(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 2 月 25 日 (25.02.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/032192 A1

(51) 国际专利分类号:
G06F 21/64 (2013.01) *G06Q 40/04* (2012.01)

(21) 国际申请号: PCT/CN2020/110512

(22) 国际申请日: 2020 年 8 月 21 日 (21.08.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910772491.4 2019年8月21日 (21.08.2019) CN

(71) 申请人: 杭州趣链科技有限公司 (HANGZHOU QULIAN TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市滨江区丹枫路399号2号楼A楼2001室, Zhejiang 310051 (CN)。

(72) 发明人: 邱炜伟(QIU, Weiwei); 中国浙江省杭州市滨江区丹枫路399号2号楼A楼2001室, Zhejiang 310051 (CN)。 李伟(LI, Wei); 中国浙江省杭州市滨江区丹枫路399号2号楼A楼2001室, Zhejiang 310051 (CN)。 蔡亮(CAI, Liang); 中国浙江省杭州市滨江区丹枫路399号2号楼A楼2001室, Zhejiang 310051 (CN)。 张帅(ZHANG, Shuai); 中国浙江省杭州市滨江区丹枫路399号2号楼A楼2001室, Zhejiang 310051 (CN)。 匡立中(KUANG, Lizhong); 中国浙江省杭州市滨江区丹枫路399号2号楼A楼2001室, Zhejiang 310051 (CN)。

(74) 代理人: 杭州华进联浙知识产权代理有限公司 (HANGZHOU HUAJIN LIANZHE INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国浙江省杭

WO 2021/032192 A1

(54) **Title:** FORMAT VERIFICATION METHOD AND SYSTEM FOR CERTIFICATE-STORING SMART CONTRACT, COMPUTER EQUIPMENT AND READABLE STORAGE MEDIUM

(54) **发明名称:** 存证智能合约的形式验证方法、系统、计算机设备和可读存储介质

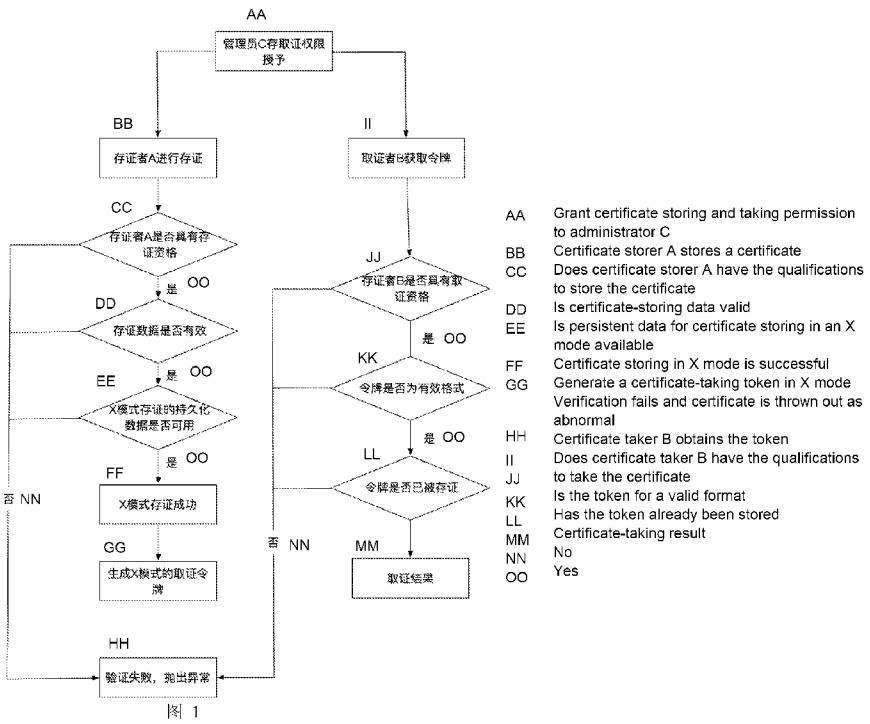

图 1

(57) **Abstract:** A format verification method and system for a certificate-storing smart contract, a computer equipment and a readable storage medium. The method comprises: obtaining a certificate-storing smart contract, adding a contract format and specifications, and verifying a contract model. The method provides a blockchain smart contract developer with a format verification method for a certificate-storing smart contract, and provides a secure reference for a blockchain on which certificate-storing items for smart contract

[见续页]

州市滨江区滨盛路1508号海亮大厦2104-2105室, Zhejiang 310051 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

developing are loaded. By means of the format verification method, the format and specifications are defined at the front part of the method body of the certificate-storing smart contract, and are converted into a mathematical model that can be recognized by a theorem prover, and the format verification result is obtained by using mathematical deductions, which improves the security and reliability of the certificate-storing smart contract, reduces testing costs for traditional contract testing, and has a wide logical coverage area. The described method is versatile with regard to certificate-storing smart contracts, provides the most basic certificate-storing contract model and format verification method therefor, provides relevant reference for the expansion and optimization of the certificate-storing contract, and has good applicability.

