(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
2022 年 3 月 24 日 (24.03.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/057720 A1

(51) 国际专利分类号:
G06F 21/57 (2013.01)

(21) 国际申请号: PCT/CN2021/117387

(22) 国际申请日: 2021 年 9 月 9 日 (09.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010982939.8 2020年9月16日 (16.09.2020) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: **王晖 (WANG, Hui)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼, Zhejiang 311121 (CN)。 **李志超 (LI, Zhichao)**; 中国浙江省杭州市余杭区文一西路969号3号楼, Zhejiang 311121 (CN)。 **陈继承 (CHEN, Jicheng)**; 中国浙江省杭州市余杭区文一西路969号3号楼, Zhejiang 311121 (CN)。 **黄子龙 (HUANG, Zilong)**; 中国浙江省杭州市余杭区文一西路969号3号楼, Zhejiang 311121 (CN)。 **吕涛 (LYU, Tao)**; 中国浙江省杭州市余杭区文一西路969号3号楼, Zhejiang 311121 (CN)。 **刘方 (LIU, Fang)**; 中国浙江省杭州市余杭区文一西路969号3号楼, Zhejiang 311121 (CN)。 **王志谦 (WANG, Zhiqian)**; 中国浙江省杭州市余杭区文一西路969号3号楼, Zhejiang 311121 (CN)。

(54) **Title:** TRUSTED VERIFICATION SYSTEM AND METHOD, MOTHERBOARD, MICRO-BOARD CARD, AND STORAGE MEDIUM

(54) **发明名称**: 一种可信验证的系统、方法、主板、微型板卡及存储介质

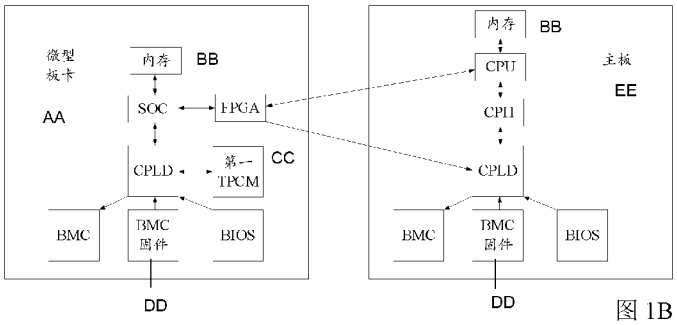

图 1B

AA Micro-board card
BB Memory
CC First TPCM
DD Firmware
EE Motherboard

(57) **Abstract:** Provided in the embodiments of the present application are a trusted verification system and method, a motherboard, a micro-board card, and a storage medium. According to the solution provided in the embodiments of the present application: when the system is powered on, performing trusted verification of a micro-board card on the basis of a first trusted platform control module TPCM on the micro-board card and, after verification is successful, controlling the other components in the micro-board card to disengage from a reset state and performing trusted verification on the motherboard by means of a motherboard verification component used for performing trusted verification on the motherboard.

(57) **摘要**: 本申请实施例提供了一种可信验证的系统、方法、主板、微型板卡及存储介质。根据本申请实施例提供的方案，系统在通电启动时，首先基于微型板卡上的第一可信平台控制模块TPCM对微型板卡本身进行可信验证，在验证通过之后，控制所述微型板卡中的其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

WO 2022/057720 A1

[见续页]

(74) 代理人：北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)；中国北京市金融街35号国际企业大厦A座16层，Beijing 100033 (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))。

一种可信验证的系统、方法、主板、微型板卡及存储介质

本申请要求2020年09月16日递交的申请号为202010982939.8、发明名称为“一种可信验证的系统、方法、主板、微型板卡及存储介质”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

本申请实施例涉及计算机技术领域，尤其涉及一种可信验证的系统、方法、主板、微型板卡及存储介质。

背景技术

随着对信息安全要求的不断提高，在设备启动时对设备中的相关信息进行可信验证已经很有必要。当前的设备的基本架构如图1A所示。在启动时，主板上的可信平台控制模块（trusted platform control module，TPCM）首先上电工作，并对主板中的各固件进行可信验证，而同时高速串行扩展总线（peripheral component interconnect express，PCIE）还没有上电工作。在这种方式下，设备启动时仍然存在一些固件（例如，PCIE中的各固件）没有进行可信验证。

基于此，需要一种在设备启动时更为全面的可信验证方案。

发明内容

有鉴于此，本申请实施例提供一种可信验证的系统、方法、主板、微型板卡及存储介质，以至少部分解决上述问题。

根据本申请实施例的第一方面，提供了一种可信验证的系统，包括：

主板；和，

微型板卡，所述微型板卡连接所述主板，所述微型板卡中包括第一可信平台控制模块TPCM；

当所述系统通电启动时，所述第一 TPCM，对所述微型板卡进行可信验证；并在所述微型板卡的可信验证通过后，控制所述系统的其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

根据本申请实施例的第二方面，提供了一种可信验证的主板，所述主板中包括复杂可编程逻辑器件CPLD和第二可信平台控制模块TPCM；

所述CPLD接收来自于已经通过可信验证的微型板卡的控制信号，并控制所述第二TPCM脱离复位状态；

所述第二TPCM对所述主板进行可信验证。

根据本申请实施例的第三方面，提供了一种可信验证的微型板卡，所述微型板卡连接主板，所述微型板卡中包括第一可信平台控制模块TPCM；

当设备通电启动时，所述第一 TPCM，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制其它部件脱离复位状态，并通过用于对主板进行可信验

证的主板验证部件对所述主板进行可信验证。

根本本申请的第四方面，提供了一种服务器，所述服务器中包括如第二方面所述的主板。

根据本申请实施例的第五方面，提供了一种可信验证的方法，应用于包含主板和微型板卡的系统中，所述方法包括：

当所述系统通电启动时，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态；并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

根据本申请实施例的第六方面，提供了一种计算机存储介质，其上存储有计算机程序，该程序被处理器执行时实现如前述的可信验证的方法。

根据本申请实施例提供的方案，系统在通电启动时，首先基于微型板卡上的第一可信平台控制模块 TPCM 对微型板卡本身进行可信验证，在验证通过之后，控制所述微型板卡中的其它部件脱离复位状态，以正常工作，然后通过系统中的主板验证部件对主板进行可信验证，从而实现在系统启动时对于系统的全面的可信验证。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请实施例中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其他的附图。

图 1A 为当前系统所涉及的架构示意图；

图 1B 为本申请实施例所提供的一种可信验证的系统的示意图；

图 1C 为本申请实施例所提供的另一种可信验证的系统的示意图；

图 1D 为本申请实施例所提供的一种可信验证的主板的结构示意图；

图 1E 为本申请实施例所提供的一种可信验证的微型板卡的结构示意图；

图 2 为本申请实施例所提供的一种系统进行可信验证的流程示意图；

图 3 为本申请实施例所提供的一种可信验证的方法的流程示意图。

具体实施方式

为了使本领域的人员更好地理解本申请实施例中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请实施例一部分实施例，而不是全部的实施例。基于本申请实施例中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于本申请实施例保护的范围。

