物体01的所有权的实体E₂)。在本示例中,被识别的物体01的输送是通过实体E₂的读取器R₂的读取来进行验证/认证。因此,系统100验证/认证实体E₂执行了输送/存储的操作OP2以及从实体E₁到实体E₂的所有权的改变。

[0133] (iii) OP3-物体01与另一个物体02的组装。在本示例中,实体E₂还参与物体01及02的组装。被识别的物体01与另一个物体的组装是通过实体E₂的读取器R₂的读取来进行验证/认证。在另一个物体02也可以通过系统100识别的例子中,例如在本示例中,物体02的识别也可以通过实体E₂的读取器R₂来进行验证/认证。因此,系统100验证/认证实体E₂执行了组装的操作OP3。

[0134] 如本领域技术人员将理解的,对于在作为物体交易310的当事方的初始实体E_i及最终实体E_f之间的物体01(以及与物体01顺着物体交易310进行组装或结合的可能附加物体(例如,02))的交易310,可能需要附加的处理操作OP₁至OP_n或其他类型的处理操作。例如,处理操作OP₁至OP_n可以表示为为了实施在当事方E_i及E_f之间的物体01的物体交易310所需的多个供应链操作。已认证/已验证的操作OP₁至OP_n(亦即,其执行参数411M至413M(例如,指示执行各个操作的实体以及所述操作要执行的物体,以及可能的附加参数))通过系统100进行读取/测量。

[0135] 用于验证物体及实体的读取器单元RU以及可能附加的传感器(例如,S₁至S₃)可以与各自的读取器R₁至R₃或各自的实体E₁至E₃相关联,以测量附加的执行参数(例如,执行操作的地理位置、操作的环境/惯性条件、及/或与操作相关的其它物体/材料)。系统100,例如在部分例子中,读取器RU本身,或更一般而言,处理管理模块30,适于访问参考数据60,如上所述,以便认证执行参数411M至413M以及确定已认证的执行参数411A至413A。在这方面,“认证”应当被理解为系统100(例如,RU或模块30)对从从读取器RU(以及可能还从传感器)获得的测量/读取进行比较/分析的操作,以便至少识别出实施/执行处理操作OP₁至OP_n的实际实体E₁至E_n,以及处理操作所执行的实际物体01以及可能的物体02的身分。在进行这类的认证时,执行参数(例如,411A至413A)的真实性被确定,其中在来自可与读取器相关联的可选的传感器S₁至S₃的这些操作期间,可获取涉及相应的处理操作OP₁至OP₃的实际实体E₁至E_n及实际物体01、02,以及识别符(可能地与附加的传感器测量/数据一起)。

[0136] 已认证的执行参数411A至413A被注册及被记录为在第二分布式帐本中管理的记

录器处理操作400的注册表410R,其与应通过相应的处理操作OP1至OPn执行的相应的物体交易310相关联。如在图2A的非限制性示例中所示,已认证的执行参数(例如,411A至413A)被记录在第二账本20中(例如,在本例中,对已测量的执行参数(例如,411M)进行认证,然后在第二账本20中记录所得到的各个经过认证的执行参数411A。)然而,在部分替代实施例中,原始/已测量的执行参数411M到413M被先记录在第二分布式账本20中,然后可执行上述的认证(例如,与验证处理操作是否满足对相应的物体交易310所需的预定处理条件{311C至313C}一起进行)。

[0137] 如本领域技术人员将容易理解的,第二分布式账本20可以在区块链系统520或500的节点(例如,服务器)521至525及可能地511至515上实现。执行已认证的执行参数411A至413A的记录的系统100(例如,处理管理模块30)可以与区块链系统520或500的特定的特权节点524及525相关联,或者是可以包含所述特定的特权节点524及525,其独有地被允许对在第二分布式账本20的记录进行写入/存储/更改。因此,由于区块链系统520或500的其他节点仅可以对执行参数(例如,411A至413A)进行读取,分布式账本中的记录器执行参数可以被信任为是可靠的。为此,在一些实施方式中,实现第二分布式账本20的区块链系统520或500可以是允许访问任何感兴趣的当事方(例如,Ei、E1到En、Ef)或其他当事方以读取注册在第二分布式账本20的执行参数(例如,411A至413A)的一开放系统。其他当事方可以是任何其他实体,或者是其他区块链系统,(例如,具体地实现注册了物体的物体交易的第一分布式账本10(其可以是智能合约账本)的区块链系统510)。在部分实施方式中,实现第二分布式账本20的区块链系统520或500可以是仅允许访问第二分布式账本20的选定的当事方成员(例如,Ei、E1、Ef及/或510)以读取注册在第二分布式账本20的执行参数(例如,411A至413A)的一封闭系统。选定的当事方可以例如是相应物体交易310的当事方Ei、Ef及/或实现注册/实现了物体的交易的第一分布式账本10的区块链系统510(其可以是智能合约账本)。这允许有关联的当事方访问与各个物体交易310相关联的记录器处理操作410的账本20中的注册表410R,以使它们能够验证物体交易的处理操作的执行参数411A至413A满足交易条件310C。

[0138] 关于这一点,在本发明的部分实施例中,系统100包含与记录了物体交易(例如,310)的处理条件311C至313C的处理条件注册表310C相关联的可选的验证模块50。验证模块50被配置且可操作用于从处理条件注册表310C中提取所述处理条件311C至313C,并将它们与通过系统100(例如,第二分布式账本20中的记录器,或是由物体处理管理模块30确定)获得的相应的已认证的执行参数411A至413A进行比较,以便验证相应的物体交易310的处理条件是否已满足。

[0139] 替代地或附加地,被允许的感兴趣当事方(例如,Ei、Ef)可以自己访问/请求记录在第二分布式账本20中的已认证的执行参数411A至413A以验证相应的物体交易310的处理条件是否已满足。

[0140] 又可替代地或附加地,第一分布式账本10可以被实现为记录了已认证的执行参数411A至413A的智能合约账本10S,其例如能够获得对第二账本20的访问。合约账本10S(例如,以太坊(Ethereum)区块链上的账本)例如可以包含用于物体交易310的执行的智能合约310S,其中用于这个物体交易310的处理条件注册表310C在本例中可以被包含在智能合约310S本身中。在本例中,物体交易(例如,310)的处理条件311C至313C可以表示为智能合约

310S的记录(例如,脚本或计算机可执行码),智能合约310S在第一分布式账本10中的各个执行导致从第二账本20中对已认证的执行参数411A至413A的相应记录的提取/读取,每个相应的处理条件311C至313C与相应的已认证的执行参数411A至413A的比较、以及智能合约310S中的相应的处理条件311C至313C是否已满足的确定。例如,对应于/表示在智能合约310S中的处理条件311C的可执行码/脚本发起从第二账本20中读取相应的已认证的执行参数411A,以及通过处理条件311C的代码/脚本来处理已认证的执行参数411A以确定已认证的执行参数411A是否满足由其相应的脚本/代码所指定的处理条件311C的要求。通过这样进行,账本10的智能合约310S中的每个处理条件311C至313C可以利用系统100的第二账本20来自动验证物体交易310的条件对于实体物体(例如,01,及可能还有02,其为物体交易310的物体)。

[0141] 因此,与系统相关联的智能合约310S或处理条件注册表310C可以用于实施物体01的物体交易310的所述处理操作(例如,0P1至0P3)的至少一预定条件(例如,311C至313C)。用于执行一处理操作的一预定条件311C至313C可以指示被指派为拥有物体01的一特定实体来执行相应的处理操作0P1至0P3。可选地,涉及相应的处理操作0P1至0P3所指定的至少一预定条件(例如,311C至313C)可以进一步包含以下的一个或多个:

[0142] -实施处理操作所需的多个环境/周围(environmental/ambient)条件(例如,温度、湿度、光照条件、压力、及/或惯性条件)。利用XRF传感器/读取器监控部份这些条件及/或对物体01的影响于例如WO 2018/055625中所述,其被共同转让给本申请的受让人,并以引用方式并入本文。

[0143] -实施所述处理操作的位置条件(例如,允许的地理坐标/位置);

[0144] -在物体交易310的条件下识别应与物体01进行组装的另一个物体(例如,02)作为处理操作的一先决条件(例如,所述识别可以是利用另一个物体02的XRF标记,以及利用另一个物体与物体的配对,如在WO 2017/175219中所述,其被共同转让给本申请的受让人,并以引用方式并入本文)。

[0145] 实际上,监控这些条件可能与诸如在实体之间转移物体01的拥有权的处理操作(例如,0P1)有关,以及可能是其他操作及/或是与物体的存储或输送有关联的操作(例如,0P2)及/或可能地将物体01与另一个物体02进行组装的操作。

[0146] 在这一点上,物体处理管理模块30可以连接至一个或多个感测系统(例如,传感器)S1、S2、S3(其可以被包含在相应的读取器R1、R2、R3中或与之相关联)。感测系统S1、S2、S3被配置且可操作用于测量关于处理操作0P1至0P3的所述至少一预定条件311C至313C的执行条件,并相应地将处理操作0P1至0P3的执行参数411M至413M附带这些执行条件传达到物体处理管理模块30。因此,可连接到读取器单元(例如,R1、R2及R3)的物体处理管理模块30适于识别物体01(通过读取物体01的特定标记M1),以及与读取器单元R1、R2及R3相关联的一个或多个传感器系统S1,S2,S3适于传达相应的处理操作(例如,0P1至0P3)的执行条件(连同通过读取器单元所读取的物体01的识别)。

[0147] 在这一点上,读取器单元(例如,R1、R2及R3)可以包含合适的标记读取器(例如,XRF读取器、QR码读取器、RFID读取器及line)、具有读取器R1_{id}的标识符的识别模块存储器、以及用于将读取器R1_{id}的标识符以及指示标记已读取的数据01_{id}传达给物体处理管理模块30的读出实用程序。感测系统(例如,传感器3)(例如,S1、S2、S3)可包含至少一个上述

的传感器S1、S2及/或S3以及用于将通过传感器测量的执行参数数据传达给物体处理管理模块30的读出实用程序。所述至少一传感器S1、S2及/或S3可以包含以下的至少一个：温度传感器、湿度传感器、光传感器、位置传感器（例如，GPS）、及惯性传感器。在部分实施例中，读取器单元及传感器系统被组合在一个系统/模块中，其能够读取物体的标记，又能够感测附加的执行参数，如上所述。

[0148] 现在参照图2C，其根据本发明的实施例的系统100的方块图，所述系统100被配置为独立的、集成的（自立的）的物体签名读取器系统（例如，在上面也称为“读取器”或“读取器单元”）。在本示例中，物体签名读取器系统100被配置且可操作于独立地运作对物体进行的监视/测量的处理操作；认证处理操作，并且可能地验证已认证的处理操作是否满足预定条件，以及在第二账本20中注册已认证且可能还已验证的处理操作。物体签名读取器可以与包含一个或多个区块链系统500及选择性的数字钱包DW的区块链网络501进行数据通信，从而可以使在通过一个或多个区块链系统500所实现的第一分布式账本10中的物体交易得以证实。在这方面，应当注意的是，物体签名读取器系统100可以被配置且可操作为通过与区块链系统500（在本图中未具体示出）的节点/服务器的直接通信或是通过与数字钱包DWs（其转而与区块链系统500的节点/服务器进行通信）的间接通信，来与区块链系统500进行通信以证实处理操作及/或物体交易。

[0149] 物体签名读取器100整体地包含（例如，在一设备中）：

[0150] (a) 签名/标记读取模块R，其被配置且可操作于读取实体物体01上的标记/签名以确定指示标记/签名的数据；

[0151] (b) 识别模块90（例如，内部的存储器/存储模块），其携带唯一地识别物体签名读取器100的读取器ID数据；

[0152] (c) 网络通信模块70，其被配置且可操作于提供物体签名读取器100的数据通信以访问参考数据60。参考数据指示一个或多个实体物体（例如，01）的标记/签名以及拥有与读取器ID数据相关联的物体签名读取器100的特定实体。网络通信模块70还被配置且可操作于在物体签名读取器100及区块链网络501（例如，一个或多个区块链系统500或与一个或多个区块链系统500相关联的数字钱包DWs）之间提供数据通信；以及

[0153] (d) 物体处理管理模块30，其连接至签名/标记读取模块R及通信模块70。物体处理管理模块30可以与上述类似地配置/可操作于通过实施以下操作来认证对实体物体01所实施的至少一处理操作的执行参数：

[0154] -通过确定以下两者之间的匹配来认证实体物体01的身分或类型或批次：从读取模块R获得的实体物体01的标记/签名的数据以及由参考数据60存储的一个或多个实体物体的标记/签名；

[0155] -通过确定以下两者之间的匹配来认证拥有物体签名读取器100的实体的身分：识别所述物体签名读取器100的读取器ID数据以及列在参考数据60中的所述实体的身分。

[0156] 相应地，物体处理管理模块30对处理操作进行认证。

[0157] 物体处理管理模块30还可以被配置且可操作为操作网络通信模块70以访问一个或多个区块链系统500（例如，通过区块链网络501）并证实第二分布式账本20中的已认证的处理操作的注册。因此，物体签名读取器100在证实了在第二账本20中与物体交易相关联的已认证的处理操作后，能够让与实体物体01相关联的物体交易得以记录在第一账本10中。

[0158] 最佳地,物体处理管理模块30适于授权读取模块R以读取实体物体01的标记/签名。这类的授权可以如上所述通过向读取模块R1提供指示用于读取特定物体01的标记/签名的读取参数的数据来实现。继而,读取模块可以适于操作与读取参数相对应的特定读取方案,从而确定指示特定物体01的标记/签名的数据。

[0159] 可选地,物体签名读取器100还包含条件验证器模块50,其如上所述可以适于获取指示处理操作的预定条件的数据,以及仅在验证了已认证的处理操作的执行参数符合预定条件时能够让已认证的处理操作在第二分布式账本中的注册得以证实。

[0160] 可选地,物体签名读取器100还包含如上所述的代币管理模块40,其可以连接到物体处理管理模块30或网络通信模块70,以及被配置且可操作为能够让在一个或多个区块链系统中的至少一预定代币交易上的处理操作得以认证/证实。

[0161] 可选地,物体签名读取器100被配置且可操作用于读取/认识嵌入在实体物体01中的本质XRF签名。在这样的实施例中,读取模块可以包含XRF测量模块(未具体示出),其被配置且可操作用于实施实体物体的XRF测量以读取XRF签名/标记(例如,通过用X射线或伽马射线照射所述物体的至少一部分,并检测指示所述XRF签名/标记的X射线-荧光响应,并可选地对所述响应执行光谱分析)。

[0162] 在部分例子中,物体签名读取器100还包含一个或多个传感器S,其被配置且可操作用于测量一个或多个执行条件(例如,在执行处理操作的时间中出现的如上所述的环境/周围条件、位置、时间及/或惯性条件)。这些执行条件可以与已认证的处理操作一起被注册在第二账本20中(例如,通过物体处理管理模块30),并且可以被用于验证处理操作是否满足在第一账本10中的物体交易的预定条件。

[0163] 应当注意的是,可选地,由物体签名读取器100用于认证处理操作所使用的至少一部分或是全部的参考数据60通过一个或多个区块链系统500以去中心化的分布式方式进行存储。为此,物体处理管理模块30可以适于直接地或间接地访问一个或多个区块链系统500,以提取认证物体的处理操作所需的参考数据60的至少所需部分。