(57) 摘要：一种存证智能合约的形式验证方法、系统、计算机设备和可读存储介质，该方法包括获取存证智能合约、添加合约形式规范并进行合约模型验证。该方法为区块链智能合约开发者提供了存证智能合约的形式验证方法，为区块链搭载智能合约开发存证项目提供了安全方面的参考。通过形式验证的方法，在存证智能合约方法体前部定义形式规范，转化为定理证明器能够识别的数学模型，利用数学推演得出形式验证结果，提高了存证智能合约的安全性和可靠性，降低了传统合约测试的测试成本，逻辑覆盖面广。上述方法具有针对存证智能合约的通用性，提供了最基本的存证合约模型及其形式验证方法，为存证合约的扩展和优化提供了相关参考，具有很好的适用性。

存证智能合约的形式验证方法、系统、计算机设备和可读存储介质

相关申请

[001] 本申请要求 2019 年 8 月 21 日申请的，申请号为 201910772491.4，发明名称为“一种基于区块链存证智能合约的形式验证方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[002] 本申请涉及智能合约和形式验证技术领域，特别是涉及一种存证智能合约的形式验证方法、系统、计算机设备和可读存储介质。

背景技术

[003] 区块链是一种基于数据加密、时间戳、分布式共识机制实现去中心化的分布式数据管理技术，具有可追溯、不可篡改、高可用的特点。智能合约作为一套以数字形式定义的承诺，承诺控制着数字资产并包含了合约参与者约定的权利和义务，由计算机系统自动执行。区块链技术的出现为智能合约提供了一套能够支持可编程的数字系统。形式验证是目前智能合约安全审计方案中行之有效的方法，其通过数学逻辑将功能描述与实际代码进行比较，从而检查代码是否符合预期结果。存证智能合约作为常见的合约应用领域，通过形式验证审计其安全性是存证结果真实可信、可追溯的前提。但是目前智能合约开发社区并没有针对存证业务相应的安全规范，使得开发存证智能合约容易出现安全漏洞，需要一套针对存证智能合约的开发流程规范以及基于形式验证的存证智能合约模板，为存证智能合约的设计和开发提供安全方面的重要参考。

发明内容

[004] 根据本申请的各种实施例，提供一种基于区块链存证智能合约的形式验证方法，所述方法包括以下步骤：（1）编写存证智能合约，根据不同生产环境和权限进行存证、取证、存取证权限授予。

[005] （2）添加合约形式规范：将步骤（1）所述存证智能合约添加用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移、不变量的形式验证的规范语句。

[006] （3）合约模型验证：对添加形式验证规范后的智能合约进行模型验证并得出验证结

果，若符合所述形式验证规范则形式验证通过，若不符合所述形式验证规范则定位所述形式验证不满足的语句位置以及具体的存证证智能合约位置。

[007] 在其中一个实施例中，步骤（1）所述存证智能合约满足以下条件：

（a）存证人、取证人、管理员的数据结构：利用映射类型的持久化变量来记录存证、取证人的身份信息，利用数组类型的持久化变量来记录管理员的身份信息；

（b）存储存证信息的数据结构：利用多组映射类型的持久化变量来记录符合多种存证模式下的存证信息；

（c）权限控制：利用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

[008] 在其中一个实施例中，步骤（2）所述合约形式规范的添加包括：

（a）合约方法添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变；

（b）合约方法传入、传出参数的形式校验，规范要求对函数传入的参数进行格式校验，对函数传出的参数进行期望校验；

（c）合约方法对持久化数据状态转移的规范说明，规范要求在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

[009] 在其中一个实施例中，步骤（3）所述合约模型验证是利用定理证明器对编写所述形式规范的智能合约进行定理证明，并给出形式验证的结果。

[010] 与现有技术相比，本申请的有益效果如下：本申请是基于区块链存证智能合约的形式验证方法，为区块链智能合约开发者提供了编写存证智能合约的流程和形式验证方法，为区块链搭载智能合约开发存证项目提供了安全方面的参考。本申请通过形式验证的方法，在存证智能合约方法体前部定义形式规范，转化为定理证明器能够识别的数学模型，利用数学推演得出形式验证结果，提高了存证智能合约的安全性和可靠性，降低了传统合约测试的测试成本，逻辑覆盖面广。本方法具有编写存证智能合约的通用性，提供了最基本的存证合约模型及其形式验证方法，为存证合约的扩展和优化提供了相关参考，具有很好的适用性。