首先，在对本申请实施例进行描述的过程中出现的部分名词或术语适用于如下解释：

TPCM：可信平台控制模块，Trusted Platform Control Module。TPCM 中可以预先存

储设备的相关信息，并用于可信验证。

FPGA：现场可编程逻辑门阵列，Field Programmable Gate Array。它是作为专用集成电路（Application Specific Integrated Circuit ，ASIC）领域中的一种半定制电路而出现的，具备可编程和可存储功能。

CPLD：复杂可编程逻辑器件，Complex Programmable Logic Device。用户可以在CPLD中根据需要而自行构造逻辑功能的数字集成电路。例如，借助集成开发软件平台，用原理图、硬件描述语言等方法，生成相应的目标文件，将代码传送到目标芯片中，实现设计的数字系统。

PCIE：高速串行扩展总线标准，Peripheral Component Interconnect Express。在常规设备中，PCIE卡通过PCIE的规范与主板连接。

如图1A所示，图1A为当前系统所涉及的架构示意图。在这种情形下，系统通电启动时，主板中的TPCM会先上电工作，而PCIE卡不会上电。主板中的TPCM对于主板中的固件验证完毕之后，即启动系统，对于PCIE中的固件则无法进行可信验证。

微型板卡：即为自带CPU和ROM/RAM的物理板卡设备，能够运行独立的操作系统，同时可以通过系统总线连入到另外的硬件上，对该硬件上提供输入输出IO设备的虚拟、IO请求的处理和转发等服务，微型板卡上还可以包含可编程部件CPLD、FPGA等等。例如，卡上微型服务器（Microserver On Card，MOC）即为微型板卡的一种。

第一TPCM：处于微型板卡中的TPCM;

第二TPCM：处于主板中的TPCM。

基于前述，本申请实施例提供一种可信验证的系统，在启动时实现更为全面的可信验证。所述系统包括：

主板；和，卡上微型服务器微型板卡，所述微型板卡连接所述主板，所述微型板卡中包括第一可信平台控制模块TPCM;

当所述系统通电启动时，所述第一 TPCM，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述系统中的其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

具体而言，在系统通电启动时，微型板卡先于主板进行通电启动。在微型板卡完成可信验证之前，所述主板（包括主板中的各部件）一直保持复位状态。

在微型板卡进行可信验证的流程中，微型板卡中的第一TPCM最先开始工作，此时微型板卡中的其它部件也处于复位状态，并等待第一TPCM对微型板卡进行可信验证。

在一种实施例中，在对于所述微型板卡的可信验证通过后，所述第一TPCM可以直接控制微型板卡上的部件（包括微型板卡中的其它部件和主板验证部件）脱离复位状态，并通过主板验证部件执行对主板的可信验证。

在一种实施例中，第一TPCM也可以通过相应的控制信号，来间接的控制主板上的

部件（包括主板中的其它部件和主板验证部件）脱离复位状态，以使得主板验证部件开始对主板进行可行验证。

例如，第一 TPCM 在控制微型板卡中的其它部件脱离复位状态之后，即可以通过位于微型板卡中的其它部件中的可编程部件对所述主板中的主板验证部件进行使能操作，以通过所述主板中的主板验证部件对所述主板进行可信验证。

所述位于微型板卡中的其它部件中的可编程部件可以是设置于微型板卡中的复杂可编程逻辑器件 CPLD 和/或现场可编程逻辑门阵列 FPGA，它们可以向主板中的 CPLD 发送使能信号，使得主板中的 CPLD 激活主板中的主板验证部件，并执行对主板的可信验证。

对所述主板进行可信验证的主板验证部件可以是微型板卡中的部件，也可以是主板中的部件。例如，第一 TPCM 可以通过微型板卡中的可编程部件 CPLD 或者 FPGA 发送使能信号，控制主板上的 CPLD 激活主板中的第二 TPCM，使得第二 TPCM 进行对主板的可信验证。又例如，对所述主板进行可信验证的主板验证部件可以是设置于微型板卡中的 FPGA 模块。

如图 1B 所示，图 1B 为本申请实施例所提供的一种可信验证的系统的示意图，所述设备包括：

主板；和，卡上微型服务器微型板卡，所述微型板卡中第一 TPCM 和现场可编程逻辑门阵列 FPGA，所述 FPGA 连接所述主板；具体而言，所述 FPGA 可以通过 PCIE 连接所述主板中的 CPU 和 CPLD。

当所述系统通电启动时，所述第一 TPCM，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态；

所述 FPGA 用于，在所述微型板卡的可信验证通过后，对所述主板进行可信验证。

换言之，当该系统通电启动时，微型板卡中的第一 TPCM 会先上电工作，充当对于微型板卡执行可信验证的部件。此时，微型板卡上的其它部件（包括 FPGA）和主板上的部件均处在复位状态。

如图 1B 所示，由于微型板卡中的固件包括诸如片上系统（System on Chip，SOC）、基本输入输出系统（Basic Input Output System，BIOS）、基板管理控制器（Baseboard Manager Controller，BMC）等多个部件，各部件中可能存在一些固件或者一些系统代码，第一 TPCM 对于微型板卡的可信验证可以包括对这些部件的固件或者系统代码的可信验证。

具体而言，第一 TPCM 在通电工作时，首先处于串行外围设备接口(Serial Peripheral Interface，SPI)主模式，在该模式下，可以基于 SPI 主接口读取微型板卡的 BIOS 中和 BMC 中的固件，并对 BIOS 和 BMC 中的固件进行可信验证。

第一 TPCM 可以在第一 TPCM 的寄存器中预先存储一份可信度量根（例如，由可信

硬件预先得到的固件的哈希值，或者预先存储的固件的指定位置的可信的部分代码），具体的验证方式可以是第一 TPCM 确认所述固件的固件度量值（即固件的哈希值，或者固件的指定位置的代码），将固件度量值与预存的可信度量根进行匹配，若二者一致，则确认所述固件可信。

在确定了 BIOS 和 BMC 中的固件可信之后，此时，第一 TPCM 即可以发出 SOC 复位失效信号和 BMC 复位失效信号，使得 SOC 和 BMC 脱离复位状态，开始正常工作，SOC 开始加载所述 BIOS 中的固件，所述 BMC 开始加载所述 BMC 中的固件。

