



(12) 发明专利

(10) 授权公告号 CN 109087204 B

(45) 授权公告日 2023.04.14

(21) 申请号 201810841038.X

KR 101877345 B1,2018.07.12

(22) 申请日 2018.07.27

CN 107391320 A,2017.11.24

(65) 同一申请的已公布的文献号

邵奇峰等.区块链技术:架构及进展.《计算机学报》.2017,(第05期),

申请公布号 CN 109087204 A

田道坤 等.在区块链中基于混合算法的数字签名技术.《电子科技》.2018,第31卷(第7期),

(43) 申请公布日 2018.12.25

Nurzhan Zhumabekuly Aitzhan 等

(73) 专利权人 杭州复杂美科技有限公司

.Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams.《IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING》.2016,第15卷(第5期),

地址 310000 浙江省杭州市西湖区文三路

90号东部软件园6号楼6层

(72) 发明人 马登极 王志文 苏彦龙 吴思进

审查员 毛冉

(51) Int.Cl.

G06Q 40/04 (2012.01)

G06Q 20/38 (2012.01)

(56) 对比文件

CN 108009917 A,2018.05.08

CN 107078898 A,2017.08.18

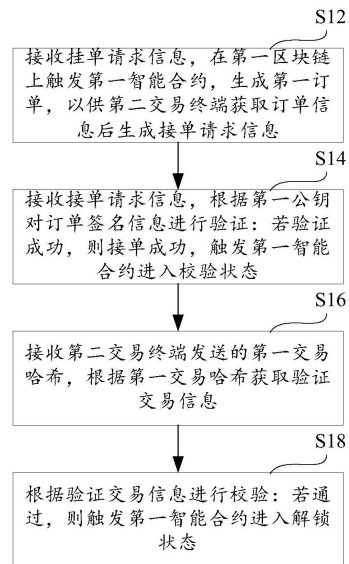
权利要求书2页 说明书6页 附图4页

(54) 发明名称

跨链交易校验方法、设备和存储介质

(57) 摘要

本发明提供一种跨链交易校验方法、设备和存储介质,该方法包括:接收第一交易终端发送的挂单请求信息,根据挂单请求信息在第一区块链上触发第一智能合约,生成第一订单,以供第二交易终端获取第一订单的订单信息后生成接单请求信息;接收接单请求信息,根据第一公钥对订单签名信息进行验证:若验证成功,则接单成功,触发第一智能合约进入校验状态;接收第二交易终端发送的第一交易哈希,根据第一交易哈希获取验证交易信息;根据验证交易信息进行校验:若通过,则触发第一智能合约进入解锁状态。本发明避免了在跨链交易中冒用交易信息而导致双花问题的风险。



1. 一种跨链交易校验方法,其特征在于,包括:

接收第一交易终端发送的挂单请求信息,根据所述挂单请求信息在第一区块链上触发第一智能合约,生成第一订单,以供第二交易终端获取所述第一订单的订单信息后生成接单请求信息;其中,所述接单请求信息包括订单签名信息和第一公钥,所述订单签名信息通过第一私钥对所述订单信息中的任意一项或多项信息签名生成;

接收所述接单请求信息,根据所述第一公钥对所述订单签名信息进行验证:若验证成功,则接单成功,触发所述第一智能合约进入校验状态;

接收所述第二交易终端发送的第一交易哈希;其中,所述第一交易哈希为所述第二交易终端根据所述订单信息在第二区块链上进行支付的交易哈希,所述第一交易哈希还用于供relay服务器或侧链:

在监测到所述第一交易哈希时,根据所述第一交易哈希从所述第二区块链获取验证交易信息;其中,所述验证交易信息来源于所述第二区块链,包括所述支付的收款账户、金额、第二公钥;

根据所述验证交易信息进行校验:若通过,则触发所述第一智能合约进入解锁状态;其中,所述校验包括收款账户校验、金额校验,以及,校验所述第二公钥与所述第一公钥是否相同;

其中,所述第一区块链和所述第二区块链为公链。

2. 根据权利要求1所述的方法,其特征在于,所述接单请求信息还包括所述支付的原始交易哈希;所述校验还包括根据所述验证交易信息对所述原始交易哈希进行验证。

3. 根据权利要求1所述的方法,其特征在于,所述接收所述第二交易终端发送的第一交易哈希,根据所述第一交易哈希获取验证交易信息包括:

接收所述第二交易终端发送的第一交易哈希;

接收服务端发送的验证交易信息;其中,所述验证交易信息由所述服务端在监测到所述第一交易哈希后同步所述第二区块链的数据获取。

4. 根据权利要求1-3任一项所述的方法,其特征在于,所述第二区块链为BTC链,所述第二公钥配置在所述交易信息的vin字段中。

5. 一种跨链交易校验方法,其特征在于,包括:

获取第一订单的订单信息,根据所述订单信息生成接单请求信息;其中,所述第一订单由第一交易终端向第一区块链的节点发送挂单请求信息以在所述第一区块链上触发第一智能合约所生成,所述接单请求信息包括订单签名信息和第一公钥,所述订单签名信息通过第一私钥对所述订单信息中的任意一项或多项信息签名生成;

向所述第一智能合约发送所述接单请求信息,以供所述第一智能合约根据所述第一公钥对所述订单签名信息进行验证:若验证成功,则接单成功,触发所述第一智能合约进入校验状态;

根据所述订单信息在第二区块链上进行支付,将所述支付的第一交易哈希发送至所述第一智能合约,以供所述第一智能合约:

接收relay服务器或侧链发送的根据所述第一交易哈希获取的验证交易信息,并根据所述验证交易信息进行校验:若通过,则触发所述第一智能合约进入解锁状态;其中,所述第一交易哈希为第二交易终端根据所述订单信息在第二区块链上进行支付的交易哈希,所

述验证交易信息来源于所述第二区块链,包括所述支付的收款账户、金额、第二公钥;所述校验包括收款账户校验、金额校验,以及,校验所述第二公钥与所述第一公钥是否相同,所述第一区块链和所述第二区块链为公链。

6. 根据权利要求5所述的方法,其特征在于,所述获取第一订单的订单信息,根据所述订单信息生成接单请求信息包括:

获取第一订单的订单信息;

根据所述订单信息在所述第二区块链上构建所述支付的原始交易;

通过第一私钥对所述订单信息的第一参数签名,生成订单签名信息;

根据原始交易哈希、所述订单签名信息和第一公钥生成接单请求信息;其中,所述原始交易哈希通过对所述原始交易中的任意一项或多项信息进行哈希生成;

所述校验还包括根据所述验证交易信息对所述原始交易哈希进行验证。

7. 根据权利要求5所述的方法,其特征在于,所述验证交易信息由服务端在监测到所述第一交易哈希后同步所述第二区块链的数据获取并发送至所述第一智能合约。

8. 根据权利要求5-7任一项所述的方法,其特征在于,所述第二区块链为BTC链,所述第二公钥配置在所述交易信息的vin字段中。

9. 一种计算机设备,其特征在于,所述设备包括:

一个或多个处理器;

存储器,用于存储一个或多个程序,

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1-8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1-8中任一项所述的方法。

跨链交易校验方法、设备和存储介质

技术领域

[0001] 本申请涉及互联网金融技术领域,具体涉及一种跨链交易校验方法、设备和存储介质。

背景技术

[0002] 在当前的跨链交易场景中,两条区块链上的交易是完全隔离的,用户的转账交易信息存在被他人冒用而导致双花问题的风险。例如,用户Alice在ETH链上构建了BTC收款账户相同的两笔订单,用户 Bob和Cindy分别接受了这两笔订单,当用户Bob在BTC链上给用户Alice转账时,由于BTC交易的非实时性、网络阻塞或其它原因,可能会导致Bob的交易信息被Cindy提前获取,则Cindy可以抢先于Bob 将Bob的交易信息提交给ETH链进行验证,此时只要Bob所支付的金额不小于Cindy所接受订单的金额,验证即会通过,从而导致双花问题。

[0003] 进一步地,除了交易信息被他人冒用而导致双花问题的风险外,现有的跨链交易方案中还存在使用本人的另一笔交易的交易信息冒充跨链交易的交易信息导致双花问题的风险。例如,Bob在接Alice的跨链订单之前,还通过交易所或其它渠道向Alice的BTC账户支付过一笔转账交易,该笔转账交易的账户金额也符合跨链订单的验证要求,则Bob可以将该笔转账交易冒用为跨链订单的交易。

发明内容

[0004] 鉴于现有技术中的上述缺陷或不足,期望提供一种避免交易信息被他人冒用而导致双花问题的风险的跨链交易校验方法、设备和存储介质;并进一步避免本人采用另一笔不同渠道、相同账户的转账交易冒用为跨链交易而导致双花问题的风险。

[0005] 第一方面,本发明提供一种跨链交易校验方法,包括:

[0006] 接收第一交易终端发送的挂单请求信息,根据挂单请求信息在第一区块链上触发第一智能合约,生成第一订单,以供第二交易终端获取第一订单的订单信息后生成接单请求信息;其中,接单请求信息包括订单签名信息和第一公钥,订单签名信息通过第一私钥对订单信息中的任意一项或多项信息签名生成;