[011] 根据本申请的各种实施例，还提供一种存证智能合约的形式验证方法，所述方法包括以下步骤：

获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予；

对所述存证智能合约添加形式规范的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证；

对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置。

[012] 在其中一个实施例中，所述获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予包括以下步骤：

采用映射类型的持久化变量记录存证人和取证人的身份信息，采用数组类型的持久化变量记录管理员的身份信息；

采用多组映射类型的持久化变量记录符合多种存证模式下的存证信息；

采用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

[013] 在其中一个实施例中，所述对所述存证智能合约添加形式规范的规范语句包括以下步骤：

添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变；

添加传入、传出参数的形式校验，包括：对所述智能合约函数传入的参数进行格式校验，对函数传出的参数进行期望校验；

添加对持久化数据状态转移的规范说明，包括：在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

[014] 在其中一个实施例中，所述对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果包括以下步骤：

采用定理证明器对所述添加形式验证的规范语句后的智能合约进行定理证明，并给出形式验证的结果。

[015] 根据本申请的各种实施例，还提供一种存证智能合约的形式验证系统，所述系统包括：合约获取模块、规范添加模块和形式验证模块。

[016] 所述合约获取模块用于获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予。

[017] 所述规范添加模块用于对所述存证智能合约添加形式验证的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证。

[018] 所述形式验证模块用于对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置。

[019] 在其中一个实施例中，所述合约获取模块还用于采用映射类型的持久化变量记录存证人和取证人的身份信息，采用数组类型的持久化变量记录管理员的身份信息；采用多组映射类型的持久化变量记录符合多种存证模式下的存证信息；采用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

[020] 在其中一个实施例中，所述规范添加模块还用于添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变。

[021] 所述规范添加模块还用于添加传入、传出参数的形式校验，包括：对所述智能合约函数传入的参数进行格式校验，对函数传出的参数进行期望校验。

[022] 所述规范添加模块还用于添加对持久化数据状态转移的规范说明，包括：在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

[023] 在其中一个实施例中，所述形式验证模块还用于采用定理证明器对所述添加形式验证的规范语句后的智能合约进行定理证明，并给出形式验证的结果。

[024] 根据本申请的各种实施例，还提供一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述存证智能合约的形式验证方法的步骤。

[025] 根据本申请的各种实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述存证智能合约的形式验证方法的步骤。

附图说明

[026] 为了更好地描述和说明这里公开的那些发明的实施例和/或示例，可以参考一幅或多幅附图。用于描述附图的附加细节或示例不应当被认为是对所公开的发明、目前描述的实施例和/或示例以及目前理解的这些发明的最佳模式中的任何一者的范围的限制。

[027] 图 1 是本申请实施例的基于区块链存证智能合约形式验证的流程图。

[028] 图 2 是本申请实施例的存证智能合约的形式验证方法的流程图。

[029] 图 3 是本申请实施例的存证智能合约的形式验证系统的结构示意图。

[030] 图 4 是本申请实施例的计算机设备的内部结构图。

具体实施方式

[031] 为了便于理解本申请，为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图对本申请的具体实施方式做详细的说明。在下面的描述中阐述了很多具体细节以便于充分理解本申请，附图中给出了本申请的较佳实施方式。但是，本申请可以以许多不同的形式来实现，并不限于本文所描述的实施方式。相反地，提供这些实施方式的目的是使对本申请的公开内容理解的更加透彻全面。本申请能够以很多不同于在此描述的其它方式来实施，本领域技术人员可以在不违背本申请内涵的情况下做类似改进，因此本申请不受下面公开的具体实施例的限制。

[032] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本申请的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。在本申请的描述中，“若干”的含义是至少一个，例如一个，两个等，除非另有明确具体的限定。

[033] 除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同。本文中所使用的术语只是为了描述具体的实施方式的目的，不是旨在于限制本申请。本文所使用的术语“及／或”包括一个或多个相关的所列项目的任意的和所有的组合。

[034] 图 1 为一实施例提供的基于区块链存证智能合约形式验证的流程图，如图 1 所示，基于区块链存证智能合约形式验证的流程如下：

（1）编写存证智能合约：根据特定生产环境和权限进行存证、取证、存取证权限授予，需要规范合约方法的访问权限，可以通过在方法头部添加修饰器的方式限定方法的访问权限。限定函数调用者的身份，可以提高系统整体的安全性和可靠性。存证功能是面向具有存证权限的用户，用户可以根据存证类型选择对应的存证函数，将存证数据持久化至区块链节点上，存证数据不可篡改且可追溯，管理员授予存证者存证权限模块，存证者得到管理员的存证允许后才可以进行存证操作，形式规范应描述，管理员应是管理员持久化数据中的一员，存证人信息将被记录到存证人信息的持久化数据中，其他持久化变量均不发生改变。取证函数是面向具有取证权限的用户，用户可以持有取证令牌进行取证，取证函数返回取证结果，管理员授予取证者取证权限模块，取证者得到管理员的取证允许后才可以进行取证操作，形式规范应描述，管理员应是管理员持久化数据中的一员，取证人信息将被记录到取证人信息的持

久化数据中，其他持久化变量均不发生改变。存取证权限授予是面向最高权限的管理员，管理员可以对存证、取证的人员进行权限管理。

[035] 所述存证智能合约满足以下条件：

（a）存证人、取证人、管理员的数据结构：利用映射类型的持久化变量来记录存证、取证人的身份信息，利用数组类型的持久化变量来记录管理员的身份信息；

（b）存储存证信息的数据结构：利用多组映射类型的持久化变量来记录符合多种存证模式下的存证信息；

（c）权限控制：编码生成持久化变量和合约方法，需要为合约方法添加形式规范，利用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