在 SOC 和 BMC 加载固件完毕之后，第一 TPCM 切换为 SPI 从模式，开始与 SOC 的 SPI 主控进程进行通信，被动地接受连接到微型板卡上的外围设备和预设的微型板卡信息，并对外围设备和预设的微型板卡信息。具体的外围设备可以包括连接于微型板卡的外围设备的型号、唯一标识、名称等等，微型板卡信息可以包括连接于微型板卡的各外围设备中的固件代码以及 SOC 的版本等等。

在对于所述微型板卡上的外围设备和预设的微型板卡信息进行可信验证通过后，此时第一 TPCM 即可以对所述 SOC 的系统代码进行可信验证。在 SOC 的操作系统的系统代码进行可信验证之后，此时即说明了微型板卡本身已经是可信的了，此时所述 SOC 加载所述 SOC 的系统代码，完成对于微型板卡的启动。

对于外围设备、预设的微型板卡信息和 SOC 的系统代码进行可信验证的方式，与对于微型板卡中的固件进行可信验证的方式类似，此处不再赘述。

在对于微型板卡完成可信验证之后，此时 FPGA 已经被第一 TPCM 指示脱离了复位状态，开始正常工作，并作为主要的实现对主板实现可信验证的功能模块，此时，主板中的部件仍然均处于复位状态。

主板中包含有主板中的 BIOS 和 BMC，以及存在于主板上的操作系统等部件，具体而言，所述 FPGA 对于主板进行可信验证，可以包括对于主板中的 BIOS、BMC 和主板上的操作系统进行可信验证。

具体而言，当微型板卡已经完成可信验证，而主板上的部件仍然均处于复位状态时，此时可以通过 FPGA 上的 SPI 主设备，对获取所述主板中的固件，并对所述主板中的固件进行可信验证，其中主板中的固件包括所述主板的基本输入输出系统 BIOS 的固件和所述主板的基板管理控制器 BMC 的固件。

具体的验证方式与前述类似，FPGA 可以预先存储一份可信度量根（例如，由可信硬件预先得到的固件的哈希值，或者预先存储的固件的指定位置的可信的部分代码），具体的验证方式可以是 FPGA 确认所述主板上的固件的固件度量值（即固件的哈希值，或者固件的指定位置的代码），将固件度量值与预存的可信度量根进行匹配，若二者一致，则确认所述主板上的固件可信。

在 FPGA 对所述主板中的固件进行可信验证通过之后，FPGA 即发送出主板上的

BMC 和 BIOS 的复位失效的信号，控制所述主板的 BIOS 和 BMC 脱离复位状态，同时所述主板的平台控制器集线器（Platform Controller Hub，PCH，又称为集成南桥）加载所述主板的 BIOS 中的固件，所述主板的 BMC 加载所述主板的 BMC 中的固件。

在 BIOS 和 BMC 中的固件被加载完毕之后，所述 FPGA，切换为串行外围设备接口 SPI 从模式，对所述主板中的外围设备和预设的主板信息进行可信验证。主板中的外围设备可以包括连接于主板的外围设备的型号、唯一标识、名称等等，预设的主板信息可以包括各连接于主板的外围设备中的固件代码、主板上的操作系统的版本等等。

进而，所述 FPGA 对所述主板中的外围设备和预设的主板信息进行可信验证通过之后，FPGA 对所述主板上的操作系统的代码进行可信验证，在验证通过后，所述主板加载所述主板上的操作系统的代码，从而构建了整个系统的硬件可信环境。

此外，需要说明的是，前述对于微型板卡的可信验证的过程中具体顺序的实现和相关复位信号的传递可以通过在 CPLD 中进行编程而可以实现。

在另一种实施例中，对所述主板进行可信验证的其它部件可以是主板中的第二 TPCM，如图 1C 所示，图 1C 为本申请实施例所提供的另一种可信验证的系统的示意图，所述系统包括：

主板；和，卡上微型服务器微型板卡，所述微型板卡中包括第一可信平台控制模块 TPCM，所述主板中包括第二可信平台控制模块 TPCM；

当所述系统通电启动时，所述第一 TPCM，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态，并通过脱离复位状态后的所述其它部件中的可编程部件（例如，微型板卡中的 CPLD）对所述主板中的主板验证部件进行使能操作，以通过所述主板中的第二 TPCM 对所述主板进行可信验证。

第一 TPCM 对于微型板卡的可信验证过程在前述部分已经进行了说明，此处不再赘述。

在第一 TPCM 对于微型板卡的可信验证通过后，此时，微型板卡上已经脱离复位状态的 BMC 可以产生主板控制信号，该控制信号经过设置于所述微型板卡中的可编程部件发送至所述主板，所述主板根据所述控制指令，控制所述第二 TPCM 脱离复位状态，所述第二 TPCM 对所述主板进行可信验证。

具体而言，所述微型板卡中的可编程部件可以是设置于微型板卡中的复杂可编程逻辑器件 CPLD 或者现场可编程逻辑门阵列 FPGA。

在主板中接收该控制指令的可以是设置于主板中的复杂可编程逻辑器件 CPLD，进而主板上的 CPLD 根据该控制信号控制所述第二 TPCM 脱离复位状态，并开始对主板执行可信验证。此时的第二 TPCM 对主板进行可信验证的流程具体如下：

第二 TPCM，读取所述主板中的固件，并对所述主板中的固件进行可信验证，其中

主板中的固件包括所述主板的基本输入输出系统 BIOS 的固件和所述主板的基板管理控制器 BMC 的固件。当计算得到的固件度量值与预存在第二 TPCM 中的值一致时，验证通过。

然后所述第二 TPCM 发出控制信号，控制所述主板的 BIOS 和 BMC 脱离复位状态并开始加载已经验证过的固件。进而，所述第二 TPCM，切换为串行外围设备接口 SPI 从模式，主板中的与 PCH 的 SPI 主控进行通信，并对所述主板中的外围设备和预设的主板信息进行可信验证，在对于外设和主板信息的验证通过之后，第二 TPCM 即对所述主板上的操作系统的代码进行可信验证，并在验证通过之后启动系统。

根据本申请实施例提供的方案，系统在通电启动时，首先基于微型板卡上的第一可信平台控制模块 TPCM 对微型板卡本身可信验证，在验证通过之后，控制所述微型板卡中的其它部件脱离复位状态，以正常工作，然后再通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证，从而实现在系统启动时对于系统的全面的可信验证。

需要说明的是，在前述的可信验证过程中，如果存在任一部件的可信验证失败，即可以中断系统的启动过程，以维护系统的安全运行环境。

此外，在一种实施例中，当启动以后主板在正常运行的过程中，微型板卡中的 FPGA 还可以对于主板的内存中的信息进行监测，以确定所述主板中运行的内容是否可信。主板的内存中的信息可以包括运行的进程的名称、进程的数量、进程占用的空间、进程调用的接口等等。