[0007] 接收接单请求信息,根据第一公钥对订单签名信息进行验证:若验证成功,则接单成功,触发第一智能合约进入校验状态;

[0008] 接收第二交易终端发送的第一交易哈希,根据第一交易哈希获取验证交易信息;其中,第一交易哈希包括第二交易终端根据订单信息在第二区块链上进行支付的交易哈希,验证交易信息来源于第二区块链,包括支付的收款账户、金额、第二公钥;

[0009] 根据验证交易信息进行校验:若通过,则触发第一智能合约进入解锁状态;其中,校验包括收款账户校验、金额校验,以及,校验第二公钥与第一公钥是否相同。

[0010] 第二方面,本发明提供另一种跨链交易校验方法,包括:

[0011] 获取第一订单的订单信息,根据订单信息生成接单请求信息;其中,第一订单由第一交易终端向第一区块链的节点发送挂单请求信息以在第一区块链上触发第一智能合约

所生成,接单请求信息包括订单签名信息和第一公钥,订单签名信息通过第一私钥对订单信息中的任意一项或多项信息签名生成;

[0012] 向第一智能合约发送接单请求信息,以供第一智能合约根据第一公钥对订单签名信息进行验证:若验证成功,则接单成功,触发第一智能合约进入校验状态;

[0013] 根据订单信息在第二区块链上进行支付,将所述支付的第一交易哈希发送至第一智能合约,以供第一智能合约根据第一交易哈希获取验证交易信息,并根据验证交易信息对第一交易哈希进行校验:若通过,则触发第一智能合约进入解锁状态;其中,验证交易信息来源于第二区块链,包括支付的收款账户、金额、第二公钥;校验包括收款账户校验、金额校验,以及,校验第二公钥与第一公钥是否相同。

[0014] 第三方面,本发明还提供一种设备,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指令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跨链交易校验方法。

[0015] 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跨链交易校验方法。

[0016] 本发明诸多实施例提供的跨链交易校验方法、设备和存储介质通过在接单请求信息中配置订单签名信息和第一公钥以供合约验证接单者是第一公钥的拥有者,并通过验证该订单的交易信息所包括的第二公钥是否与第一公钥相同来验证该笔交易是由接单者支付的,从而使被他人冒用的交易信息无法通过验证,避免了交易信息被他人冒用而导致双花问题的风险;

[0017] 本发明一些实施例提供的跨链交易校验方法、设备和存储介质进一步通过在接单请求信息中配置原始交易哈希,并通过验证该订单的交易信息对原始交易哈希进行验证,从而使接单者本人将另一笔不同渠道、相同账户的转账交易冒用为跨链交易时无法通过验证,进一步避免了双花问题的风险。

附图说明

[0018] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述,本申请的其它特征、目的和优点将会变得更明显:

[0019] 图1为本发明一实施例中跨链交易的校验场景示意图。

[0020] 图2为本发明一实施例提供的一种跨链交易校验方法的流程图。

[0021] 图3为本发明一实施例提供的另一种跨链交易校验方法的流程图。

[0022] 图4为图3所示方法的一种优选实施方式中步骤S22的流程图。

[0023] 图5为本发明一实施例提供的一种设备的结构示意图。

具体实施方式

[0024] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是,此处所描述的具体实施例仅仅用于解释相关发明,而非对该发明的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与发明相关的部分。

[0025] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0026] 图1为本发明一实施例中跨链交易的校验场景示意图。如图1所示,在本实施例中,通过以下跨链交易的校验场景为例,对本发明提供跨链交易校验解决方案进行阐述:

[0027] 用户甲的第一交易终端100在ETH链上构建了在BTC链上进行收款的跨链订单,用户乙的第二交易终端200接受该笔跨链订单、在 BTC链上对用户甲进行转账交易,并向ETH链的智能合约发送第一交易哈希,ETH链的智能合约根据第一交易哈希获取验证交易信息后进行校验。

[0028] 图1在展示上述校验场景的同时还展示了一种优选的校验过程,以下将结合图2-4进行详细阐述。

[0029] 在更多实施例中,本发明提供的解决方案还可以应用于任意的两条区块链之间的跨链交易校验,可实现相同的技术效果。

[0030] 图2为本发明一实施例提供的一种跨链交易校验方法的流程图。

[0031] 如图2所示,在本实施例中,本发明提供一种适用于第一区块链节点的跨链交易校验方法,包括:

[0032] S12:接收第一交易终端发送的挂单请求信息,根据挂单请求信息在第一区块链上触发第一智能合约,生成第一订单,以供第二交易终端获取第一订单的订单信息后生成接单请求信息;其中,接单请求信息包括订单签名信息和第一公钥,订单签名信息通过第一私钥对订单信息中的任意一项或多项信息签名生成;