[0164] 为此,将系统100配置为独立/完整的物体签名读取器100(不与任何集中化服务/服务器或模块有关联),及/或用于认证处理操作的参考数据60的存储(系统)以去中心化的分布式方式存储在区块链中,以及使用与实体物体01不可分离的本质标记/签名,共同提供了一种实际上无法伪造或仿制的健全的处理操作认证技术。此外,将已认证的处理操作注册在第二分布式账本20中,一方面可以使任何感兴趣的一方(例如,数字钱包或实体)在处理操作与物体交易相关联时访问已认证的数据,同时另一方面无法实际伪造,从而促使一种对关于实体物体的物体交易的注册所需的已认证处理操作的存在进行验证的健全方式。

[0165] 因此,图2C的系统100可以被提供给沿着供应链的各种独立实体,所述独立实体可以彼此独立地或者与任何集中式系统/实体独立地使用这种系统,以认证由此对实体物体所执行的处理操作并将所述处理操作记录在分布式账本20中。

[0166] 应当理解的是,图2C的系统100的进一步细节及实施方式可以类似于上面参考图2A的系统100所述的细节及实施方式,且可选地具有适当修改使这样的系统完整,如本领域技术人员可理解的。

[0167] 图3中示出了本发明的系统的另一实施例,其是根据本发明的用于实现智能合约

的特定实施例的系统100的总体结构的示意图。在本申请的附图中,相似的附图标记用于表示本发明的不同实施例中的相似元件模块、或系统或模块、或具有相似功能的系统。

[0168] 图3的系统100包含可类似于图1及2A的管理系统的管理系统30、可选的代币管理工具40及多个区块链系统BC1、BC2、至BCn。管理系统30与类似于图1及2A的读取器R1至Rn的多个读取器单元R1、R2、至Rn进行通信。区块链系统BC1至BCn中的每一个与类似于上述参考图1至图3的数字钱包DW1、DW2、至DWn的多个数字钱包(图3中未具体示出)交互作用。代币管理工具40与区块链系统BC1至BCn交互作用,也就是代币管理系统可以能够访问由管理系统所存储的数据及/或由管理系统30提供的服务(例如,读取被标记物体的标记所需要的)。部分或全部的区块链系统BC1至BCn还可以实现第一账本(例如,如上述的标号10),并且管理所有权的记录及对应的原生代币/货币(亦即,每个具有它的原生代币的区块链)的交易。在执行这些原生代币中的交易时可以授予对管理系统30的访问权限。例如,代币管理工具40可以响应于支付而允许访问,所述支付可以在这些原生代币(针对与每个区块链相关联的预选数字钱包制成)中的任何一个中进行。区块链系统BC1至BCn中的一个或多个也可以管理涉及被标记的物体(还有其原生代币)的记录及交易。

[0169] 本发明的系统100可以实现各种类型的智能合约,这些合约可以涉及或不涉及被标记的物体。例如,本发明的系统可以通过诸如提供通用的脚本语言的以太坊区块链之类的平台来实现。另外,通过使用代币管理工具,本发明能够涉及被标记的物体或包含从管理系统中提取数据的智能合约得以实现。

[0170] 第一种类型的操作是将被标记的物体的记录注册/创建在区块链系统上,也就是说,被标记的物体被记录为属于通过例如公钥识别的一特定当事方(一数字钱包)。这种类型的操作可以以一定数量的代币的转移为条件(亦即,所述操作需要以代币进行支付)。

[0171] 可以通过本发明的系统100实现的智能合约的一种类型是被标记的物体的所有权的改变,其条件是验证已标记的物体是通过一特定签名或代码所标记。例如,接收所有权的一方可能希望通过检查物体是否带有特定标记(例如,可以在制造过程中将这种标记施加于物体)来验证物体是真实的。

[0172] 在一示例中,对物体上的签名的读取是在一初始阶段中所实施,其中仅在识别出正确的签名时才执行智能合约。可替代地,签名可以仅在交易的最后阶段才进行读取,其中接收所有权的一方验证物体是真实的。在另一示例中,对物体上的签名进行读取的次数大于一次,例如在初始阶段(其中提取正确的签名是执行智能合约的下个步骤的条件)以及在最后阶段以完成交易。

[0173] 现在参照图4,其是根据本发明的用于实现智能合约的系统100的示意图。

[0174] 创建被标记的物体的新记录:有物体的所有权的当事方Ei(例如,物体的制造商)可能希望标记物体并在系统中创建物体的记录,也就是在管理系统中与标记对应的记录,及在区块链系统中的物体的所有权的记录。当事方Ei具有数字钱包DWi,存储在数字钱包DWi上与物体相对应的数据包含能使当事方Ei证明它对物体的所有权的的数据(例如,私钥)。此外,数字钱包DWi还可以存储与代币关联的数据,特别是证明当事方Ei拥有一定数量代币的数据。数字钱包DWi与区块链系统500进行通信。通过标记物体及使用注册的读取器(亦即,由管理系统30注册其ID的读取器)读取标记来将物体记录在系统100中。读取器与管理系统40进行通信以接收许可来实施对物体的读取以及将与标记相对应的数据传送至管理

系统30。管理系统30与区块链系统500进行通信以将与物体上的标记相对应的数据以及可选地附加数据传送至区块链系统500。例如,附加数据可以涉及被标记的物体的类型、指示读取的时间及/或位置的数据、识别当事方Ei及/或用于读取标记的特定读取器的数据等等。可选地,物体在区块链系统500中的注册可能通过从读取器到区块链系统500的信息传输所限制以提供与读取被标记物体的物体有关的数据(例如,读取的时间及位置、识别操作读取器的当事方或被标记的物体的拥有者的数据等等)。另外,在区块链系统上注册被标记物体的记录可以是将一定数量的代币转移到例如当事方Ei的前提/条件。预选的数字钱包/账户可以通过代币管理工具进行验证(例如,代币可以在物体已被注册的情况下被转移到数字钱包)。

[0175] 在转移被标记的物体的所有权时,所有权的转移可以由当事方Ei通过使用它的数字钱包DWi来证明它对物体的所有权并提供指令将所有权转让给使用数字钱包DWf的当事方Ef(例如,分销商或客户)来进行。可以仅由当事方Ef(或它的代表)通过利用与管理系统30相关联的读取器读取对物体上的标记,将指示所读取的标记的数据传达给管理系统30,以及利用管理系统30对物体上的标记进行认证,来完成这类的交易。通信可以包含其他数个步骤,例如接收进行读取的许可及/或接收读取所需的数据。

[0176] 在另一示例中,所有权的转移可以在物体由当事方Ei持有且被移交给当事方Ef之前时,通过对物体上的标记进行读取来实施。在又一示例中,转移被标记物体的所有权的交易需要在移交给当事方Ef之前(通过当事方Ei)对被标记物体进行读取以及在接收到被标记物体之后通过当事方Ef对被标记物体进行读取。

[0177] 在本发明的一方面,为了验证要在区块链系统中注册的物体有被标记并注册在管理系统30中,管理系统30仅在初始阶段与区块链系统500进行通信。一旦管理系统向区块链系统500确认物体已被标记及注册,来自管理系统30的任何附加数据都可以通过数字钱包进行传输。例如,一旦管理系统30向区块链系统500确认一物体已被标记及注册,它就可以生成与标记的物体相关联的一公共密钥或一组密钥(使用公共密钥加密及/或数字签名方案)。物体,使得管理系统30可以通过数字钱包传输数据(例如,与物体有关联的数字签名),所述数据确认所述数字钱包正在实现的交易与已注册的被标记物体有关,以及确认在所述交易需要进行读取的情况下,所述标记已被管理系统30读取并认证。