进一步地，FPGA 对所述内存中的信息进行监测可以包括确定获取得到的内存中的信息的哈希值；将所述内存中的信息的哈希值与 FPGA 中预存的哈希值进行匹配。

预存的哈希值可以是一些对主板上的数据或程序的安全性产生不良影响的危险进程的名称或者标识所对应的哈希值，相当于黑名单。从而如果主板上的内存中存在某个进程的相关的哈希值与预存的哈希值相同，则可以认为主板所处的设备上运行了某些存在安全风险的进程；或者，预存的哈希值也可以是已经被确认的安全进程的名称或者标识所对应的哈希值，相当于白名单，从而如果主板上的内存中存在某个进程的相关哈希值与预先存储的哈希值不相同，则可以认为该进程是存在安全风险的进程。进而可以对存在安全风险的进程实施相应的监控，或者可以调用微型板卡强制关闭该进程，以实现动态的安全环境的维护。

在一种实施例中，该系统中的主板可以是服务器主板。

为使本申请的方案更为浅显易懂，以下给出一个更为具体的示例，如图 2 所示，图 2 为本申请实施例所提供的一种系统进行可信验证的流程示意图，在该示意图中，采用了系统的微型板卡中的 FPGA 模块对于主板进行可信验证，其具体包括：

201，系统通电，开始启动；

其中，所述系统中包含有微型板卡和主板。

202，微型板卡中的第一 TPCM 上电工作，其余部件均处于复位状态；

203，第一 TPCM 验证微型板卡的 BIOS 和 BMC 中的固件；

204，验证通过，微型板卡上的 SOC 和 BMC 脱离复位状态，微型板卡上的 SOC 和 BMC 加载固件；

205，第一 TPCM 切换为从模式，验证微型板卡的外设和微型板卡信息；

206，验证通过，第一 TPCM 验证 SOC 的系统代码；

207，验证通过，微型板卡上的 FPGA 验证主板的 BIOS 及 BMC 中的固件；

208，验证通过，主板上的 BIOS 和 BMC 脱离复位状态，主板上的 BIOS 和 BMC 加载固件；

209，FPGA 切换为从模式，验证主板的外设和主板信息；

210，验证通过，FPGA 验证主板上的操作系统的代码；

211，验证通过，主板加载所述主板上的操作系统的代码，设备启动。

前述任一可信验证失败，均可以中断系统的启动过程。

在系统启动之后，FPGA 还可以监测主板中的内存信息，实现对于系统的安全环境的动态的监测。

本申请的第二方面，还提供一种可信验证的主板，如图 1D 所示，图 1D 为本申请实施例所提供的一种可信验证的主板的结构示意图，所述主板中包括复杂可编程逻辑器件 CPLD 和第二可信平台控制模块 TPCM；

所述 CPLD 接收来自于已经通过可信验证的微型板卡的控制信号，并控制所述第二 TPCM 脱离复位状态；

所述第二 TPCM 对所述主板进行可信验证。

本申请的第三方面，还提供一种可信验证的微型板卡，如图 1E 所示，图 1E 为本申请实施例所提供的一种可信验证的微型板卡的结构示意图，所述微型板卡连接主板（图中未示出），所述微型板卡中包括第一可信平台控制模块 TPCM；

当设备通电启动时，所述第一 TPCM，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

其中，主板验证部件包括设置于微型板卡中的现场可编程逻辑门阵列 FPGA，和/或，复杂可编程逻辑器件 CPLD。

本申请实施例的第四方面，还提供一种服务器，包括：如第二方面所述的可信验证的主板；

进一步地，在所述服务器中，还包括如第三方面所述的可信验证的微型板卡。

本申请实施例的第五方面，还提供一种可信验证的方法，应用于包含主板和微型板卡的系统中，如图 3 所示，图 3 为本申请实施例所提供的一种可信验证的方法的流程示意图，所述方法具体包括：

S301，当所述系统通电启动时，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态；

S303，通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。可选地，对所述微型板卡进行可信验证可以采用微型板卡中的第一 TPCM 对所述微型板卡进行可信验证；

可选地，所述第一 TPCM 在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件和所述主板验证部件脱离复位状态，并通过脱离复位状态后的所述主板验证部件对所述主板进行可信验证；

可选地，所述微型板卡中的所述主板验证部件包括设置于所述微型板卡中的现场可编程逻辑门阵列 FPGA，所述 FPGA 连接所述主板；所述微型板卡通过所述 FPGA 对所述主板进行可信验证。

可选地，所述第一 TPCM 在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态，并通过脱离复位状态后的所述其它部件中的可编程部件对所述主板中的主板验证部件进行使能操作，以通过所述主板中的主板验证部件对所述主板进行可信验证。

可选地，所述主板中的主板验证部件包括所述主板中的第二 TPCM；所述微型板卡通过所述可编程部件对所述主板中的主板验证部件进行使能操作，以通过所述主板中的第二 TPCM 对所述主板进行可信验证。

可选地，所述微型板卡通过设置于所述微型板卡中的可编程部件发送控制指令至所述主板；所述主板根据所述控制指令，控制所述第二 TPCM 脱离复位状态，并通过所述第二 TPCM 对所述主板进行可信验证。

可选地，所述可编程部件包括：复杂可编程逻辑器件 CPLD 和/或现场可编程逻辑门阵列 FPGA。

可选地，所述微型板卡中还包括基本输入输出系统 BIOS 和基板管理控制器 BMC，对所述微型板卡进行可信验证包括，读取固件，对所述固件进行可信验证，其中，所述固件包括所述微型板卡的基本输入输出系统 BIOS 中的固件和所述微型板卡的 BMC 中的固件。

可选地，对所述固件进行可信验证，包括：确认所述固件的哈希值，与预存的哈希值进行匹配，若二者一致，则确认所述固件可信。

可选地，当对所述固件进行可信验证通过后，控制所述 SOC 和所述 BMC 脱离复位状态；相应的，所述 SOC 加载所述 BIOS 中的固件，以及，所述 BMC 加载所述 BMC 中的固件；

可选地，对所述微型板卡进行可信验证，包括：所述第一 TPCM 切换为串行外围设备接口 SPI 从模式，对所述微型板卡上的外围设备和预设的微型板卡信息进行可信验证。

可选地，所述微型板卡上的外围设备和预设的微型板卡信息进行可信验证通过后；对所述 SOC 的系统代码进行可信验证，在验证通过后，所述 SOC 加载所述 SOC 的系统代码。

可选地，对所述主板进行可信验证，包括：获取所述主板中的固件，并对所述主板中的固件进行可信验证，其中主板中的固件包括所述主板的基本输入输出系统 BIOS 的固件和所述主板的基板管理控制器 BMC 的固件。

可选地，在所述主板的可信验证通过之后，控制所述主板脱离复位状态，包括：对所述主板中的固件进行可信验证通过之后，控制所述主板的 BIOS 和 BMC 脱离复位状态；所述主板的平台控制器集线器 PCH 加载所述主板的 BIOS 中的固件，所述主板的 BMC 加载所述主板的 BMC 中的固件。

