



(12) 发明专利申请

(10) 申请公布号 CN 111884808 A

(43) 申请公布日 2020. 11. 03

(21) 申请号 202010697255.3

(22) 申请日 2020.07.20

(71) 申请人 杭州溪塔科技有限公司

地址 310000 浙江省杭州市西湖区文三路
478号华星时代广场A座10层1001号

(72) 发明人 王晓亮 张亚宁

(51) Int. Cl.

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

G06Q 40/04 (2012.01)

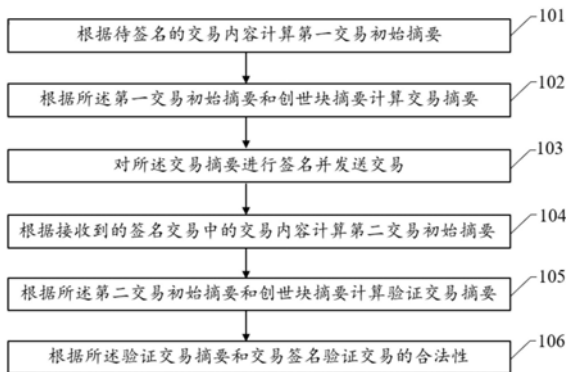
权利要求书1页 说明书6页 附图2页

(54) 发明名称

一种防止交易跨链重放的方法、装置及电子设备

(57) 摘要

本说明书实施例涉及一种防止交易跨链重放的方法、装置及电子设备,主要包括:根据待签名的交易内容计算第一交易初始摘要;根据所述第一交易初始摘要和创世块摘要计算交易摘要;对所述交易摘要进行签名并发送交易;根据接收到的签名交易中的交易内容计算第二交易初始摘要;根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;根据所述验证交易摘要和交易签名验证交易的合法性。通过在用户构造交易的过程中,需要将交易内容与创世块摘要一并参与计算交易摘要,用户再根据得到的交易摘要进行签名。节点在进行验签的时候,也需要包含创世块的摘要进行验证,从而经济便捷地解决了交易跨链重放的问题。



1. 一种防止交易跨链重放的方法,应用于区块链系统,所述方法包括:
根据待签名的交易内容计算第一交易初始摘要;
根据所述第一交易初始摘要和创世块摘要计算交易摘要;
对所述交易摘要进行签名并发送交易;
根据接收到的签名交易中的交易内容计算第二交易初始摘要;
根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;
根据所述验证交易摘要和交易签名验证交易的合法性。
2. 如权利要求1所述的方法,进一步包括:根据所述验证交易摘要和交易签名验证交易为合法时,所述交易进入交易池;
根据所述验证交易摘要和交易签名验证交易为非法时,所述交易被终止。
3. 如权利要求2所述的方法,进一步包括:对所述区块链系统设置RPC接口,调取所述RPC接口获取所述创世块摘要。
4. 如权利要求1-3所述的方法,进一步包括:所述创世块摘要包括创世块的时间戳、初始共识列表、区块链识别标识、初始配置参数中的一个或多个。
5. 一种防止交易跨链重放的装置,应用于区块链系统,所述装置包括:
第一交易初始摘要模块:用于根据待签名的交易内容计算第一交易初始摘要;
交易摘要模块:根据所述第一交易初始摘要和创世块摘要计算交易摘要;
签名模块:用于对所述交易摘要进行签名并发送交易;
第二交易初始摘要模块:根据接收到的签名交易中的交易内容计算第二交易初始摘要;
验证交易摘要模块:根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;
验证模块:根据所述验证交易摘要和交易签名验证交易的合法性。
6. 如权利要求5所述的装置,进一步包括:所述验证模块验证交易为合法时,所述交易进入交易池;
所述验证模块验证交易为非法时,所述交易被终止。
7. 如权利要求6所述的装置,进一步包括RPC接口,通过调取所述RPC接口获取所述创世块摘要。
8. 如权利要求5-7所述的装置,进一步包括:所述创世块摘要包括创世块的时间戳、初始共识列表、区块链识别标识、初始配置参数中的一个或多个。
9. 一种电子设备,包括:
一个或多个处理器;
存储器,用于存储一个或多个计算机程序;
当所述一个或多个程序被所述一个或多个处理器执行时,使得所述一个或多个处理器执行如权利要求1-4中任一项所述的方法。
10. 一种存储有计算机程序的存储介质,其特征在于,该程序被处理器执行时实现如权利要求1-4中任一项所述的方法。