[036] （2）添加合约形式规范：将步骤（1）所述存证智能合约添加用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移、不变量的形式验证的规范语句。所述形式规范语句必须能够清晰、无歧义地描述方法的期望运作流程，保证形式验证结果的正确性。

[037] 所述合约形式规范的添加包括：

（a）合约方法添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变；

（b）合约方法传入、传出参数的形式校验，规范要求对函数传入的参数进行格式校验，对函数传出的参数进行期望校验；

（c）合约方法对持久化数据状态转移的规范说明，规范要求在各种类型的存证方法中，明确存证的映射类型持久化变量得到了存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

[038] （3）合约模型验证：对添加形式验证规范后的智能合约模型验证是指利用定理证明器对编写所述形式规范的智能合约进行定理证明，并得出验证结果，若符合所述形式规范则形式验证通过，若不符合所述形式规范则定位所述形式验证不满足的语句位置以及具体的合约代码位置。

[039] 对于存证者存证模块，存证者选择合适的存证模式进行区块链存证，需要满足以下条件才能存证成功：形式规范应描述，存证者具有存证的资格，否则抛出异常，形式验证不通过；存证的数据是该存证模式下的有效参数，否则抛出异常，形式验证不通过；在特定存证模式下的存证结果持久化变量是可用的，否则抛出异常，形式验证不通过；存证成功后函数

返回取证令牌符合的格式要求，否则形式验证不通过；存证过程中，存证结果将被记录到存证结果的持久化变量中，其他持久化变量均不发生改变。

[040] 对于取证者取证模块，取证者进行区块链取证，需要满足以下条件才能取证成功：形式规范应描述，取证者具有取证的资格，否则抛出异常，形式验证不通过；取证者令牌格式符合格式要求，否则抛出异常，形式验证不通过；取证令牌存在于存证的持久化变量中，否则抛出异常，形式验证不通过；取证的结果是对应取证令牌的存证结果，否则形式验证不通过；取证过程中，所有的持久化变量都不发生改变。

[041] 进一步的，针对存证智能合约，如图 2 所示，可以采用以下方案实现形式验证：

S110：获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予；

S120：对所述存证智能合约添加形式规范的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证；

S130：对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置。

[042] 在本实施例中，为区块链智能合约开发者提供了对存证智能合约进行形式验证的方法，为区块链搭载智能合约开发存证项目提供了安全方面的参考。在存证智能合约方法体前部定义形式规范，转化为定理证明器能够识别的数学模型，利用数学推演得出形式验证结果，提高了存证智能合约的安全性和可靠性，降低了传统合约测试的测试成本，逻辑覆盖面广。提供了最基本的存证合约模型及其形式验证方法，为存证合约的扩展和优化提供了相关参考，具有很好的适用性。

[043] 在一个实施例中，所述获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予包括以下步骤：

采用映射类型的持久化变量记录存证人和取证人的身份信息，采用数组类型的持久化变量记录管理员的身份信息；

采用多组映射类型的持久化变量记录符合多种存证模式下的存证信息；

采用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

[044] 在本实施例中，需要规范合约方法的访问权限，可以通过在方法头部添加修饰器的方式限定方法的访问权限。限定函数调用者的身份，可以提高系统整体的安全性和可靠性。存证功能是面向具有存证权限的用户，用户可以根据存证类型选择对应的存证函数，将存证数据持久化至区块链节点上，存证数据不可篡改且可追溯，管理员授予存证者存证权限模块，存证者得到管理员的存证允许后才可以进行存证操作，形式规范应描述，管理员应是管理员

持久化数据中的一员，存证人信息将被记录到存证人信息的持久化数据中，其他持久化变量均不发生改变。取证函数是面向具有取证权限的用户，用户可以持有取证令牌进行取证，取证函数返回取证结果，管理员授予取证者取证权限模块，取证者得到管理员的取证允许后才可以进行取证操作，形式规范应描述，管理员应是管理员持久化数据中的一员，取证人信息将被记录到取证人信息的持久化数据中，其他持久化变量均不发生改变。存取证权限授予是面向最高权限的管理员，管理员可以对存证、取证的人员进行权限管理。

[045] 在一个实施例中，所述对所述存证智能合约添加形式规范的规范语句包括以下步骤：

添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变；

添加传入、传出参数的形式校验，包括：对所述智能合约函数传入的参数进行格式校验，对函数传出的参数进行期望校验；

添加对持久化数据状态转移的规范说明，包括：在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

[046] 具体的，对于存证者存证模块，存证者选择合适的存证模式进行区块链存证，需要满足以下条件才能存证成功：形式规范应描述，存证者具有存证的资格，否则抛出异常，形式验证不通过；存证的数据是该存证模式下的有效参数，否则抛出异常，形式验证不通过；在特定存证模式下的存证结果持久化变量是可用的，否则抛出异常，形式验证不通过；存证成功后函数返回取证令牌符合的格式要求，否则形式验证不通过；存证过程中，存证结果将被记录到存证结果的持久化变量中，其他持久化变量均不发生改变。