可选地，对所述主板进行可信验证，包括：对所述主板中的外围设备和预设的主板信息进行可信验证。

可选地，对所述主板中的外围设备和预设的主板信息进行可信验证通过之后，对所述主板上的操作系统的代码进行可信验证，在验证通过后，所述主板加载所述主板上的操作系统的代码。

可选地，获取所述主板的内存中的信息，对所述内存中的信息进行监测。

可选地，对所述内存中的信息进行监测，包括：确定获取得到的内存中的信息的代码的哈希值；将所述内存中的信息的代码的哈希值与预存的哈希值进行匹配。

可选地，当所述系统通电启动时，所述微型板卡先于所述主板通电启动，且，在所述微型板卡的可信验证通过之前，所述主板保持复位状态；相应的，在所述微型板卡的可信验证通过后，所述微型板卡控制所述通过主板脱离复位状态。

可选地，所述主板为服务器主板。

根据本申请实施例提供的方案，系统在通电启动时，首先基于微型板卡上的第一可信平台控制模块 TPCM 对微型板卡本身可信验证，在验证通过之后，控制所述微型板卡中的其它部件脱离复位状态，以正常工作，然后通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证，从而实现在系统启动时对于系统的全面的可信验证。

本申请实施例的第六方面，还提供一种计算机机存储介质，其上存储有计算机程序，该程序被处理器执行时实现如图 3 所述的可信验证的方法。

需要指出，根据实施的需要，可将本申请实施例中描述的各个部件/步骤拆分为更多部件/步骤，也可将两个或多个部件/步骤或者部件/步骤的部分操作组合成新的部件/步骤，以实现本申请实施例的目的。

上述根据本申请实施例的方法可在硬件、固件中实现，或者被实现为可存储在记录介质（诸如 CD ROM、RAM、软盘、硬盘或磁光盘）中的软件或计算机代码，或者被实现通过网络下载的原始存储在远程记录介质或非暂时机器可读介质中并将被存储在本地记录介质中的计算机代码，从而在此描述的方法可被存储在使用通用计算机、专用处理器或者可编程或专用硬件（诸如 ASIC 或 FPGA）的记录介质上的这样的软件处理。可以理解，计算机、处理器、微处理器控制器或可编程硬件包括可存储或接收软件或计算机代码的存储组件（例如，RAM、ROM、闪存等），当所述软件或计算机代码被计算机、处理器或硬件访问且执行时，实现在此描述的可信验证的方法。此外，当通用计算机访问用于实现在此示出的可信验证的方法的代码时，代码的执行将通用计算机转换为用于执行在此示出的可信验证的方法的专用计算机。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及方法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请实施例的范围。

以上实施方式仅用于说明本申请实施例，而并非对本申请实施例的限制，有关技术领域的普通技术人员，在不脱离本申请实施例的精神和范围的情况下，还可以做出各种变化和变型，因此所有等同的技术方案也属于本申请实施例的范畴，本申请实施例的专利保护范围应由权利要求限定。

权 利 要 求 书

1.一种可信验证的系统，包括：

主板；和，

微型板卡，所述微型板卡连接所述主板，所述微型板卡中包括第一可信平台控制模块 TPCM；

当所述系统通电启动时，第一 TPCM，对所述微型板卡进行可信验证；并在所述微型板卡的可信验证通过后，控制所述微型板卡的其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

2.如权利要求 1 所述的系统，其中，所述第一 TPCM 在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件和所述主板验证部件脱离复位状态，并通过脱离复位状态后的所述主板验证部件对所述主板进行可信验证。

3.如权利要求 2 所述的系统，其中，所述微型板卡中的所述主板验证部件包括设置于所述微型板卡中的现场可编程逻辑门阵列 FPGA，所述 FPGA 连接所述主板；

所述微型板卡通过所述 FPGA 对所述主板进行可信验证。

4.如权利要求 1 所述的系统，其中，所述第一 TPCM 在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态，并通过脱离复位状态后的所述其它部件中的可编程部件对所述主板中的主板验证部件进行使能操作，以通过所述主板中的主板验证部件对所述主板进行可信验证。

5.如权利要求 4 所述的系统，其中，所述主板中的主板验证部件包括所述主板中的第二 TPCM；

所述微型板卡通过所述可编程部件对所述主板中的主板验证部件进行使能操作，以通过所述主板中的第二 TPCM 对所述主板进行可信验证。

6.如权利要求 5 所述的系统，其中，

所述微型板卡通过设置于所述微型板卡中的可编程部件发送控制指令至所述主板；

所述主板根据所述控制指令，控制所述第二 TPCM 脱离复位状态，并通过所述第二 TPCM 对所述主板进行可信验证。

7.如权利要求 4-6 任一项所述的系统，其中，所述可编程部件包括：复杂可编程逻辑器件 CPLD 和/或现场可编程逻辑门阵列 FPGA。

8.如权利要求 1 所述的系统，其中，所述微型板卡中还包括基本输入输出系统 BIOS 和基板管理控制器 BMC；

所述第一 TPCM，对所述微型板卡进行可信验证，包括：所述第一 TPCM 读取固件，对所述固件进行可信验证，其中，所述固件包括所述微型板卡的基本输入输出系统 BIOS 中的固件和所述微型板卡的 BMC 中的固件。

9.如权利要求 8 所述的系统，其中，所述第一 TPCM 读取固件，对所述固件进行可信验证，包括：

所述第一 TPCM 读取固件，确认所述固件的哈希值，与预存于所述第一 TPCM 中的哈希值进行匹配，若二者一致，则确认所述固件可信。

10. 如权利要求 8 所述的系统，其中，所述微型板卡中还包括片上系统 SOC；

当对所述固件进行可信验证通过后，所述第一 TPCM 控制所述 SOC 和所述 BMC 脱离复位状态；

相应的，所述 SOC 加载所述 BIOS 中的固件，以及，所述 BMC 加载所述 BMC 中的固件。

11. 如权利要求 10 所述的系统，其中，所述第一 TPCM，对所述微型板卡进行可信验证，包括：

所述第一 TPCM 切换为串行外围设备接口 SPI 从模式，对所述微型板卡上的外围设备和预设的微型板卡信息进行可信验证。

12. 如权利要求 11 所述的系统，其中，当所述微型板卡上的外围设备和预设的微型板卡信息进行可信验证通过后，

所述第一 TPCM 对所述 SOC 的系统代码进行可信验证，在验证通过后，所述 SOC 加载所述 SOC 的系统代码。

13. 如权利要求 3 所述的系统，其中，所述微型板卡通过所述 FPGA 对所述主板进行可信验证包括：

所述 FPGA，获取所述主板中的固件，并对所述主板中的固件进行可信验证，其中主板中的固件包括所述主板的基本输入输出系统 BIOS 的固件和所述主板的基板管理控制器 BMC 的固件。