一种防止交易跨链重放的方法、装置及电子设备

技术领域

[0001] 本说明书实施例涉及网络技术领域,尤其涉及一种防止交易跨链重放的方法、装置及电子设备。

背景技术

[0002] 在联盟链中,存在多个私有化部署的联盟链。例如参与方M可以同时两个不同的联盟链chain-A和chain-B中,在这两个区块链系统中M都有参与,也都有发送交易的权限。如果参与方M在两个链中使用的是同一个私钥,则其在chain-A发送过的交易,有可能被恶意攻击者拿到chain-B上进行重放,这样对于chain-B无法判断交易是由M主动发出的还是由恶意攻击者进行的跨链重放。

[0003] 现有的一种方案是在交易中增加字段,比如增加链ID(chain_id)的字段,chain_id是私有化部署的时候,链进行初始化随机生成的,然后固化到创世块中且不允许被修改。通过在交易中增加chain_id字段,用户在发送交易的时候指定chain_id,节点在收到交易的时候通过判断chain_id是否匹配,通过这种方式来防止交易跨链重放。这种方式存在两个缺点,如果chain_id的范围不够大,很容易产生碰撞,同时,交易中chain_id的增加使得交易体积变大,增加了存储和通讯的负担。

发明内容

[0004] 本说明书实施例提供一种防止交易跨链重放的方法、装置及电子设备,用以解决现有技术的如何便捷、准确的防止交易跨链重放的问题。

[0005] 为了解决上述技术问题,本说明书实施例采用下述技术方案:

[0006] 第一方面,提供了一种防止交易跨链重放的方法,应用于区块链系统,所述方法包括:

[0007] 根据待签名的交易内容计算第一交易初始摘要;

[0008] 根据所述第一交易初始摘要和创世块摘要计算交易摘要;

[0009] 对所述交易摘要进行签名并发送交易;

[0010] 根据接收到的签名交易中的交易内容计算第二交易初始摘要;

[0011] 根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;

[0012] 根据所述验证交易摘要和交易签名验证交易的合法性。

[0013] 第二方面,提供了一种防止交易跨链重放的装置,应用于区块链系统,所述装置包括:

[0014] 第一交易初始摘要模块:用于根据待签名的交易内容计算第一交易初始摘要;

[0015] 交易摘要模块:根据所述第一交易初始摘要和创世块摘要计算交易摘要;

[0016] 签名模块:用于对所述交易摘要进行签名并发送交易;

[0017] 第二交易初始摘要模块:根据接收到的签名交易中的交易内容计算第二交易初始摘要;

[0018] 验证交易摘要模块:根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;

[0019] 验证模块:根据所述验证交易摘要和交易签名验证交易的合法性。

[0020] 第三方面,提供了一种电子设备,包括:一个或多个处理器和存储器,其中存储器包含可由该一个或多个处理器执行的一个或多个计算机程序,以使得该一个或多个处理器执行根据本发明各实施例提供的防止交易跨链重放的方法。

[0021] 第四方面,本发明还提供一种存储有计算机程序的存储介质,该计算机程序使计算机执行根据本发明各实施例提供的防止交易跨链重放的方法。

[0022] 本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果:在用户构造交易的过程中,需要将交易内容与创世块摘要一并参与计算交易摘要,用户再根据得到的交易摘要进行签名。节点在进行验签的时候,也需要包含创世块的摘要进行验证,从而经济便捷地解决了交易跨链重放的问题。同时因为交易中不需要包含链ID等额外字段,所以不需要浪费额外的存储和通讯空间。

附图说明

[0023] 为了更清楚地说明本说明书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说明书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,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0024] 图1为本发明实施例提供的防止交易跨链重放的方法的步骤示意图;

[0025] 图2为本发明实施例提供的防止交易跨链重放的装置的结构示意图;

[0026] 图3为本发明实施例提供的电子设备的结构示意图。

具体实施方式

[0027] 为使本说明书实施例的目的、技术方案和优点更加清楚,下面将结合本说明书具体实施例及相应的附图对本说明书实施例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说明书一部分实施例,而不是全部的实施例。基于本说明书中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本说明书实施例保护的范围。

[0028] 以下结合附图,详细说明本说明书各实施例提供的技术方案。

[0029] 实施例一

[0030] 参照图1所示,为本说明书实施例提供的一种防止交易跨链重放的方法的步骤示意图,应用于区块链系统,所述方法包括:

[0031] 步骤101:根据待签名的交易内容计算第一交易初始摘要;

[0032] 步骤102:根据所述第一交易初始摘要和创世块摘要计算交易摘要;

[0033] 步骤103:对所述交易摘要进行签名并发送交易;

[0034] 步骤104:根据接收到的签名交易中的交易内容计算第二交易初始摘要;