[0033] S14:接收接单请求信息,根据第一公钥对订单签名信息进行验证:若验证成功,则接单成功,触发第一智能合约进入校验状态;

[0034] S16:接收第二交易终端发送的第一交易哈希,根据第一交易哈希获取验证交易信息;其中,第一交易哈希包括第二交易终端根据订单信息在第二区块链上进行支付的交易哈希,验证交易信息来源于第二区块链,包括支付的收款账户、金额、第二公钥;

[0035] S18:根据验证交易信息进行校验:若通过,则触发第一智能合约进入解锁状态;其中,校验包括收款账户校验、金额校验,以及,校验第二公钥与第一公钥是否相同。

[0036] 具体地,以图1所示的场景为例:

[0037] 当用户甲想要用若干以太坊(eth)置换若干比特币(btc)时,通过第一交易终端100向ETH链的节点301发送挂单请求;

[0038] 在步骤S12中,ETH链的节点301接收到上述挂单请求,在ETH链上触发第一智能合约,生成第一订单,并根据挂单请求冻结用户甲的eth;

[0039] 用户乙的第二交易终端200获取第一订单的订单信息,并接收到用户乙的接单指令后,根据该订单信息在BTC链上构建一项原始交易,例如:

[0040] bitcoind createrawtransaction\
[0041] '[{"txid":"296ea7bf981b44999d689853d17fe0ceb852a8a34e68fcd19f0a41e589132156","vout":0}]'\

[0042] '{"1Q8s4qDRbCbFypG5AFNR9tFC57PstkPX1x":0.1, "1Lab618UuWjLmVA1Q64tHZXcLoc4397ZX3":0.0989}'

[0043] 第二交易终端200同时还通过用户乙的第一私钥a对上述订单信息中的挂单ID:O₁进行签名,生成订单签名信息sign(O₁),并生成接单请求信息。其中,该接单请求信息包括订单签名信息sign(O₁)和对应于第一私钥a的第一公钥A。在本实施例中,订单签名信息通

通过对挂单ID签名生成,在更多实施例中,还可以根据实际需求将订单签名信息配置为对订单信息中的任意一项或多项信息进行签名生成,例如,第二区块链上的收款账户、第一区块链上的交易金额、第二区块链上的交易金额,等等,可实现相同的技术效果。

[0044] 在步骤S14中,第一智能合约接收到第二交易终端200发送的接单请求信息,通过第一公钥A对订单签名信息 $\text{sign}(O_1)$ 进行验证:

[0045] 若验证失败,则接单失败;

[0046] 若验证成功,则证明接单者为第一公钥A的持有者,接单成功,触发第一智能合约进入校验状态。

[0047] 在接单成功后,第二交易终端200通过上述构建的原始交易在BTC链上对用户甲进行转账交易,获得该笔转账交易的第一交易哈希 H_2 ,并将第一交易哈希 H_2 发送至第一智能合约。

[0048] 在步骤S16中,第一智能合约接收第一交易哈希 H_2 并写入ETH链;

[0049] 服务端(relay)500通过同步ETH链的数据监测到第一交易哈希 H_2 后,同步BTC链的数据并根据第一交易哈希 H_2 查找到验证交易信息,具体包括spv信息(用于验证收款账户、收款金额等信息)和vin字段信息(vin字段中的asm字段中包括第二公钥,用于验证是否与第一公钥相同),并将验证交易信息发送至第一智能合约。

[0050] 具体地,在本实施例中,采用中继的方式(配置relay)来为第一智能合约获取验证交易信息,在更多实施例中,还可以通过侧链等本领域常用的不同跨链技术来为第一智能合约获取验证交易信息,可实现相同的技术效果。

[0051] 在步骤S18中,第一智能合约根据验证交易信息进行以下校验:校验收款账户是否正确、校验收款金额是否满足订单要求、校验第一公钥与第二公钥是否相同,等等:

[0052] 若任一项校验失败,则校验未通过,继续等待验证交易信息,直至超时回退;例如,当用户乙并没有对用户甲进行支付,而是将用户丙对用户甲支付的交易哈希 H_3 冒用为第一交易哈希发送给第一智能合约时,则第一智能合约根据 H_3 获取到的第二公钥是用户丙的公钥B,第一公钥A与第二公钥B不相同,无法通过验证,说明交易哈希为 H_3 的该笔BTC链上的转账交易不是接单者用户乙所支付的,而是冒用了他人支付的交易信息;