14. 如权利要求 13 所述的系统，其中，所述 FPGA 还用于，对所述主板中的固件进行可信验证通过之后，控制所述主板的 BIOS 和 BMC 脱离复位状态；

相应的，所述主板的平台控制器集线器 PCH 加载所述主板的 BIOS 中的固件，所述主板的 BMC 加载所述主板的 BMC 中的固件。

15. 如权利要求 14 所述的系统，其中，所述微型板卡通过所述 FPGA 对所述主板进行可信验证，包括：

所述 FPGA，切换为串行外围设备接口 SPI 从模式，对所述主板上的外围设备和预设的主板信息进行可信验证。

16. 如权利要求 15 所述的系统，其中，所述微型板卡通过所述 FPGA 对所述主板进行可信验证，包括：

当对所述主板上的外围设备和预设的主板信息进行可信验证通过之后，所述 FPGA，对所述主板上的操作系统的代码进行可信验证。

17. 如权利要求 3 所述的系统，其中，所述 FPGA 还用于，获取所述主板的内存中的信息，对所述内存中的信息进行监测。

18. 如权利要求 17 所述的系统，其中，所述 FPGA 还用于，对所述内存中的信息进

行监测，包括：

确定获取得到的内存中的信息的哈希值；

将所述内存中的信息的哈希值与 FPGA 中预存的哈希值进行匹配。

19. 如权利要求 5 所述的系统，其中，所述微型板卡通过所述其它部件控制所述主板中的第二 TPCM 对所述主板进行可信验证，包括：

所述第二 TPCM，读取所述主板中的固件，并对所述主板中的固件进行可信验证，其中主板中的固件包括所述主板的基本输入输出系统 BIOS 的固件和所述主板的基板管理控制器 BMC 的固件。

20. 如权利要求 19 所述的系统，其中，所述第二 TPCM 还用于， 对所述主板中的固件进行可信验证通过之后，控制所述主板的 BIOS 和 BMC 脱离复位状态。

21. 如权利要求 19 所述的系统，其中，所述微型板卡通过所述其它部件控制所述主板中的第二 TPCM 对所述主板进行可信验证，包括：

所述第二 TPCM，切换为串行外围设备接口 SPI 从模式，对所述主板中的外围设备和预设的主板信息进行可信验证。

22. 如权利要求 21 所述的系统，其中，所述微型板卡通过所述其它部件控制所述主板中的所述第二 TPCM 对所述主板进行可信验证，包括：

当对所述主板中的外围设备和预设的主板信息进行可信验证通过之后，所述第二 TPCM，对所述主板上的操作系统的代码进行可信验证。

23. 如权利要求 1 所述的系统，其中，当所述系统通电启动时，包括：

当所述系统通电启动时，所述微型板卡先于所述主板通电启动，且，在所述微型板卡的可信验证通过之前，所述主板保持复位状态；

相应的，在所述微型板卡的可信验证通过后，所述微型板卡控制所述通过主板脱离复位状态。

24. 如权利要求 1 所述的系统，其中，所述主板为服务器主板。

25. 一种可信验证的主板，所述主板中包括复杂可编程逻辑器件 CPLD 和第二可信平台控制模块 TPCM；

所述 CPLD 接收来自于已经通过可信验证的微型板卡的控制信号，并控制第二 TPCM 脱离复位状态；

所述第二 TPCM 对所述主板进行可信验证。

26. 一种可信验证的微型板卡，所述微型板卡连接主板，所述微型板卡中包括第一可信平台控制模块 TPCM；

当设备通电启动时，第一 TPCM，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

27. 如权利要求 26 所述的微型板卡，其中，所述主板验证部件包括现场可编程逻辑

门阵列 FPGA，和/或，复杂可编程逻辑器件 CPLD。

28. 一种服务器，包括：如权利要求 25 所述的主板。

29. 如权利要求 28 所述的服务器，其中，所述服务器还包括：如权利要求 26 或 27 所述的微型板卡。

30. 一种可信验证的方法，应用于包含主板和微型板卡的系统中，所述方法包括：

当所述系统通电启动时，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态，并通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证。

31. 一种计算机存储介质，其上存储有计算机程序，该程序被处理器执行时实现如权利要求 30 所述的可信验证的方法。

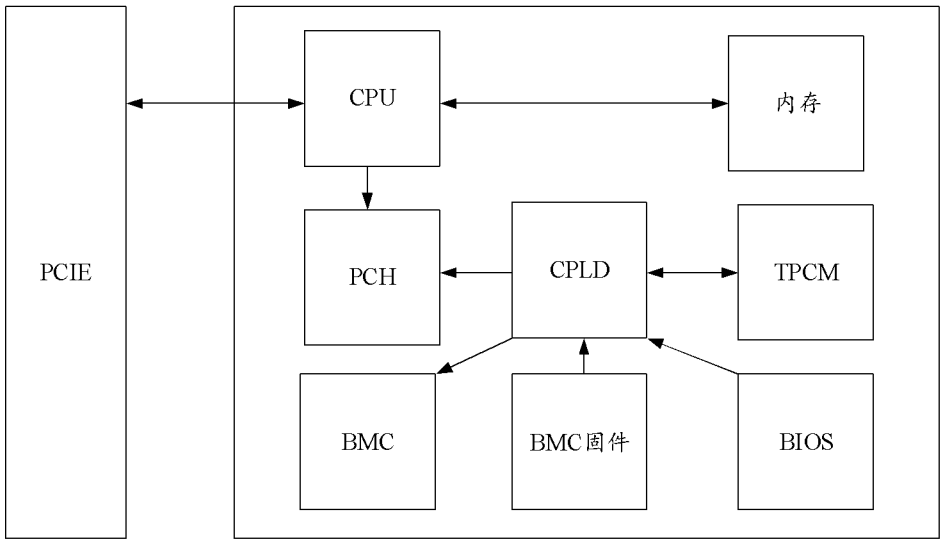
PCIE
CPU
内存
PCH
CPLD
TPCM
BMC
BMC固件
BIOS