[0035] 步骤105:根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;

[0036] 步骤106:根据所述验证交易摘要和交易签名验证交易的合法性。

[0037] 需要说明的是,所述创世块摘要可包括创世块的时间戳、初始共识列表、区块链识别标识、初始配置参数中的一个或多个。以此保证创世块摘要的唯一性,保证在正常的区块链运行过程中,创世块摘要信息发生重复的概率几乎为零。

[0038] 其中,所述方法还可以包括对所述区块链系统设置RPC接口,调取所述 RPC接口获取所述创世块摘要。因此用户在发送交易前,可以先获取链的创世块摘要。在计算交易摘要时,先根据待签名的交易内容计算出其第一交易初始摘要,再将其加上创世块摘要新计算出最终的交易摘要,再进行交易签名和发送。

[0039] 节点在所有需要验证交易合法性的协议中需要新的验证签名规则:节点收到交易者发送的交易之后,根据交易内容计算出第二交易原始摘要,再加上创世块摘要共同计算出验证交易摘要,根据所述验证交易摘要和交易签名验证交易的合法性。

[0040] 进一步的,当根据所述验证交易摘要和交易签名验证交易为合法时,所述交易进入交易池;

[0041] 根据所述验证交易摘要和交易签名验证交易为非法时,该交易可能是伪造或者是从其他链进行的跨链重放,所述交易被终止。

[0042] 同时在共识协议的区块验证中同样需要遵循相同的交易验证规则,如果不符合交易验证规则,则可以认为区块非法,包含伪造的交易或者跨链重放的交易。在节点收到其他节点转发的交易时,同样需要遵循此交易验证规则。

[0043] 通过本说明书技术方案,在用户构造交易的过程中,需要将交易内容与创世块摘要一并参与计算交易摘要,用户再根据得到的交易摘要进行签名。节点在进行验签的时候,也需要包含创世块的摘要进行验证,从而经济便捷地解决了交易跨链重放的问题。同时因为交易中不需要包含链ID等额外字段,所以不需要浪费额外的存储和通讯空间。

[0044] 实施例二

[0045] 参照图2所示,为本说明书实施例提供的防止交易跨链重放的装置的结构示意图,应用于区块链系统,该装置主要包括:

[0046] 第一交易初始摘要模块201:用于根据待签名的交易内容计算第一交易初始摘要;

[0047] 交易摘要模块202:根据所述第一交易初始摘要和创世块摘要计算交易摘要;

[0048] 签名模块203:用于对所述交易摘要进行签名并发送交易;

[0049] 第二交易初始摘要模块204:根据接收到的签名交易中的交易内容计算第二交易初始摘要;

[0050] 验证交易摘要模块205:根据所述第二交易初始摘要和创世块摘要计算验证交易摘要;

[0051] 验证模块206:根据所述验证交易摘要和交易签名验证交易的合法性。

[0052] 可选的,当所述验证模块验证交易为合法时,所述交易进入交易池;所述验证模块验证交易为非法时,所述交易被终止。

[0053] 可选的,所述装置进一步包括RPC接口,通过调取所述RPC接口获取所述创世块摘要。

[0054] 可选的,所述创世块摘要包括创世块的时间戳、初始共识列表、区块链识别标识、初始配置参数中的一个或多个。

[0055] 通过本说明书技术方案,在用户构造交易的过程中,需要将交易内容与创世块摘

要一并参与计算交易摘要,用户再根据得到的交易摘要进行签名。节点在进行验签的时候,也需要包含创世块的摘要进行验证,从而经济便捷地解决了交易跨链重放的问题。同时因为交易中不需要包含链ID等额外字段,所以不需要浪费额外的存储和通讯空间。

[0056] 应理解,本实施例二中所述的装置可以功能模块的形式执行防止交易跨链重放方法所涉及的所有技术方案,并实现相应技术效果,在此不做赘述。

[0057] 实施例三

[0058] 下面参照图3详细介绍本说明书实施例的电子设备。请参考图3,在硬件层面,该电子设备包括一个或多个处理器及存储器。可选地还包括内部总线、网络接口。其中,存储器可能包含内存,例如高速随机存取存储器(Random-Access Memory,RAM),也可能还包括非易失性存储器(Non-Volatile Memory),例如至少1个磁盘存储器等。当然,该电子设备还可能包括其他业务所需要的硬件。

[0059] 处理器、网络接口和存储器可以通过内部总线相互连接,该内部总线可以是工业标准体系结构(Industry Standard Architecture,ISA)总线、外设部件互连标准(Peripheral Component Interconnect,PCI)总线或扩展工业标准结构(Extended Industry Standard Architecture,EISA)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图3中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0060] 存储器,用于存放计算机程序。具体地,计算机程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[0061] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成防止交易跨链重放装置。处理器,执行存储器所存放的程序,并具体用于执行前文所述的防止交易跨链重放装置作为执行主体时所执行的方法操作。