[0053] 若全部校验成功,则校验通过,触发第一智能合约进入解锁状态。

[0054] 上述实施例通过在接单请求信息中配置订单签名信息和第一公钥以供合约验证接单者是第一公钥的拥有者,并通过验证该订单的交易信息所包括的第二公钥是否与第一公钥相同来验证该笔交易是由接单者支付的,从而使被他人冒用的交易信息无法通过验证,避免了交易信息被他人冒用而导致双花问题的风险。

[0055] 在一优选实施例中,上述接单请求信息还包括上述支付的原始交易哈希,上述校验还包括根据验证交易信息对原始交易哈希进行验证。

[0056] 具体地,该优选实施例与上述图2所示实施例的区别在于:

[0057] 第二交易终端200在构建原始交易之后,对原始交易中的若干信息,例如txid、vout等信息中的任意一项或多项(优选为多项)进行哈希,得到原始交易哈希 H_1 ,并将原始交易哈希 H_1 作为接单请求信息的一项参数。

[0058] 在步骤S18中的验证还包括:从验证交易信息中提取txid、vout等信息,对原始交易哈希 H_1 进行验证:

[0059] 若验证失败,则证明该笔BTC链上的转账交易并非接单时构建的交易,而是冒用的另一笔交易的交易信息(若第一公钥与第二公钥相同,则说明是接单者本人支付的另一笔交易);

[0060] 若验证成功,则证明该笔转账交易确实是接单时构建的交易,验证通过。

[0061] 上述实施例进一步通过在接单请求信息中配置原始交易哈希,并通过验证该订单的交易信息对原始交易哈希进行验证,从而使接单者本人将另一笔不同渠道、相同账户的转账交易冒用为跨链交易时无法通过验证,进一步避免了双花问题的风险。

[0062] 图3为本发明一实施例提供的另一种跨链交易校验方法的流程图。图3所示的方法可配合图2所示的方法执行。

[0063] 如图3所示,在本实施例中,本发明还提供另一种适用于第二交易终端200的跨链交易校验方法,包括:

[0064] S22:获取第一订单的订单信息,根据订单信息生成接单请求信息;其中,第一订单由第一交易终端向第一区块链的节点发送挂单请求信息以在第一区块链上触发第一智能合约所生成,接单请求信息包括订单签名信息和第一公钥,订单签名信息通过第一私钥对订单信息中的任意一项或多项信息签名生成;

[0065] S24:向第一智能合约发送接单请求信息,以供第一智能合约根据第一公钥对订单签名信息进行验证;若验证成功,则接单成功,触发第一智能合约进入校验状态;

[0066] S26:根据订单信息在第二区块链上进行支付,将所述支付的第一交易哈希发送至第一智能合约,以供第一智能合约根据第一交易哈希获取验证交易信息,并根据验证交易信息对第一交易哈希进行校验;若通过,则触发第一智能合约进入解锁状态;其中,验证交易信息来源于第二区块链,包括支付的收款账户、金额、第二公钥;校验包括收款账户校验、金额校验,以及,校验第二公钥与第一公钥是否相同。

[0067] 具体地,图3所示方法的校验原理可参考图2所示的方法,此处不再赘述。

[0068] 图4为图3所示方法的一种优选实施方式中步骤S22的流程图。图4所示方法可配合上述图2所示方法的优选实施例执行。

[0069] 如图4所示,在一优选实施例中,步骤S22包括:

[0070] S221:获取第一订单的订单信息;

[0071] S223:根据订单信息在第二区块链上构建支付的原始交易;

[0072] S225:通过第一私钥对订单信息的第一参数签名,生成订单签名信息;

[0073] S227:根据原始交易哈希、订单签名信息和第一公钥生成接单请求信息;其中,原始交易哈希通过对原始交易中的任意一项或多项信息进行哈希生成。

[0074] 上述校验还包括根据验证交易信息对原始交易哈希进行验证。

[0075] 具体地,图4所示方法的校验原理可参照上述图2所示方法的优选实施例,此处不再赘述。

[0076] 在一优选实施例中,验证交易信息由服务端在监测到第一交易哈希后同步第二区块链的数据获取并发送至第一智能合约。

[0077] 在一优选实施例中,第二区块链为BTC链,第二公钥配置在交易信息的vin字段中。

[0078] 图5为本发明一实施例提供的一种设备的结构示意图。

[0079] 如图5所示,作为另一方面,本申请还提供了一种设备500,包括一个或多个中央处

理单元 (CPU) 501, 其可以根据存储在只读存储器 (ROM) 502 中的程序或者从存储部分 508 加载到随机访问存储器 (RAM) 503 中的程序而执行各种适当的动作和处理。在 RAM 503 中, 还存储有设备 500 操作所需的各种程序和数据。CPU 501、ROM 502 以及 RAM 503 通过总线 504 彼此相连。输入/输出 (I/O) 接口 505 也连接至总线 504。