图 1A

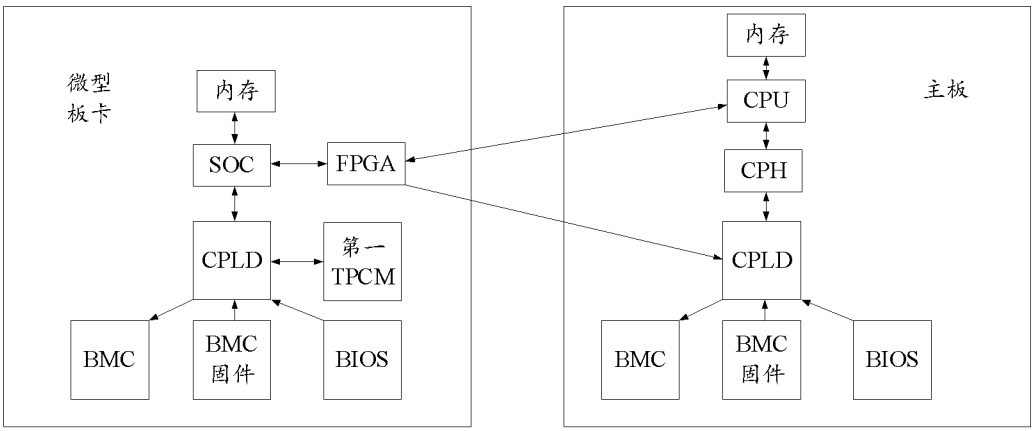
微型
板卡
内存
SOC
FPGA
CPLD
第一
TPCM
BMC
BMC
固件
BIOS
内存
CPU
主板
CPH
CPLD
BMC
BMC
固件
BIOS

图 1B

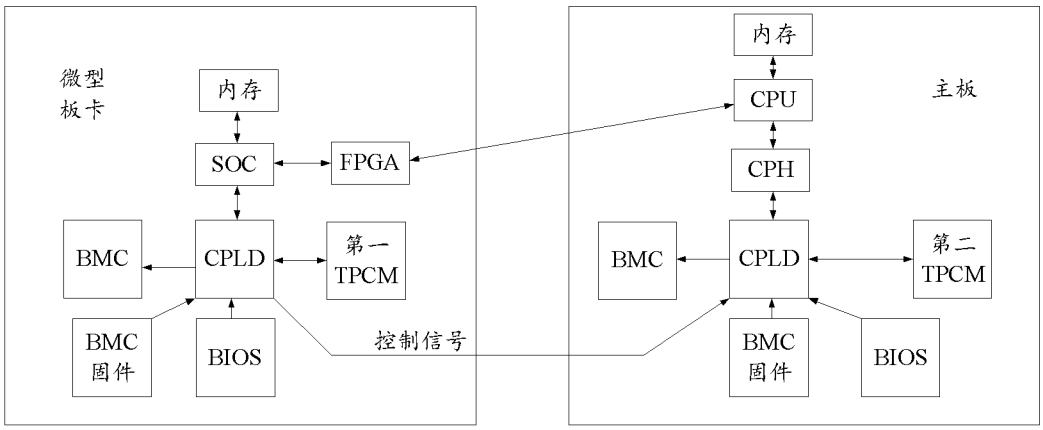
微型
板卡
内存
SOC
FPGA
BMC
CPLD
第一
TPCM
BMC
固件
BIOS
控制信号
内存
CPU
主板
CPH
BMC
CPLD
第二
TPCM
BMC
固件
BIOS