[047] 对于取证者取证模块，取证者进行区块链取证，需要满足以下条件才能取证成功：形式规范应描述，取证者具有取证的资格，否则抛出异常，形式验证不通过；取证者令牌格式符合格式要求，否则抛出异常，形式验证不通过；取证令牌存在于存证的持久化变量中，否则抛出异常，形式验证不通过；取证的结果是对应取证令牌的存证结果，否则形式验证不通过；取证过程中，所有的持久化变量都不发生改变。

[048] 在一个实施例中，所述对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果包括以下步骤：

采用定理证明器对所述添加形式验证的规范语句后的智能合约进行定理证明，并给出形式验证的结果。

[049] 在一个实施例中，如图 3 所示，提供了一种存证智能合约的形式验证系统，包括：合

约获取模块 210、规范添加模块 220 和形式验证模块 230。

[050] 所述合约获取模块 210 用于获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予。

[051] 所述规范添加模块 220 用于对所述存证智能合约添加形式验证的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证。

[052] 所述形式验证模块 230 用于对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置。

[053] 在一个实施例中，所述合约获取模块 210 还用于采用映射类型的持久化变量记录存证人和取证人的身份信息，采用数组类型的持久化变量记录管理员的身份信息；采用多组映射类型的持久化变量记录符合多种存证模式下的存证信息；采用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

[054] 在一个实施例中，所述规范添加模块 220 还用于添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变。

[055] 所述规范添加模块 220 还用于添加传入、传出参数的形式校验，包括：对所述智能合约函数传入的参数进行格式校验，对函数传出的参数进行期望校验。

[056] 所述规范添加模块 220 还用于添加对持久化数据状态转移的规范说明，包括：在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

[057] 在一个实施例中，所述形式验证模块 230 还用于采用定理证明器对所述添加形式验证的规范语句后的智能合约进行定理证明，并给出形式验证的结果。

[058] 关于存证智能合约的形式验证系统的具体限定可以参见上文中对于存证智能合约的形式验证方法的限定，在此不再赘述。上述存证智能合约的形式验证系统中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[059] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是终端，其内部结构图

可以如图 4 所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口、显示屏和输入装置。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种存证智能合约的形式验证方法。该计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏，该计算机设备的输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

[060] 本领域技术人员可以理解，图 4 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[061] 在一个实施例中，提供了一种计算机设备，包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现上述存证智能合约的形式验证方法的步骤。

[062] 在一个实施例中，提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时实现上述存证智能合约的形式验证方法的步骤。

[063] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器（ROM）、可编程 ROM（PROM）、电可编程 ROM（EPROM）、电可擦除可编程 ROM（EEPROM）或闪存。易失性存储器可包括随机存取存储器（RAM）或者外部高速缓冲存储器。作为说明而非局限，RAM 以多种形式可得，诸如静态 RAM（SRAM）、动态 RAM（DRAM）、同步 DRAM（SDRAM）、双数据率 SDRAM（DDRSDRAM）、增强型 SDRAM（ESDRAM）、同步链路（Synchlink） DRAM（SLDRAM）、存储器总线（Rambus）直接 RAM（RDRAM）、直接存储器总线动态 RAM（DRDRAM）、以及存储器总线动态 RAM（RDRAM）等。

[064] 以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[065] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在

不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

权利要求

1、一种存证智能合约的形式验证方法，其特征在于，所述方法包括以下步骤：

获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予；

对所述存证智能合约添加形式规范的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证；

对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置。

2、根据权利要求 1 所述的存证智能合约的形式验证方法，其特征在于，所述获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予包括以下步骤：

采用映射类型的持久化变量记录存证人和取证人的身份信息，采用数组类型的持久化变量记录管理员的身份信息；

采用多组映射类型的持久化变量记录符合多种存证模式下的存证信息；

采用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

3、根据权利要求 1 所述的存证智能合约的形式验证方法，其特征在于，所述对所述存证智能合约添加形式规范的规范语句包括以下步骤：

添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变；

添加传入、传出参数的形式校验，包括：对所述智能合约函数传入的参数进行格式校验，对函数传出的参数进行期望校验；

添加对持久化数据状态转移的规范说明，包括：在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

4、根据权利要求 1 所述的存证智能合约的形式验证方法，其特征在于，所述对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果包括以下步骤：

采用定理证明器对所述添加形式验证的规范语句后的智能合约进行定理证明，并给出形式验证的结果。

5、一种存证智能合约的形式验证系统，其特征在于，所述系统包括合约获取模块、规范添加模块和形式验证模块；

所述合约获取模块用于获取存证智能合约，根据不同生产环境和权限进行存证、取证和

存取证权限授予；

所述规范添加模块用于对所述存证智能合约添加形式验证的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证；