[0080] 以下部件连接至 I/O 接口 505: 包括键盘、鼠标等的输入部分 506; 包括诸如阴极射线管 (CRT)、液晶显示器 (LCD) 等以及扬声器等的输出部分 507; 包括硬盘等的存储部分 508; 以及包括诸如 LAN 卡、调制解调器等网络接口卡的通信部分 509。通信部分 509 经由诸如因特网的网络执行通信处理。驱动器 510 也根据需要连接至 I/O 接口 505。可拆卸介质 511, 诸如磁盘、光盘、磁光盘、半导体存储器等等, 根据需要安装在驱动器 510 上, 以便于从其上读出的计算机程序根据需要被安装入存储部分 508。

[0081] 特别地, 根据本公开的实施例, 上述任一实施例描述的跨链交易校验方法可以被实现为计算机软件程序。例如, 本公开的实施例包括一种计算机程序产品, 其包括有形地包含在机器可读介质上的计算机程序, 所述计算机程序包含用于执行跨链交易校验方法的程序代码。在这样的实施例中, 该计算机程序可以通过通信部分 509 从网络上被下载和安装, 和/或从可拆卸介质 511 被安装。

[0082] 作为又一方面, 本申请还提供了一种计算机可读存储介质, 该计算机可读存储介质可以是上述实施例的装置中所包含的计算机可读存储介质; 也可以是单独存在, 未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序, 该程序被一个或者一个以上的处理器用来执行描述于本申请的跨链交易校验方法。

[0083] 附图中的流程图和框图, 图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上, 流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分, 该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意, 在有些作为替换的实现中, 方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如, 两个接连地表示的方框实际上可以基本并行地执行, 它们有时也可以按相反的顺序执行, 这根据所涉及的功能而定。也要注意, 框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合, 可以通过执行规定的功能或操作的专用的基于硬件的系统来实现, 或者可以通过专用硬件与计算机指令的组合来实现。

[0084] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现, 也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中, 例如, 各所述单元可以是设置在计算机或移动智能设备中的软件程序, 也可以是单独配置的硬件装置。其中, 这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0085] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解, 本申请中所涉及的发明范围, 并不限于上述技术特征的特定组合而成的技术方案, 同时也应涵盖在不脱离本申请构思的情况下, 由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的 (但不限于) 具有类似功能的技术特征进行互相替换而形成的技术方案。