[0178] 区块链系统500可以包含两种不同类型的物体的所有权及交易的记录:被标记的物体及代币。这允许涉及第一类型同意的交易及程序的智能合约的实现是以涉及另一类型同意的交易为条件限制。例如,被标记物体的所有权的转移(从当事方Ei到当事方Ef)仅在执行将预选数量的代币从当事方Ef转移到当事方Ei的并行交易时才可以执行。也就是第一交易(转移物体的所有权)以第二交易(转移代币)为条件限制。替代地,这样的条件限制可以反过来。亦即,可以使第二交易依赖于第一交易的执行。在一第三示例中,两个交易可以被共同执行及完成。也就是这些交易没有在不执行另一交易的情况下被执行。

[0179] 这类有条件限制的交易可以通过下述操作来实现:只有当被指示为第一交易的限制条件的先前所执行的第二交易在多个交易的区块的链中被找到时,区块链系统中的节点才允许包含第一交易区块。因此,操作对交易进行证实的节点仅在验证第二交易存在于区块的链中时才证实第二交易。

[0180] 现在参照图5,其是根据本发明一实施例的用于实现用于转移被标记物体的所有

权的智能合约的方法600的流程图,其中所有权的转移以从管理系统30接收到与已标记的物体有关的信息为条件限制。

[0181] 在步骤602中,区块链系统500从代表一个当事方(当事方Ei)的数字钱包接收一请求以发起一智能合约,在所述智能合约中被标记物体的所有权将从当事方Ei转移到当事方Ef(亦即,将所有权的转移记录在即将要包含在区块链500内的新区块中),其以读取物体上出现的签名为条件限制(从而验证其真实性)。

[0182] 在步骤604中,当事方Ei的数字钱包通过与区块链系统500通信并提供所需的数据(例如,向区块链系统证明当事方Ei在公开密钥密码协议中保留一私钥的数据)来证明其对被标记物体的所有权。

[0183] 在步骤606中,对于智能合约的多个当事方的一方(当事方Ei或当事方Ef)向代币管理工具40发送请求,以访问由管理系统30管理的与被标记物体有关的特定信息。例如,这类的信息可以是指示物体上的签名的数据(例如,签名的哈希值(hash))。在另一示例中,所述信息可以通过读取单元读取的物体上的签名;在又一示例中,所述信息可以就是对读取单元读取的签名相同于管理系统30所存储的签名的确认。

[0184] 在步骤608中,当事方的一方或双方向代币管理工具40提供他们拥有一预选数量的代币的证明,所述预选数量是提供给步骤606中所请求的信息所需的数量。代币的数量是用于授权或支付提供来自管理系统30所请求的数据。

[0185] 在步骤610中,从管理系统接收所请求的数据。

[0186] 在步骤612中,区块链系统500根据从管理系统30所接收的数据,在区块链500系统内的一新区块中创建所有权从当事方Ei到当事方Ef的转移的记录。例如,仅在从管理系统30接收到由读取单元读取的被标记物体上的签名相同于管理系统30所存储的相对应的签名的确认后,新记录才可以被创建。

[0187] 根据部分实施例,本发明的系统100被配置且可操作用于管理及监督各种产品及商品(以下也称为物体)的供应链。例如,经历供应链的物体可以被标记及记录在区块链系统500中。区块链记录可以在给定时间下指定拥有所述物体的当事方。随着物体在易主的供应链中前进,附加的记录将添加到区块链500,以便将拥有权的链(亦即,拥有所述物体的所有当事方的列表)记录在从制造商到最终目的地(例如,最终客户、分销商、其他制造商)的区块链上。

[0188] 有物体的拥有权(in possession of)的当事方可能不同于有物体的所有权(own)的当事方。例如,一当事方可能已购买一产品或零件,甚至在它被制造之前,使得已经在工厂中的物体是客户而不是制造商所有的。在本发明的一个方面,区块链保存有物体的拥有权的当事方与有物体的所有权的当事方两者的记录。为此,本文所述的区块链系统500可以被认为是一个以上的账本,例如,一个账本用于记录物体的所有权,另一个账本用于记录实际拥有物体的实体的变更,以及可选地附加的账本,例如,指示物体上的标记的账本,或是指示在它们的拥有物中具有本发明的读取器单元的实体及各自读取器单元的标识符的账本。

[0189] 更新或改变以上两种类型的记录(亦即,改变所有权及改变拥有权的记录)可能需要来自管理系统30的确认或数据及/或使用读取器以便读取及证实物体上的标记。代币管理工具40可以通过针对不同交易要求的不同的代币授权/支付来区分这些类型的更新记录

(交易)。例如,仅在代币转移的并行交易(亦即,代币支付)存在时,代币管理工具40才可允许为了改变所有权而对管理系统30(及读取器)进行访问,同时允许为了改变拥有权的记录而对管理系统30进行访问。

[0190] 供应链管理系统可以利用或包含监视环境条件(例如,温度、湿度等)及/或沿着供应链前进的物体的状态(例如,在运输的期间)的传感器系统(例如,附加到产品或包装上)。由传感器获取的数据可以记录在区块链系统500中,其提供传感器数据的不可改变记录表。记录在区块链500上的传感器数据可以开放给所有当事方(或者在许可区块链的情况下至少向所有已认证当事方开放),例如,接收物体或产品的当事方E_f可以在预选时间的期间内(例如,在运输的期间)验证环境条件不超过允许的范围。另外,用于传感器数据的区块链系统500使得涉及在预选时间的期间内通过与物体有关的传感器所获取的数据的智能合约能够实现。例如,只有在环境条件中没有偏差被记录的情况下(例如,将食品或药品持续地保持在适当的温度下),所有权从一方转移到另一方的交易才可以执行。

[0191] 根据本发明的部分实施例,系统100可以通过使相关当事方(例如,E_i、E_f以及供应链中的任何介入方/实体)能够验证上传到区块链的用于产品或包装的传感器数据确实属于正确的产品,来向这类的方案提供安全性及可靠性的附加层。也就是通过读取物体上的应对应于传感器的ID的标记来创建传感器(及传感器数据)与物体(例如产品、包装或容器)之间的一一对应关系。例如,存储在传感器上的数据可以包含对应于通过系统上的标记所提供的签名的ID号。传感器的ID号以及传感器与物体签名之间的对应关系可以存储在管理系统30中。可替代地或附加地,传感器自身可以通过可利用读取器进行读取及识别的标记来进行标记。

[0192] 根据本发明的部分实施例,系统100可以仅在读取物体上的标记并获得“正确”结果时才能够让传感器数据被记录在区块链上。另外,本发明的系统可以实现智能合约,其中只有在验证了被记录的传感器数据不包含偏离预选范围的偏差以及传感器确实对应于它所附接的物体之后,才对被标记物体的所有权的改变或是拥有权的改变进行记录。

[0193] 在另一方面,本发明提供了一种用于实现智能合约的系统,其中拥有链(chain of possession)以及可选地附加条款及条件通过有特权的当事方来设置。在一示例中,有特权的当事方是物体或产品的拥有者。在其他示例中,有特权的当事方可以是物体的制造商,或者是区块链系统内的有特权的当事方(例如,被许可的区块链中的被授权方)。沿着拥有链拥有物体的当事方可以例如是参与产品供应链的各种实体,例如制造商、快递公司、装运公司、分销商及最终客户或是产品的拥有者或将来拥有者。产品的制造商(或替代地,拥有者)可以发起智能合约,其中从制造商到最终客户或一组客户(例如,来自同一地区的客户)的供应链是通过制造商进行设置。

[0194] 现在参考图6,其是根据本发明一实施例的用于实现智能合约及管理供应链的系统100的实施例的示意图。系统100包含区块链系统500或与区块链系统500相关联,以及包含管理系统30、以及可选地代币管理工具40。另外,系统100可以包含多个读取器,例如,R1及R2,如图6所示例。读取器与管理系统30及区块链系统500进行通信。图6还示出了多个当事方E_i、E₁、E₂及E_f,它们与区块链系统500及管理系统30进行通信以及进一步通过数字钱包或系统应用程序(未在图6中具体显示)来实施交易及在区块链系统500上实现智能合约。系统100使多个当事方能够实现与通过管理系统40所记录的被标记的实体资产/物体