所述形式验证模块用于对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置。

6、一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求 1 至 4 中任意一项所述存证智能合约的形式验证方法的步骤。

7、一种可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求 1 至 4 中任意一项所述存证智能合约的形式验证方法的步骤。

8、一种基于区块链存证智能合约的形式验证方法，其特征在于，所述方法具体包括以下步骤：

（1）编写存证智能合约，根据不同生产环境和权限进行存证、取证、存取证权限授予；

（2）添加合约形式规范：将步骤（1）所述存证智能合约添加用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移、不变量的形式验证的规范语句；

（3）合约模型验证：对添加形式验证规范后的智能合约进行模型验证并得出验证结果，若符合所述形式验证规范则形式验证通过，若不符合所述形式验证规范则定位所述形式验证不满足的语句位置以及具体的存证证智能合约位置。

9、根据权利要求 8 所述的形式验证方法，其特征在于，步骤（1）所述存证智能合约满足以下条件：

（a）存证人、取证人、管理员的数据结构：利用映射类型的持久化变量来记录存证、取证人的身份信息，利用数组类型的持久化变量来记录管理员的身份信息；

（b）存储存证信息的数据结构：利用多组映射类型的持久化变量来记录符合多种存证模式下的存证信息；

（c）权限控制：利用修饰器对涉及所述存证、取证、存取证权限授予的方法进行权限控制。

10、根据权利要求 8 所述的形式验证方法，其特征在于，步骤（2）所述合约形式规范的添加包括：

（a）合约方法添加异常捕捉规范，包括：存证场景下规范要求发生异常的充分必要条件是存证人没有存证资格且存证数据无效；取证场景下规范要求发生异常的充分必要条件是取

证人没有取证资格且取证令牌不存在；在发生异常的情况下，所有所述持久化变量不能被改变；

（b）合约方法传入、传出参数的形式校验，规范要求对函数传入的参数进行格式校验，对函数传出的参数进行期望校验；

（c）合约方法对持久化数据状态转移的规范说明，规范要求在各种类型的存证方法中，明确存证的映射类型持久化变量得到存证数据的追加；在取证方法中，明确所有的持久化变量不被改变；在存取证权限授予方法中，明确存取证人信息表数据的改变。

11、根据权利要求 8 所述形式验证方法，其特征在于，步骤（3）所述合约模型验证是利用定理证明器对编写所述形式规范的智能合约进行定理证明，并给出形式验证的结果。

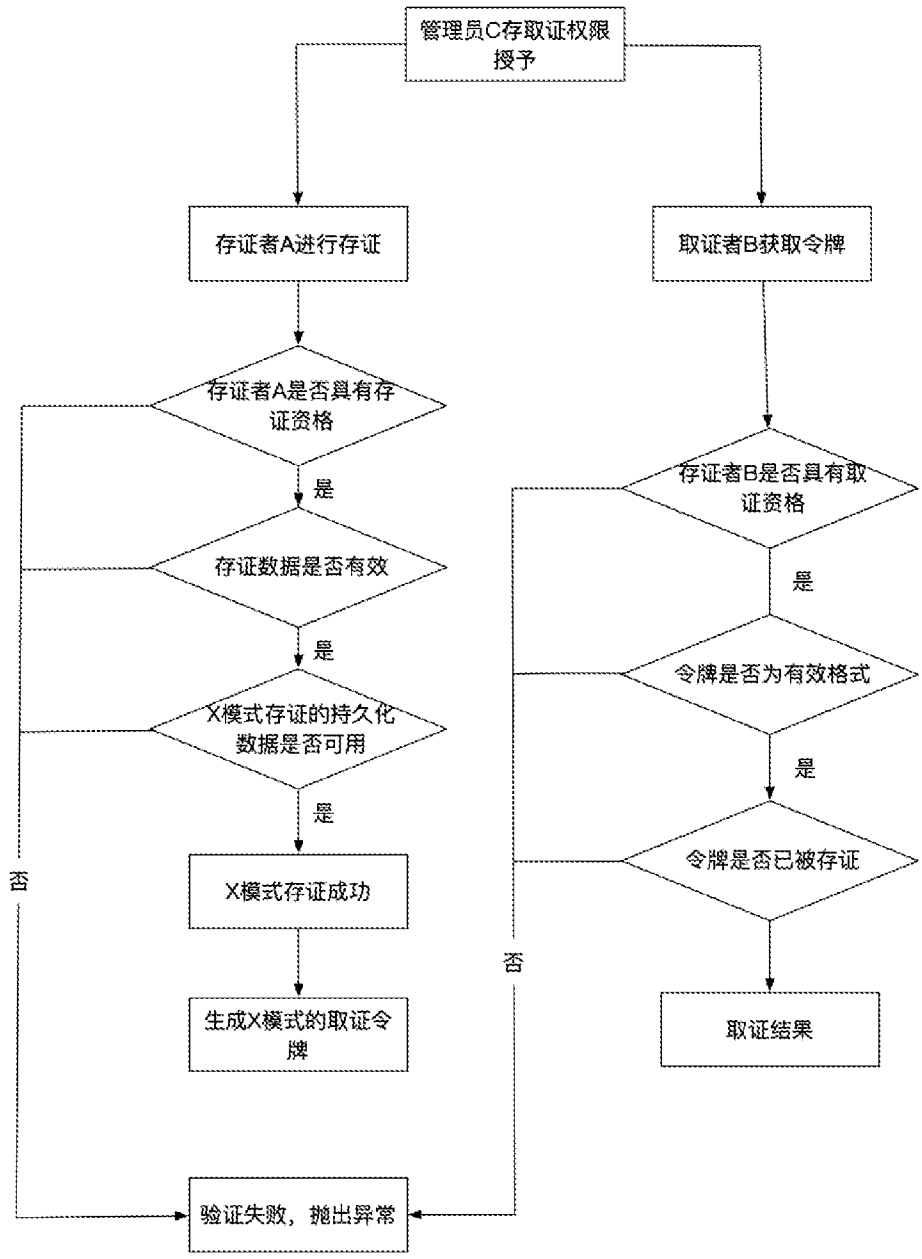
管理员C存取证权限授予
存证者A进行存证
取证者B获取令牌
存证者A是否具有存证资格
是
存证数据是否有效
是
X模式存证的持久化数据是否可用
是
否
X模式存证成功
生成X模式的取证令牌
存证者B是否具有取证资格
是
令牌是否为有效格式
是
令牌是否已被存证
否
取证结果
验证失败，抛出异常