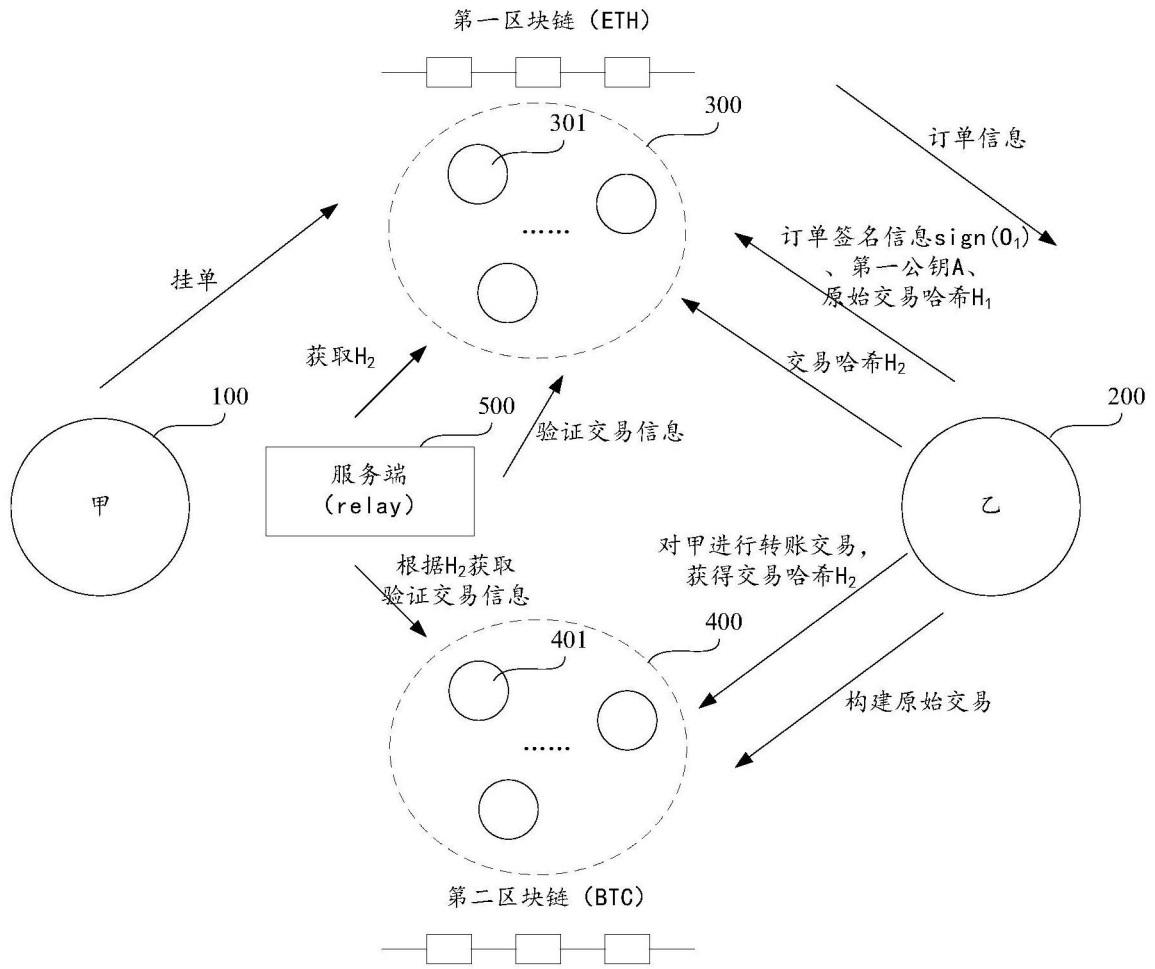


图1

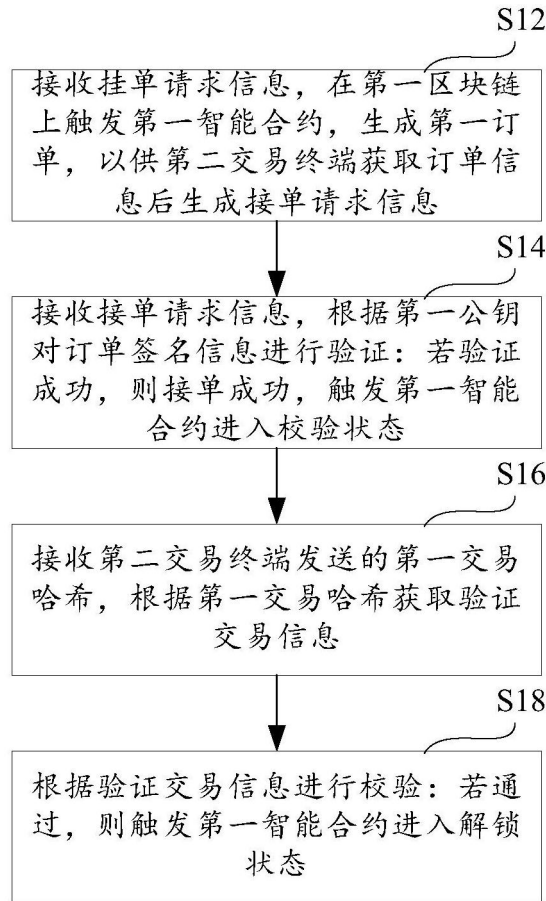


图2

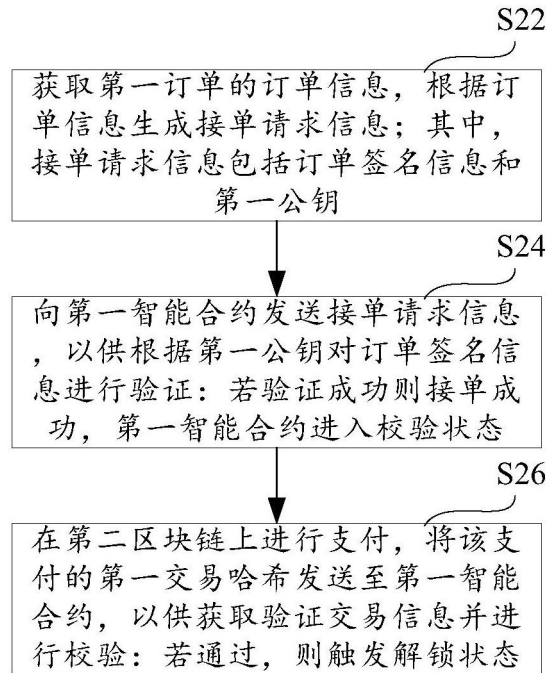