有关的智能合约(例如,在区块链系统500上),由此智能合约也可以涉及虚拟资产,例如原生代币或加密货币。举例来说,当事方E_i可能希望通过当事方E₁及E₂将物体移交给将拥有物体的最终拥有人(当事方E_f)。在一特定示例中,当事方E_i可以是物体的制造商或最初拥有人,当事方E_f可以是物体的最终拥有人(假定购买物体的客户),其中当事方E₁可以是装运或快递公司,以及当事方E₂可能是分销商。在另一示例中,当事方E_i可能是艺术作品的拥有人,其希望将艺术作品转移给另一实体E_f(假定博物馆或画廊)进行展览。当事方E_i一方可以发起智能合约,其中物体的拥有链是根据当事方E_i的需求来设置。也就是当事方E_i可以允许仅通过特定的快递及/或装运公司,或一组已授权公司来递送物体。此外,当事方E_i可以以读取物体上的标记来限制供应链中所有或部分拥有权的改变,从而在包含读取器在内的任何拥有权的转移中,证明被授权方被授予了物体。参照图6,智能合约设置了拥有链,以及还以物体的标记的读数(分别通过读取器R₁及R₂)作为当事方E₁到当事方E₂以及从当事方E₂到当事方E_f的拥有权的改变的条件限制,而在此示例中,从当事方E_i到当事方E₁的拥有权转移并不需要获取标记的读数。物体拥有权改变的交易记录被存储在区块链500上(例如,在上述第二账本20中),以及所有权记录也被存储在区块链500上(例如,可以存储在上述第一账本10中)。智能合约还可能涉及物体的所有权的改变,所述物体的所有权的改变可能会或可能不会以标记的读数为条件限制。

[0195] 当事方E_i(或拥有物体的任何其他当事方)可以实现以各种因素(包含读取物体上的标记以外的因素)为条件限制的智能合约。拥有权(或所有权)的转移可能取决于以下条件:读取的时间及/或位置(例如,通过使用GPS进行验证)、可以利用可被传送到管理系统或区块链系统的读取器的ID进行验证的特定的读取器以及操作读取器的人员/公司、以及操作读取器的人员。在系统100的另一方面,在物体利用两种不同类型的标记(每个标记提供不同级别的有效性)进行标记的例子中,当事方E_i可以发起包含在多个当事方之间转移的拥有链的智能合约,其中部分拥有权的转移需要一种类型的读取器,而其他拥有权的转移需要使用另一种类型的读取器(提供不同级别的安全性、有效性或真实性)。在一示例中,物体可以通过对XRF敏感的标记及条形码或QR码来进行标记。智能合约可能需要读取XRF标记,其在部分拥有权的转移时提供高级别的安全性及真实性(并可能需要来自管理系统30的数据),而在其他拥有权的转移时则可能需要读取条形码及QR码。

[0196] 如上所述,系统100还可以出于各种目的利用各种类型的传感器,例如沿着供应链保持追踪及记录环境状况。智能合约也可以以传感器所记录的数据为条件限制。如果条件及智能合约的条款不满足,则区块链系统500可以拒绝更改物体的所有权或拥有权。替代地,区块链系统500可以记录所有权或拥有权的改变并将其记录为未经授权的改变。在不同的示例中,区块链可以从与无法满足智能合约条款的一方或多方相关联的账户或数字钱包中提取以区块链系统500的原生代币支付的罚款或费用给预选的数字钱包(例如,拥有人或发起智能合约的当事方的数字钱包)。

[0197] 在另一方面,根据本发明的系统100允许对物体或产品及其成分及子成分两者进行,以及对组合成单一物体/产品的成分及子成分的拥有链进行记录。也就是说,区块链500可以记录表示多个拥有链的成分及子成分(以及可能地最终产品)的拥有“树”。这例如通过上述图2A中的操作OP3所示出,其中第一物体O₁及第二物体O₂被组装在一起,由此可选地,两个物体上的标记可以被读取并进行其他认证以证实处理操作。这导致实际上(de-facto)

树被记录在区块链500中,其表示多个物体从它们的起源(最初各个实体Ei's),直到它们到达(例如,组装在一起)到最终/接收者实体Ef的位置链。

[0198] 因此,由制造商接收的组件(最终产品的或他的多个组件中的一者)可以使用所述组件,前提是所述组件已被标记以及所述标记被读取并记录在区块链上。这种对组件进行标记并将其记录在区块链系统上的方案可确保被标记的组件(或其中的一些)是“正确的”组件。此外,最终产品的制造商不仅可以确保他收到的组件是真实的,还可以确保其子组件(一直到基本组件)都是真实的且起始于正确的来源。

[0199] 根据本发明的部分实施例,系统100可以被配置且可操作用于通过在ID(例如,产品或序列号)及施加于物体或产品上的XRF标记之间创建的对应关系来实现物体及其处理交易的离线认证。关于这一点,术语“离线认证”应理解为不需要指示标记物体的标记与物体的相应识别身份(例如,不一定需要访问如上面的参考图2A所述的参考数据Obj'Data)之间的对应关系的“先”存储的参考数据的认证。因此,由于可能不需要访问参考数据,因此处理操作的认证可以离线执行。这可以通过用标记对物体进行标记来实现,所述标记的签名对应于(例如,指示)要被识别的物体或批次的ID(例如对应于产品ID或特定产品的序列号的签名)。因此,ID可以对应于单一物体或是一批物体。所述ID可以是在制造期间或制造后施加到物体上的明显标记,例如ID识别产品或序列号。ID可以是机器可读的标记,例如条形码或QR码。在另一示例中,ID可以是隐蔽的,其可以通过适当的手段或在适当的条件下来识别。XRF标记施加于对应于ID的物体。也就是说,包含在标记中的材料及元素是根据编码系统来将标记材料的数量及/或浓度,以及可能地影响XRF响应光谱的附加因素(例如,物体中存在的材料、包含激发响应信号的初级辐射的能量的测量条件、以及源-物体-检测器的几何形状(source-object-detector geometry))转化成表示物体的ID的签名的代码(例如,二进制码)。签名是ID的函数,例如,ID的哈希函数或加密哈希函数。XRF标记可以通过计量机(dosing machine)来配制。XRF标记可以通过包含打印、压印、喷涂、注射、刷涂及喷枪的各种技术施加于物体。

[0200] XRF标记可以利用以引用方式并入本文的国际专利申请公开号PCT/IL2018/050527中所描述的类型标记装置施加或配置在物体上。

[0201] ID及XRF标记之间的对应关系可以添加一个附加的认证及防伪层,因为对物体的ID的任何改变或篡改尝试可以通过读取物体上的XRF标记来检测。

[0202] 此外,由于对应关系允许离线认证,它可以用在供应链管理方案中(例如,在图6的实施例的方案中)。例如,系统100可以实现智能合约,其中拥有链是通过发起智能合约的当事方进行设置的。两个当事方之间的所有权的转移可以在所有权转移发生之前先读取标记的情况下脱机实施。换句话说,标记是在读取器与区块链系统500及/或与管理系统30之间没有连接的情况下进行读取,但在XRF标记被读取及被发现与物体上的ID相对应的条件下,一旦建立连接后,转移则被记录在区块链系统中。这种类型的离线认证可能需要来自代币管理系统40的授权。