图 1

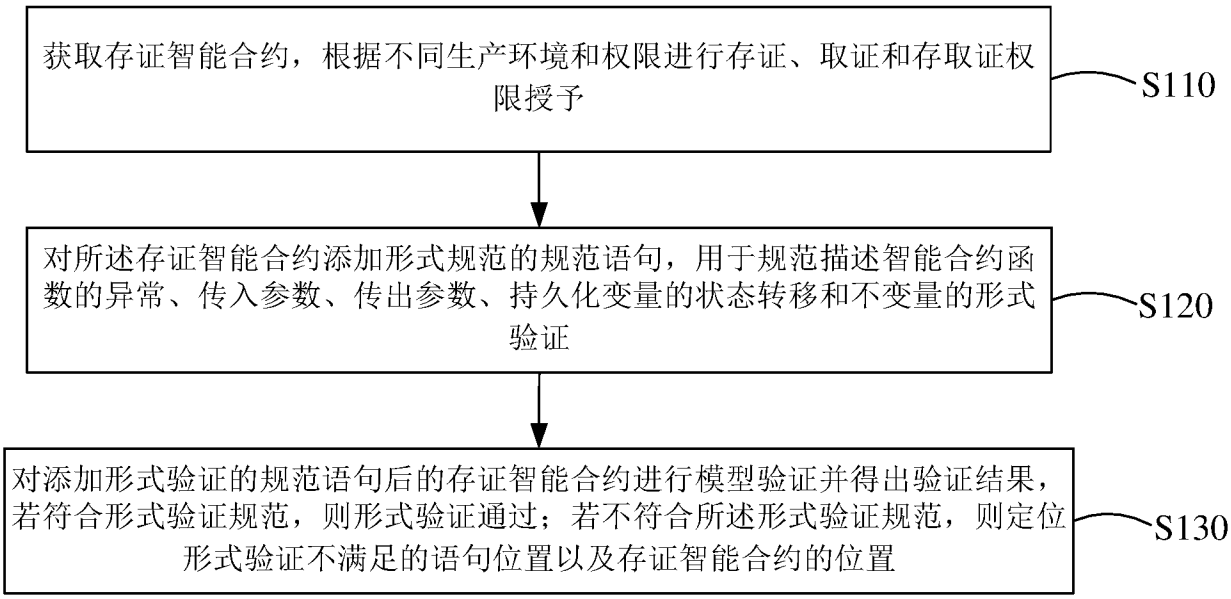
获取存证智能合约，根据不同生产环境和权限进行存证、取证和存取证权限授予
S110
对所述存证智能合约添加形式规范的规范语句，用于规范描述智能合约函数的异常、传入参数、传出参数、持久化变量的状态转移和不变量的形式验证
S120
对添加形式验证的规范语句后的存证智能合约进行模型验证并得出验证结果，若符合形式验证规范，则形式验证通过；若不符合所述形式验证规范，则定位形式验证不满足的语句位置以及存证智能合约的位置
S130