图3

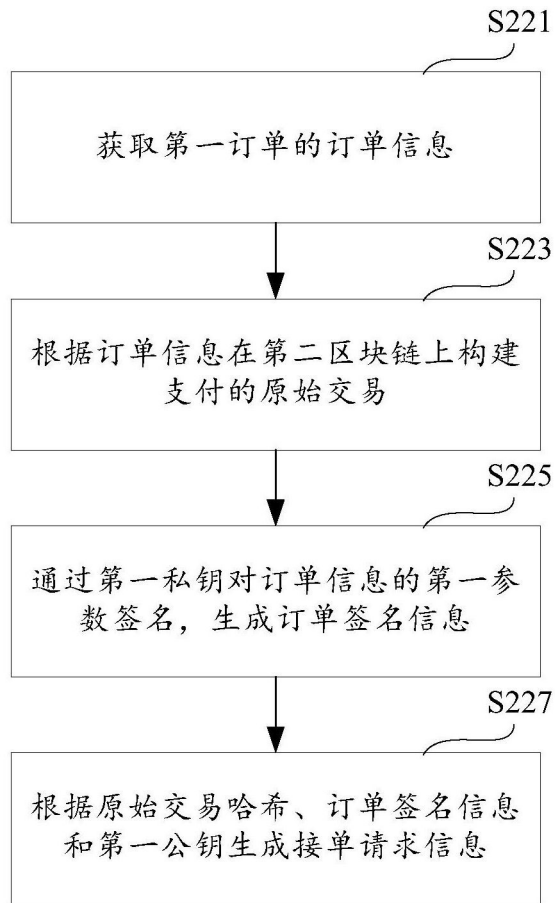


图4

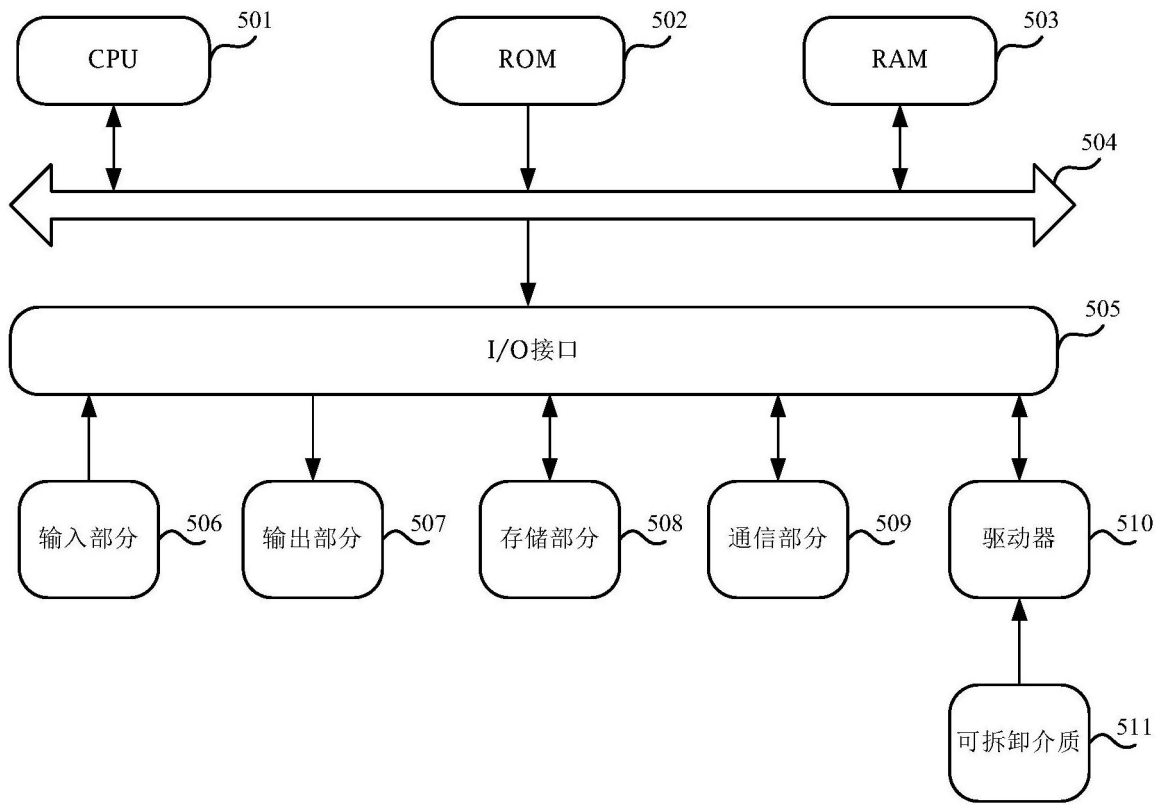


图5