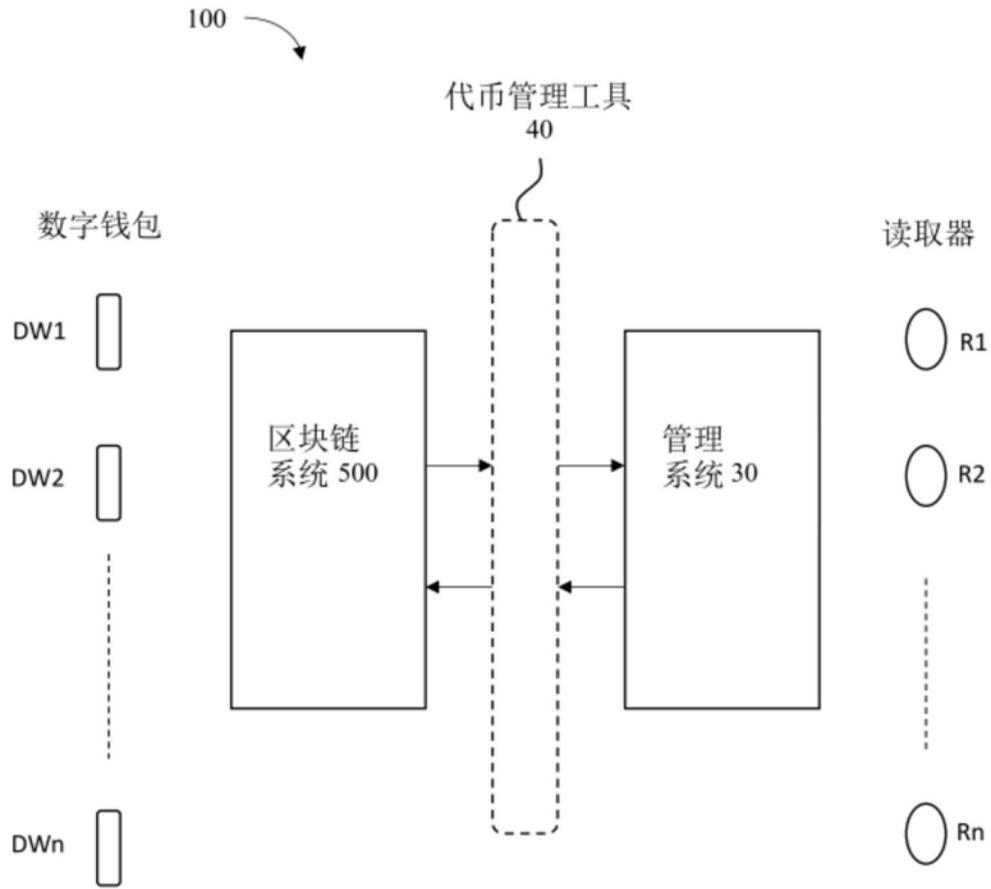


图1

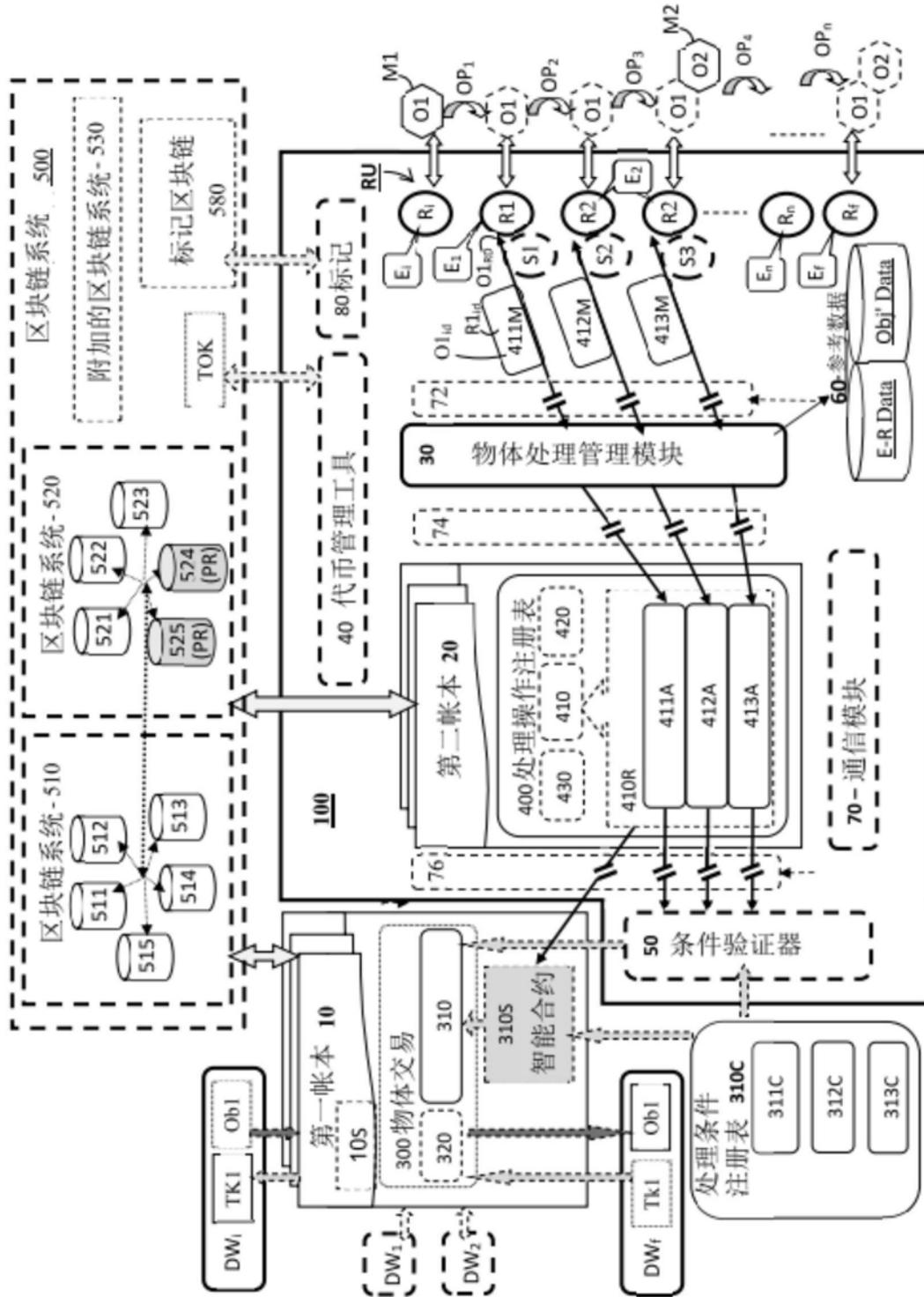


图2A

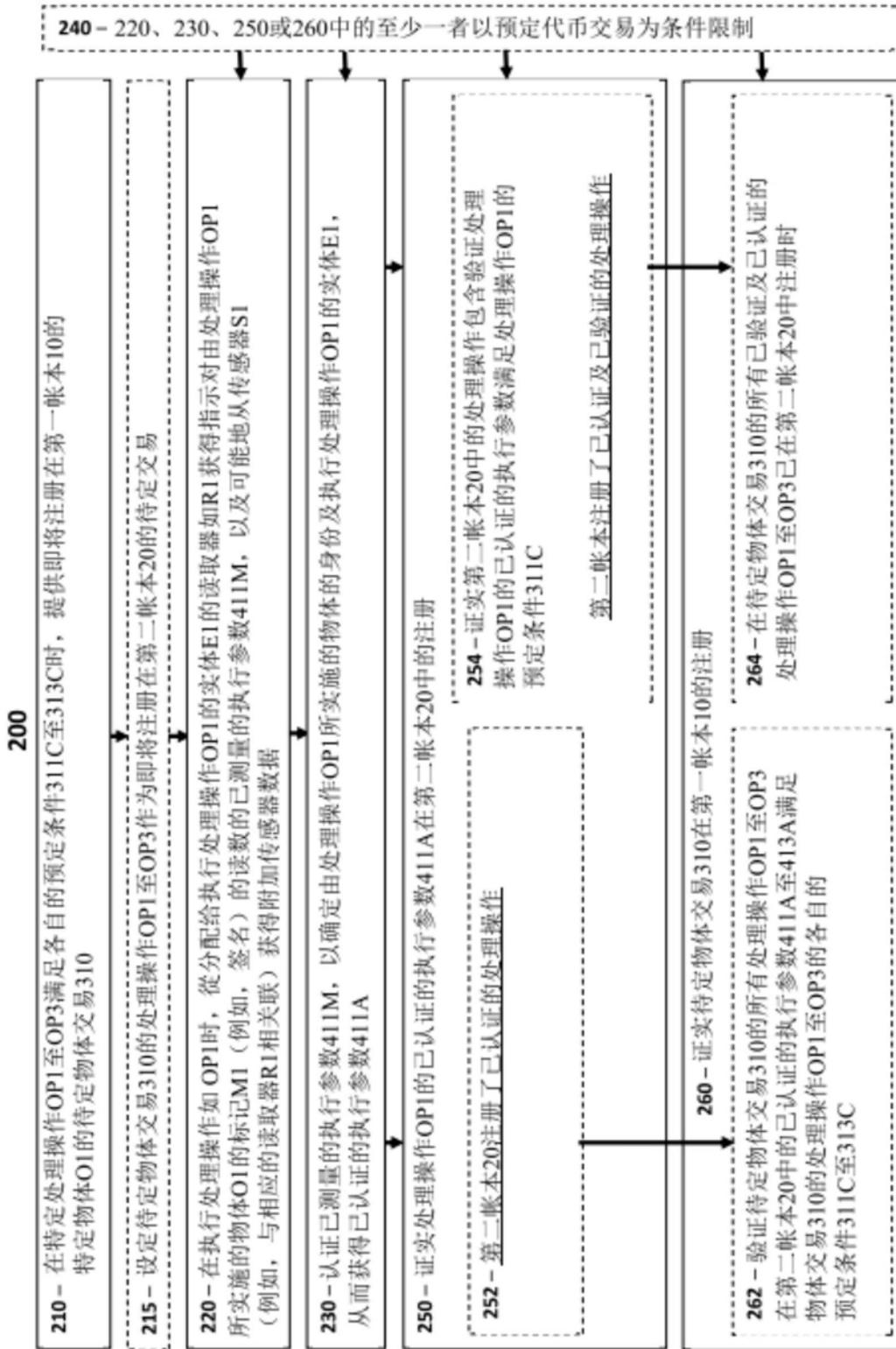