图 2

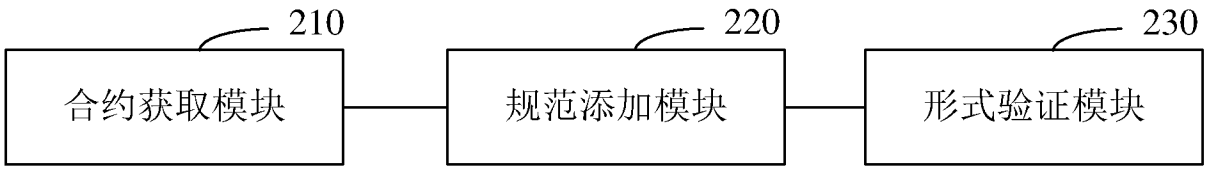
210
合约获取模块
220
规范添加模块
230
形式验证模块

图 3

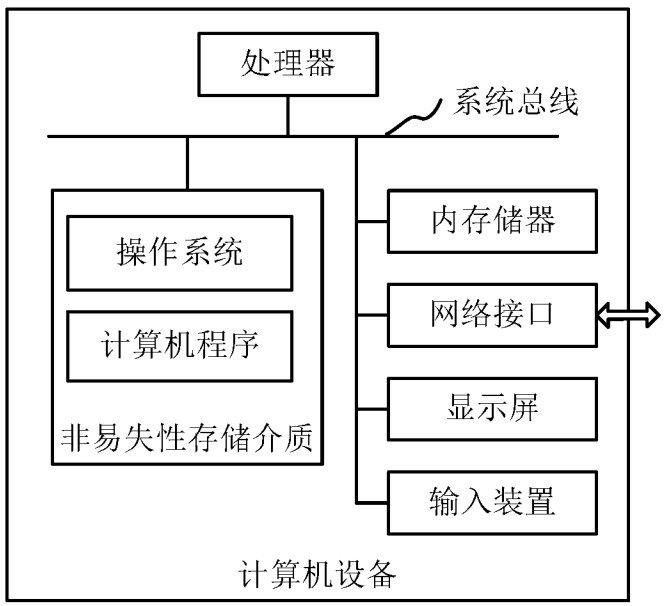
处理器
系统总线
操作系统
计算机程序
非易失性存储介质
内存储器
网络接口
显示屏
输入装置
计算机设备

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/110512

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/64(2013.01)i; G06Q 40/04(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F,; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, GOOGLE, ISI: 区块链, 智能合约, 存证, 形式验证, 形式化验证, 规范; block chain, smart contract, formal verification, deposit, specification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110555320 A (HANGZHOU QULIAN TECHNOLOGY CO., LTD.) 10 December 2019 (2019-12-10) description paragraphs [0002], [0021]-[0033]	1-11
X	CN 109375899 A (HANGZHOU QULIAN TECHNOLOGY CO., LTD.) 22 February 2019 (2019-02-22) description paragraphs [0054]-[0068], [0144]-[0155], figure 2	1, 4-8, 11
A	CN 107783758 A (BEIHANG UNIVERSITY) 09 March 2018 (2018-03-09) entire document	1-11
A	CN 108776936 A (PING AN LIFE INSURANCE COMPANY OF CHINA, LTD.) 09 November 2018 (2018-11-09) entire document	1-11
A	WO 2019108676 A1 (YALE UNIVERSITY) 06 June 2019 (2019-06-06) entire document	1-11

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 October 2020	**28 October 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/110512

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110555320 A	10 December 2019	None	
CN 109375899 A	22 February 2019	None	
CN 107783758 A	09 March 2018	CN 107783758 B	18 January 2019
CN 108776936 A	09 November 2018	None	
WO 2019108676 A1	06 June 2019	WO 2019108676 A8	04 June 2020

国际检索报告

国际申请号
PCT/CN2020/110512

A. 主题的分类

G06F 21/64(2013.01)i; G06Q 40/04(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F,; G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, GOOGLE, ISI: 区块链，智能合约，存证，形式验证，形式化验证，规范; block chain, smart contract, formal verification, deposit, specification

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 110555320 A (杭州趣链科技有限公司) 2019年 12月 10日 (2019-12-10) 说明书第[0002]、[0021]-[0033]段	1-11
X	CN 109375899 A (杭州趣链科技有限公司) 2019年 2月 22日 (2019-02-22) 说明书第[0054]-[0068]、[0144]-[0155]段、图2	1，4-8，11
A	CN 107783758 A (北京航空航天大学) 2018年 3月 9日 (2018-03-09) 全文	1-11
A	CN 108776936 A (中国平安人寿保险股份有限公司) 2018年 11月 9日 (2018-11-09) 全文	1-11
A	WO 2019108676 A1 (YALE UNIVERSITY) 2019年 6月 6日 (2019-06-06) 全文	1-11

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 10月 15日	2020年 10月 28日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	张琳琳
传真号 (86-10)62019451	电话号码 86-(10)-53961404

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/110512

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 110555320 A	2019年 12月 10日	无	
CN 109375899 A	2019年 2月 22日	无	
CN 107783758 A	2018年 3月 9日	CN 107783758 B	2019年 1月 18日
CN 108776936 A	2018年 11月 9日	无	
WO 2019108676 A1	2019年 6月 6日	WO 2019108676 A8	2020年 6月 4日