[0062] 上述如本说明书图1所示实施例揭示的装置执行的方法可以应用于处理器中,或者由处理器实现。处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等;还可以是数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本说明书一个或多个实施例中公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本说明书一个或多个实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器 etc 本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

[0063] 当然,除了软件实现方式之外,本说明书实施例的电子设备并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限

定于各个逻辑单元,也可以是硬件或逻辑器件。

[0064] 通过本说明书技术方案,在用户构造交易的过程中,需要将交易内容与创世块摘要一并参与计算交易摘要,用户再根据得到的交易摘要进行签名。节点在进行验签的时候,也需要包含创世块的摘要进行验证,从而经济便捷地解决了交易跨链重放的问题。同时因为交易中不需要包含链ID等额外字段,所以不需要浪费额外的存储和通讯空间。

[0065] 实施例四

[0066] 本说明书实施例还提供一种存储有计算机程序的存储介质,所述计算机可读存储介质存储一个或多个程序,所述一个或多个程序被处理器用来执行描述于本申请的防止交易跨链重放方法。

[0067] 通过本说明书技术方案,在用户构造交易的过程中,需要将交易内容与创世块摘要一并参与计算交易摘要,用户再根据得到的交易摘要进行签名。节点在进行验签的时候,也需要包含创世块的摘要进行验证,从而经济便捷地解决了交易跨链重放的问题。同时因为交易中不需要包含链ID等额外字段,所以不需要浪费额外的存储和通讯空间。

[0068] 总之,以上所述仅为本说明书的较佳实施例而已,并非用于限定本说明书的保护范围。凡在本说明书的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本说明书的保护范围之内。

[0069] 上述一个或多个实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的,计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0070] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体 (transitory media),如调制的数据信号和载波。

[0071] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0072] 本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于系统实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0073] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