图2B

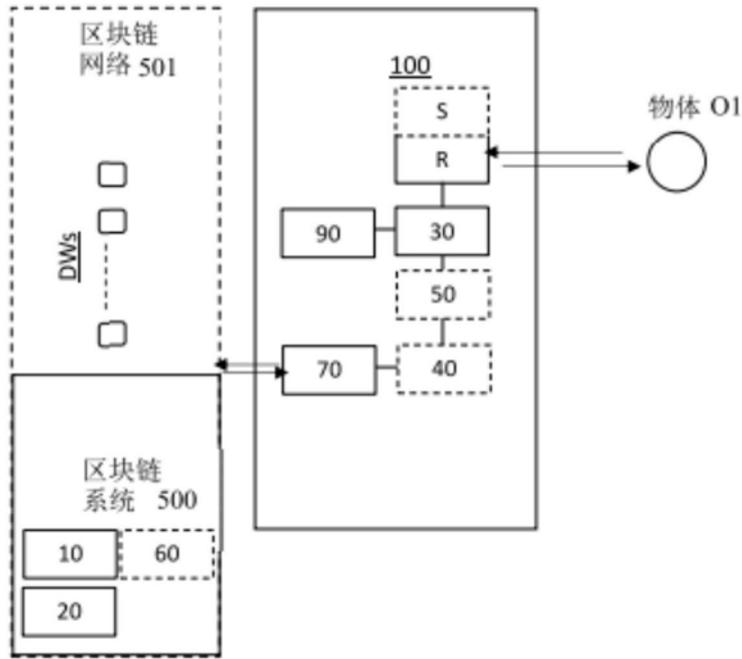


图2C

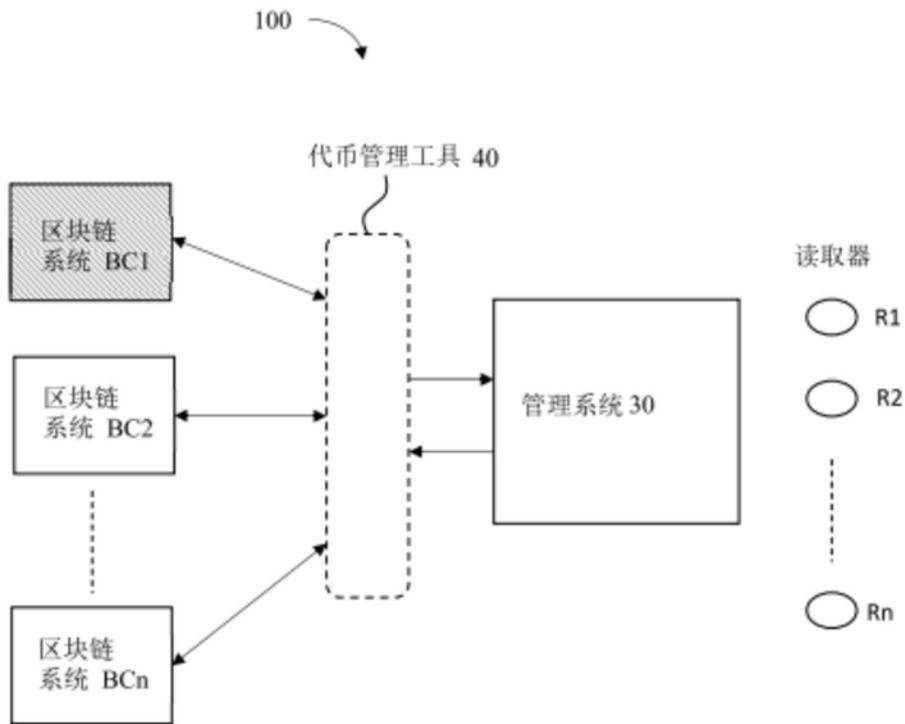


图3