图 1C

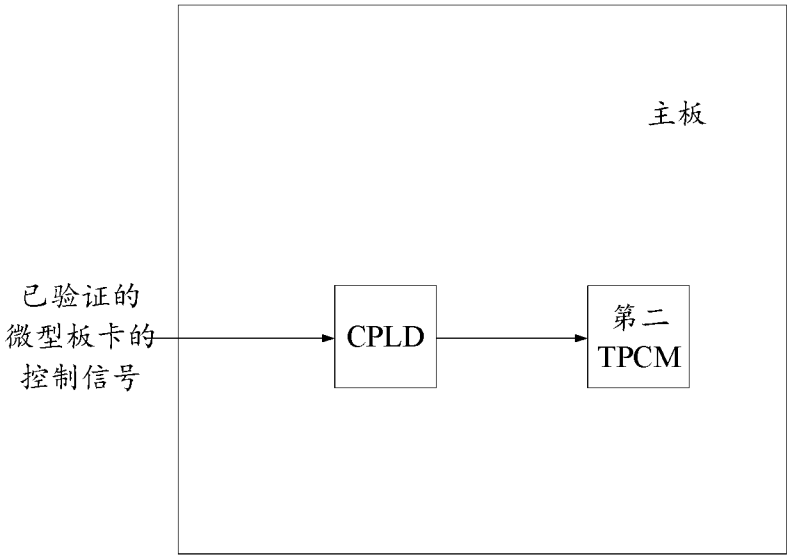

图 1D

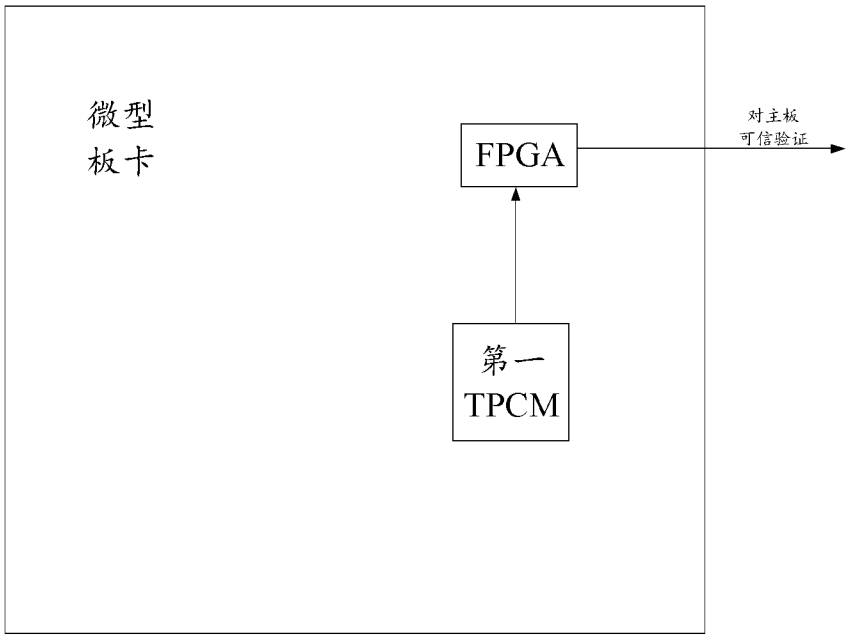

图 1E

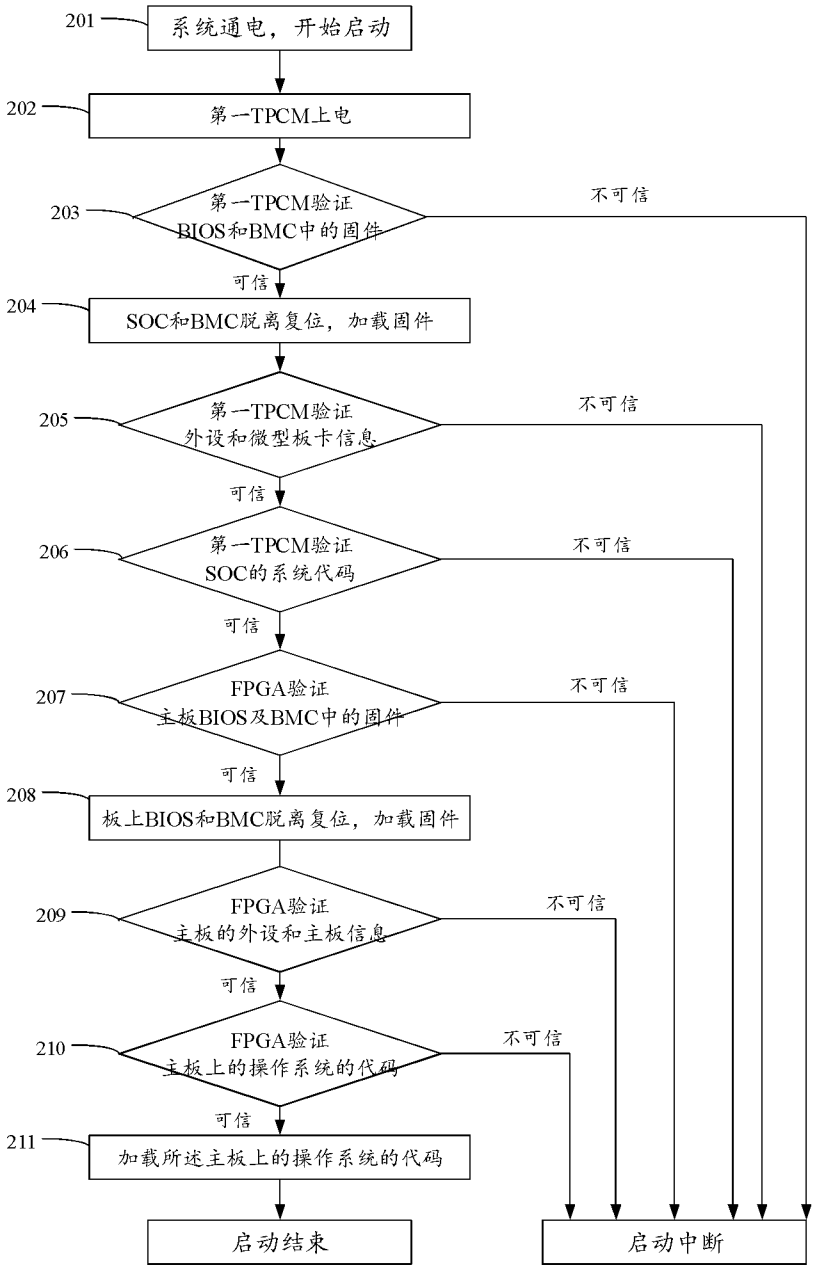
201
系统通电，开始启动
202
第一TPCM上电
203
第一TPCM验证
BIOS和BMC中的固件
不可信
可信
204
SOC和BMC脱离复位，加载固件
205
第一TPCM验证
外设和微型板卡信息
不可信
可信
206
第一TPCM验证
SOC的系统代码
不可信
可信
207
FPGA验证
主板BIOS及BMC中的固件
不可信
可信
208
板上BIOS和BMC脱离复位，加载固件
209
FPGA验证
主板的外设和主板信息
不可信
可信
210
FPGA验证
主板上的操作系统的代码
不可信
可信
211
加载所述主板上的操作系统的代码
启动结束
启动中断

图 2

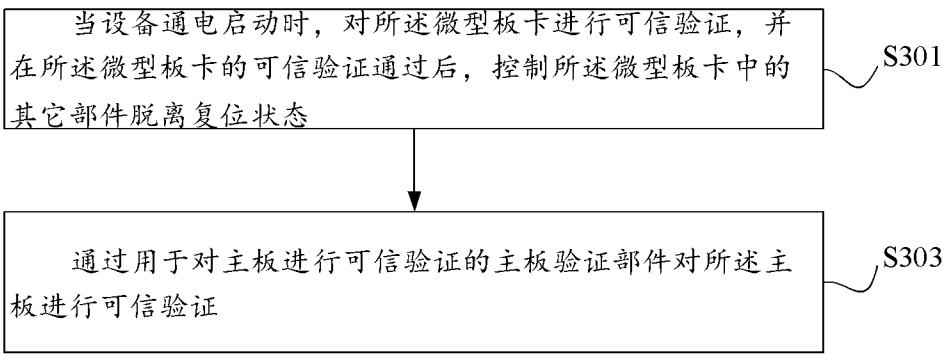
当设备通电启动时，对所述微型板卡进行可信验证，并在所述微型板卡的可信验证通过后，控制所述微型板卡中的其它部件脱离复位状态
S301
通过用于对主板进行可信验证的主板验证部件对所述主板进行可信验证
S303

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/117387

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(2013.01)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

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)

CNKI, CNPAT, WPI, EPODOC: 可信, 验证, 微型板卡, 主板, 复位, TPCM, FPGA, PCIE, CPLD, trust, verify, predict, micro, card, main, board, reset

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 111008379 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 14 April 2020 (2020-04-14) description, paragraphs [0043]-[0101]	1-31
A	CN 109753804 A (BEIJING KEXIN HUATAI INFORMATION TECHNOLOGY CO., LTD. et al.) 14 May 2019 (2019-05-14) entire document	1-31
A	US 2006224878 A1 (INTEL CORPORATION) 05 October 2006 (2006-10-05) entire document	1-31

☐ 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
25 November 2021	**08 December 2021**

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/CN2021/117387

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111008379 A	14 April 2020	None	
CN 109753804 A	14 May 2019	None	
US 2006224878 A1	05 October 2006	None	

国际检索报告

国际申请号
PCT/CN2021/117387

A. 主题的分类

G06F 21/57(2013.01)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

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））

CNKI, CNPAT, WPI, EPODOC: 可信， 验证， 微型板卡， 主板， 复位， TPCM, FPGA, PCIE, CPLD, trust, verify, predict, micro, card, main, board, reset

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
A	CN 111008379 A (腾讯科技深圳有限公司) 2020年4月14日 (2020-04-14) 说明书第[0043]-[0101]段	1-31
A	CN 109753804 A (北京可信华泰信息技术有限公司 等) 2019年5月14日 (2019-05-14) 全文	1-31
A	US 2006224878 A1 (INTEL CORPORATION) 2006年10月5日 (2006-10-05) 全文	1-31

☐ 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
2021年11月25日	2021年12月8日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 邹予婷 电话号码 86-(10)-53961440

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/117387

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 111008379 A	2020年4月14日	无	
CN 109753804 A	2019年5月14日	无	
US 2006224878 A1	2006年10月5日	无	