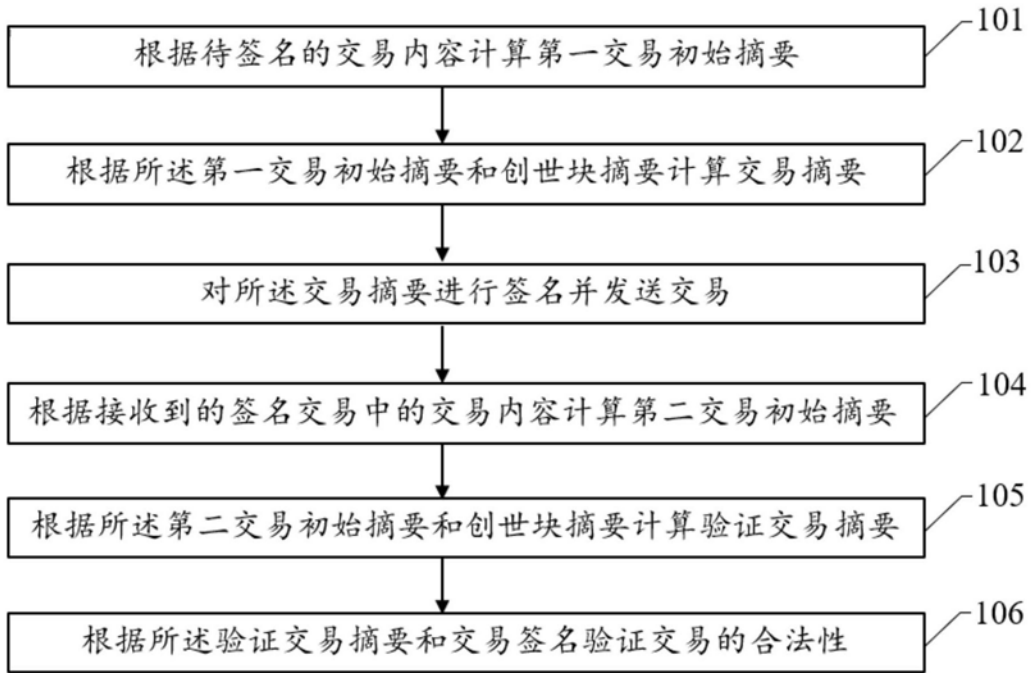


图1

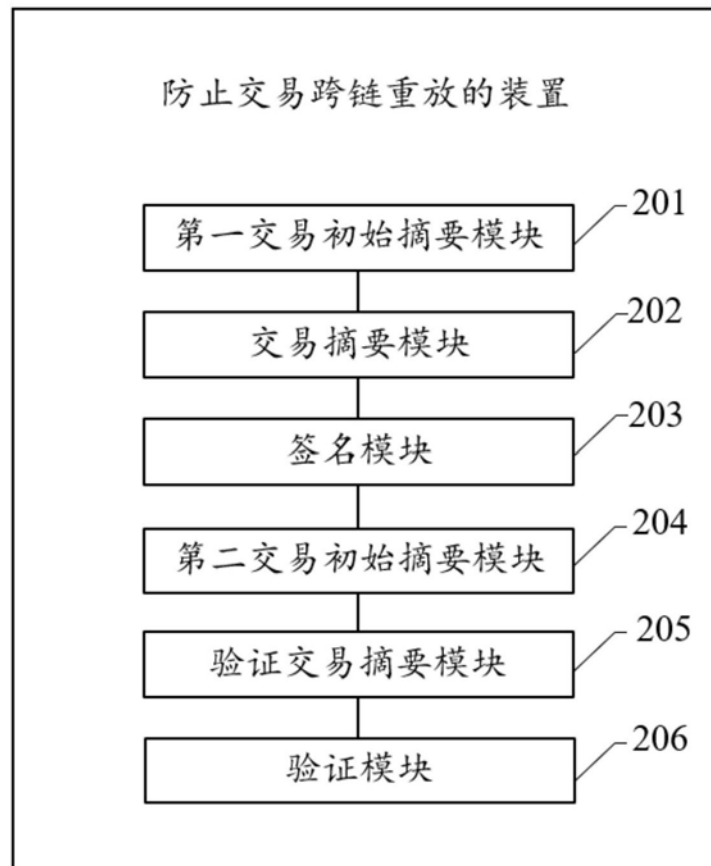


图2

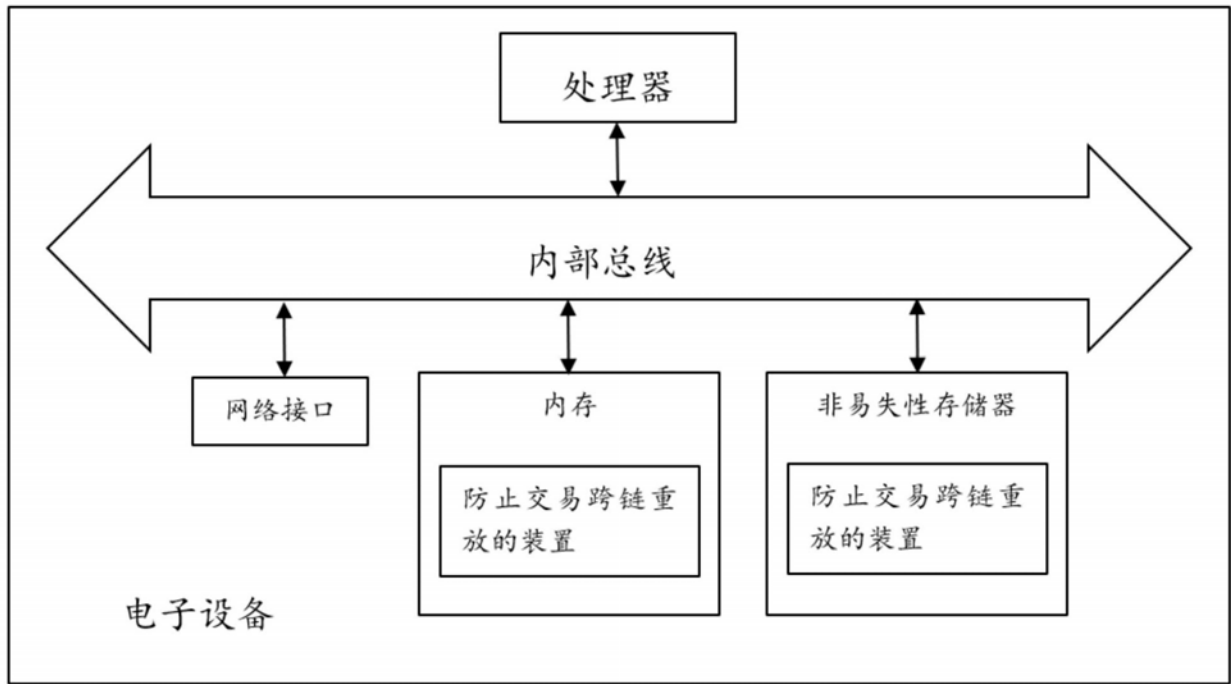


图3