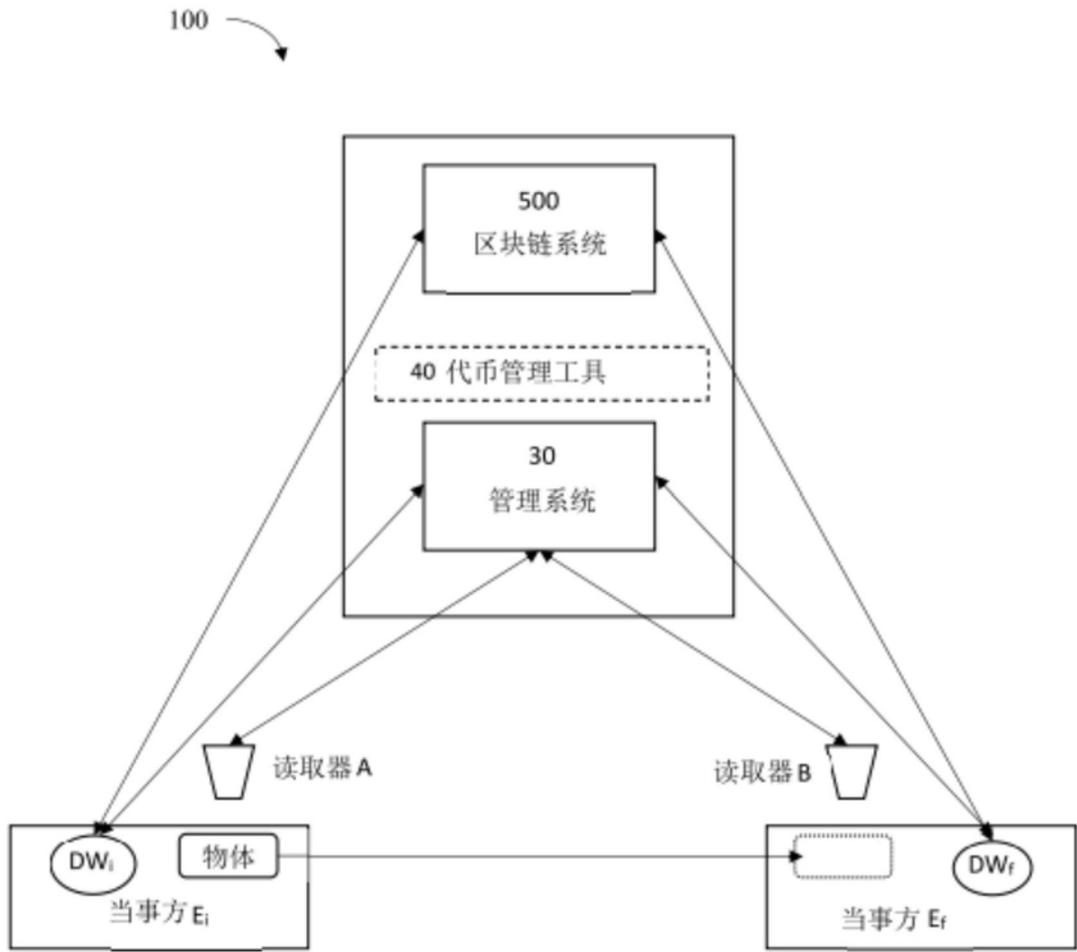


图4

600

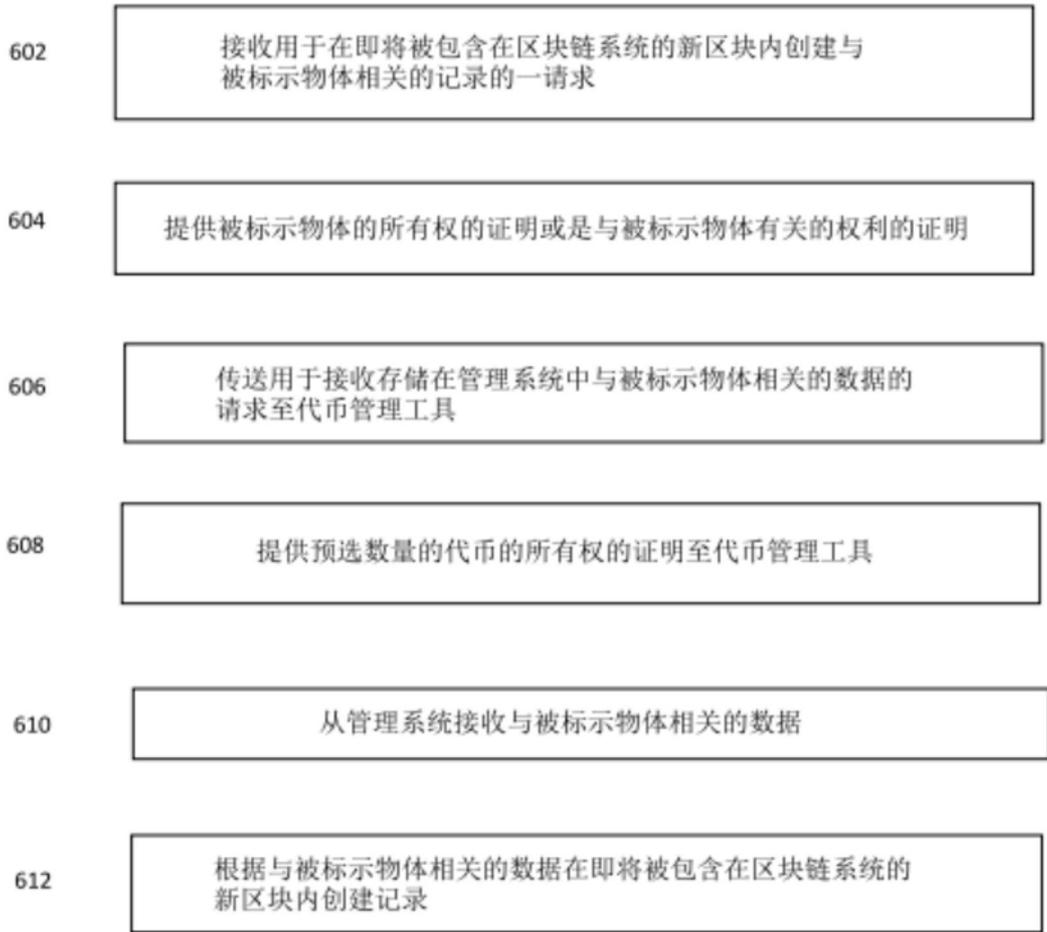


图5

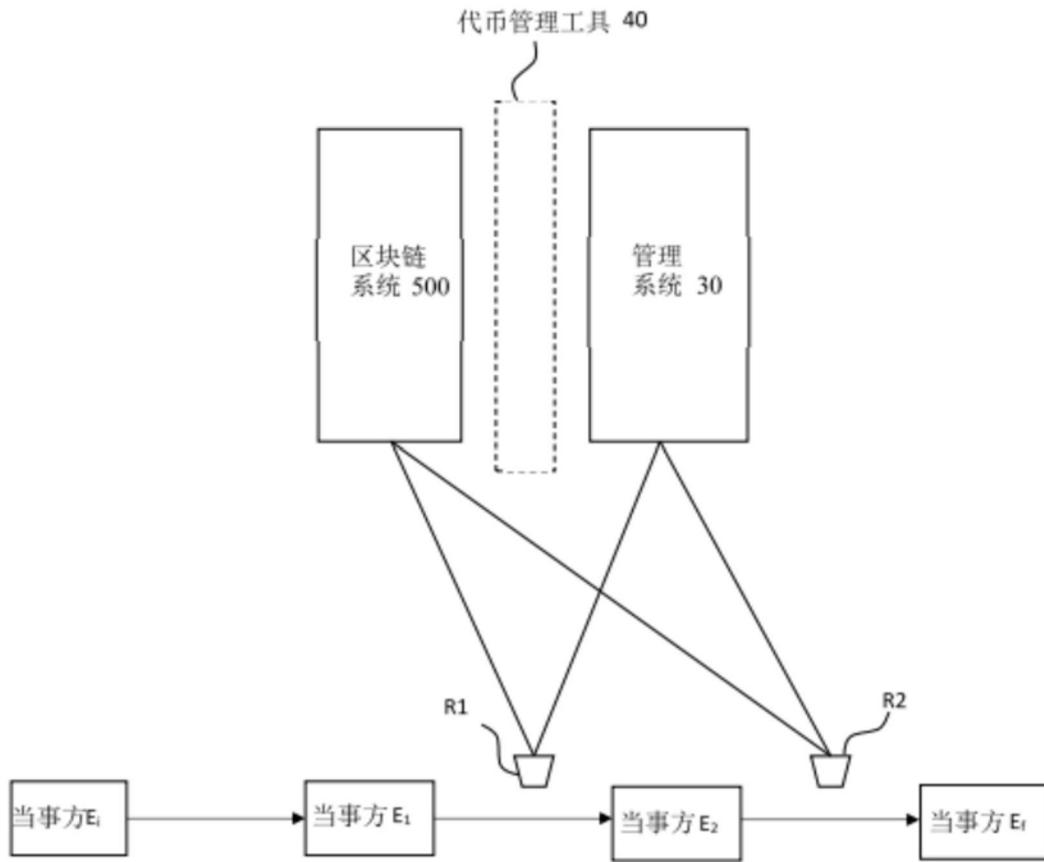


图6